VPRN Service Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context config>service>vprn
config>service>vprn>dhcp6>server>failover
config>service>vprn>igmp-trk
config>service>vprn>red-if
config>service>vprn>router-advert>if
config>service>vprn>gsmp
config>service>vprn>gsmp>group
config>service>vprn>gsmp>group>neighbor
config>service>vprn>igmp
config>service>vprn>igmp>if
config>service>vprn>igmp>if>mcac
config>service>vprn>igmp>if>mcac>mc-constraints
config>service>vprn>if
config>service>vprn>if>dhcp
config>service>vprn>if>dhcp>proxy
config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp
config>service>vprn>if>sap
config>service>vprn>if>sap>static-host
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor
config>service>vprn>mvpn>provider-tunnel>inclusive>pim
config>service>vprn>ospf
config>service>vprn>ospf>area>if
config>service>vprn>ospf3
config>service>vprn>ospf3>area>if
config>service>vprn>ospf3>area>virtual-link
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf>area>sham-link
config>service>vprn>red-if>spoke-sdp
config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor
config>service>vprn>pim
config>service>vprn>pim>if
config>service>vprn>pim>rp>bsr-candidate
config>service>vprn>pim>rp>ipv6>bsr-candidate

config>service>vprn>pim>rp>ipv6>embedded-rp
config>service>vprn>pim>rp>ipv6>rp-candidate
config>service>vprn>sub-if>grp-if
config>service>vprn>sub-if>grp-if>dhcp
config>service>vprn>sub-if>grp-if>dhcp>proxy-server
config>service>vprn>sub-if>grp-if>sap
config>service>vprn>sub-if>grp-if>arp-host
config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt
config>service>vprn>dhcp>server>failover
config>service>vprn>nw-if>dhcp
config>service>vprn>nw-if>eth-cfm>mep
config>service>vprn>radius-proxy>server>cache
config>service>vprn>radius-proxy>server
config>service>vprn>radius-server
config>service>vprn>ipsec-if
config>service>vprn>ipsec-if>sap>tunnel

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

If the AS number was previously changed, the BGP AS number inherits the new value.

Special Cases:

Service Admin State — Bindings to an SDP within the service will be put into the out-of-service state when the service is shutdown. While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

A service is regarded as operational providing that one IP Interface SAP and one SDP is operational.

VPRN BGP and RIP — This command disables the BGP or RIP instance on the given IP interface. Routes learned from a neighbor that is shutdown are immediately removed from the BGP or RIP database and RTM. If BGP or RIP is globally shutdown, then all RIP group and neighbor interfaces are shutdown operationally. If a BGP or RIP group is shutdown, all member neighbor interfaces are shutdown operationally. If a BGP or RIP neighbor is shutdown, just that neighbor interface is operationally shutdown.

description

Syntax **description** *description-string*
no description

Context config>service>vprn>if>dhcp
config>service>vprn>bgp
config>service>vprn>rip

config>service>vprn
config>service>vprn>red-if
config>service>vprn>if
config>service>vprn>if>sap
config>service>vprn>if>dhcp
config>service>vprn>if>dhcp5
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor
config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor
config>service>vprn>subscriber-interface
config>service>vprn>sub-if>dhcp
config>service>vprn>sub-if>grp-if
config>service>vprn>sub-if>grp-if>dhcp
config>service>vprn>sub-if>grp-if>sap>atm
config>service>vprn>dhcp
config>service>vprn>dhcp>server>pool
config>service>vprn>sub-if>grp-if>pppoe
config>service>vprn>nw-if
config>service>vprn>radius-proxy>server
config>service>vprn>ipsec-if>sap>tunnel

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default No description associated with the configuration context.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Global Commands

vprn

Syntax **vprn** *service-id* [**customer** *customer-id*] [**create**]
no vprn *service-id*

Context config>service

Description This command creates or edits a Virtu9al Private Routed Network (VPRN) service instance.

If the *service-id* does not exist, a context for the service is created. If the *service-id* exists, the context for editing the service is entered.

VPRN services allow the creation of customer-facing IP interfaces in the same routing instance used for service network core routing connectivity. VPRN services require that the IP addressing scheme used by the subscriber must be unique between it and other addressing schemes used by the provider and potentially the entire Internet.

IP interfaces defined within the context of an VPRN service ID must have a SAP created as the access point to the subscriber network.

When a service is created, the **customer** keyword and *customer-id* must be specified and associates the service with a customer. The *customer-id* must already exist having been created using the customer command in the service context. When a service is created with a customer association, it is not possible to edit the customer association. The service must be deleted and re-created with a new customer association.

When a service is created, the use of the **customer** *customer-id* is optional to navigate into the service configuration context. If attempting to edit a service with the incorrect *customer-id* results in an error.

Multiple VPRN services are created to separate customer-owned IP interfaces. More than one VPRN service can be created for a single customer ID. More than one IP interface can be created within a single VPRN service ID. All IP interfaces created within an VPRN service ID belongs to the same customer.

The **no** form of the command deletes the VPRN service instance with the specified *service-id*. The service cannot be deleted until all the IP interfaces and all routing protocol configurations defined within the service ID have been shutdown and deleted.

Default None — No VPRN service instances exist until they are explicitly created.

Parameters *service-id* — The unique service identification number identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7750 SR and 7710 SR on which this service is defined.

Values

service-id:	1 — 2147483648
svc-name:	64 characters maximum

customer *customer-id* — Specifies an existing customer identification number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 — 2147483647

aggregate

Syntax **aggregate** *ip-prefix/ip-prefix-length* [**summary-only**] [**as-set**] [**aggregator** *as-number: ip-address*] [**community** *comm-id*] [**black-hole** | **indirect** *ip-address*]
no aggregate *ip-prefix/ip-prefix-length*

Context config>service>vprn

Description This command creates an aggregate route.

Use this command to automatically install an aggregate in the routing table when there are one or more component routes. A component route is any route used for forwarding that is a more-specific match of the aggregate.

The use of aggregate routes can reduce the number of routes that need to be advertised to neighbor routers, leading to smaller routing table sizes.

Overlapping aggregate routes may be configured; in this case a route becomes a component of only the one aggregate route with the longest prefix match. For example if one aggregate is configured as 10.0.0.0/16 and another as 10.0.0.0/24, then route 10.0.128/17 would be aggregated into 10.0.0.0/16, and route 10.0.0.128/25 would be aggregated into 10.0.0.0/24. If multiple entries are made with the same prefix and the same mask the previous entry is overwritten.

A standard 4-byte BGP community may be associated with an aggregate route in order to facilitate route policy matching.

By default aggregate routes are not installed in the forwarding table, however there are configuration options that allow an aggregate route to be installed with a black-hole next hop or with an indirect IP address as next hop.

The **no** form of the command removes the aggregate.

Default No aggregate routes are defined.

Parameters *ip-prefix* — The destination address of the aggregate route in dotted decimal notation.

Values

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 — 32
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 — FFFF]H d: [0 — 255]D
ipv6-prefix-length	0 — 128

The mask associated with the network address expressed as a mask length.

Values 0 — 32

summary-only — This optional parameter suppresses advertisement of more specific component routes for the aggregate.

To remove the **summary-only** option, enter the same aggregate command without the **summary-only** parameter.

as-set — This optional parameter is only applicable to BGP and creates an aggregate where the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Use this feature carefully as it can increase the amount of route churn due to best path changes.

aggregator *as-number*:*ip-address* **—** This optional parameter specifies the BGP aggregator path attribute to the aggregate route. When configuring the aggregator, a two-octet AS number used to form the aggregate route must be entered, followed by the IP address of the BGP system that created the aggregate route.

community *comm-id* **—** This configuration option associates a BGP community with the aggregate route. The community can be matched in route policies and is automatically added to BGP routes exported from the aggregate route.

Values	comm-id	asn:comm-val | well-known-comm
	asn	0 — 65535
	comm-val	0 — 65535
	well-known-comm	no-advertise, no-export, no-export-subconfed

black-hole — This optional parameter installs the aggregate route, when activated, in the FIB with a black-hole next-hop; where packets matching this route are discarded.

indirect *ip-address* **—** This configuration option specifies that the aggregate route should be installed in the FIB with a next-hop taken from the route used to forward packets to ip-address.

Values	ipv4-prefix	a.b.c.d
	ipv6-prefix	x:x:x:x:x:x:x:x x:x:x:x:x:x:d.d.d.d x: [0 — FFFF]H d: [0 — 255]D

auto-bind

Syntax **auto-bind** {**ldp | gre | rsvp-te | mpls**}
no auto-bind

Context config>service>vprn

Description This command specifies the automatic binding type for the SDP assigned to this service.

Default None — The auto-bind type must be explicitly specified.

Parameters **ldp —** Specifies LDP to be the automatic binding for the SDP assigned to the service.

gre — Specifies GRE to be the automatic binding for the SDP assigned to the service.

rsvp-te — Specifies RSVP-TE to be the automatic binding for the SDP assigned to the service

mpls — Specifies that both LDP and RSVP-TE can be used to resolve the BGP nexthop for VPRN routes in an associated VPRN instance.

autonomous-system

Syntax **autonomous-system** *as-number*
no autonomous-system

Context config>service>vprn

Description This command defines the autonomous system (AS) to be used by this VPN routing/forwarding (VRF). This command defines the autonomous system to be used by this VPN routing

The **no** form of the command removes the defined AS from this VPRN context.

Default no autonomous-system

Parameters *as-number* — Specifies the AS number for the VPRN service.

Values 1 — 4294967295

backup-path

Syntax **backup-path [ipv4] [ipv6]**
no backup-path [ipv4] [ipv6]

Context config>router
config>service>vprn

Description This command enables the computation and use of a backup path for IPv4 and/or IPv6 BGP-learned prefixes belonging to the base router or a particular VPRN. Multiple paths must be received for a prefix in order to take advantage of this feature. When a prefix has a backup path and its primary path(s) fail the affected traffic is rapidly diverted to the backup path without waiting for control plane re-convergence to occur. When many prefixes share the same primary path(s), and in some cases also the same backup path, the time to failover traffic to the backup path is independent of the number of prefixes. In some cases prefix independent convergence may require use of FP2 or later IOMs/IMMs/XMAs.

By default, IPv4 and IPv6 prefixes do not have a backup path installed in the IOM.

Default no backup-path

Parameters **ipv4** — Enables the use of a backup path for BGP-learned IPv4 prefixes

ipv6 — Enables the use of a backup path for BGP-learned IPv6 prefixes

carrier-carrier-vpn

Syntax [**no**] **carrier-carrier-vpn**

Context config>service>vprn

Description This command configures a VPRN service to support a Carrier Supporting Carrier model. It should be configured on a network provider's CSC-PE device.

This command cannot be applied to a VPRN unless it has no SAP or spoke-SDP interfaces. Once this command has been entered one or more MPLS-capable CSC interfaces can be created in the VPRN.

The **no** form of the command removes the Carrier Supporting Carrier capability from a VPRN.

Default no carrier-carrier-vpn

confederation

Syntax **confederation** *confed-as-num* **members** *as-number* [*as-number…*(up to 15 max)]
no confederation *confed-as-num* **members** *as-number* [*as-number…*(up to 15 max)]
no confederation

Context config>service>vprn

Description This command configures the VPRN BGP instance to participate in a BGP confederation. BGP confederations can be used to reduce the number of IBGP sessions required within an AS.

When a VPRN BGP instance is part of a confederation, it can form confederation-EBGP sessions with CE router peers in a different sub-autonomous systems of the same confederation as well as regular EBGP sessions with CE router peers outside the confederation. A VPRN BGP instance that is part of a confederation cannot import or export its routes to the base router instance (as VPN-IP routes).

The **no** form of the command deletes the specified member AS from the confederation. When members are not specified in the no statement, the entire list is removed and confederations is disabled. When the last member of the list is removed, confederations is disabled.

Default No confederations are defined.

Parameters *confed-as-num* — The confederation AS number defined as a decimal value.

Values 1 — 4294967295

members *as-number* **—** The AS number(s) that are members of the confederation, each expressed as a decimal integer. Configure up to 15 members per confed-as-num.

Values 1 — 4294967295

dns

Syntax [**no**] **dns**

Context config>service>vprn

Description This command enables the context to configure domain name servers.

The **no** form of the command disables DNS for this service.

ipv4-source-address

Syntax **ipv4-source-address** *ipv4-address*
no ipv4-source-address

Context config>service>vprn>dns

Description This command configures the IPv4 address of the default secondary DNS server for the subscribers using this interface. Subscribers that cannot obtain an IPv4 DNS server address by other means, can use this for DNS name resolution.

The ipv4-address value can only be set to a nonzero value if the value of VPRN type is set to **subscriber-split-horizon**.

The **no** form of the command reverts to the default.

Default none

Parameters *ipv4-address* — Specifies the IPv4 address of the default secondary DNS server.

Values ipv4-address - a.b.c.d

ipv6-source-address

Syntax **ipv6-source-address** *ipv6-address*
no ipv6-source-address

Context config>service>vprn>dns

Description This command configures the IPv6 address of the default secondary DNS server for the subscribers using this interface. Subscribers that cannot obtain an IPv6 DNS server address by other means, can use this for DNS name resolution.

The ipv6-address value can only be set to a nonzero value if the value of VPRN type is set to **subscriber-split-horizon**.

The **no** form of the command reverts to the default.

Default none

Parameters *ipv4-address* — Specifies the IPv6 address of the default secondary DNS server.

Values ipv4-address - a.b.c.d

primary-dns

Syntax **primary-dns** *ip-address*
no primary-dns

Context config>service>vprn>dns

Description This command configures the primary DNS server used for DNS name resolution. DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the primary DNS server from the configuration.

Default **no primary-dns** — No primary DNS server is configured.

Parameters *ip-address* — The IP or IPv6 address of the primary DNS server.

Values ipv4-address - a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x[-interface]
x:x:x:x:x:x:d.d.d.d[-interface]
x: [0..FFFF]H
d: [0..255]D
interface - 32 chars max, for link local addresses.

secondary-dns

Syntax **secondary-dns** *ip-address*
no secondary-dns

Context config>service>vprn>dns

Description This command configures the secondary DNS server for DNS name resolution. The secondary DNS server is used only if the primary DNS server does not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the secondary DNS server from the configuration.

Default **no secondary-dns** — No secondary DNS server is configured.

Parameters *ip-address* — The IP or IPv6 address of the secondary DNS server.

Values ipv4-address - a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x[-interface]
x:x:x:x:x:x:d.d.d.d[-interface]
x: [0..FFFF]H
d: [0..255]D
interface - 32 chars max, for link local addresses

tertiary-dns

Syntax **tertiary-dns** *ip-address*
no tertiary-dns

Context config>service>vprn>dns

Description This command configures the tertiary DNS server for DNS name resolution. The tertiary DNS server is used only if the primary DNS server and the secondary DNS server do not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the tertiary DNS server from the configuration.

Default **no tertiary-dns** — No tertiary DNS server is configured.

Parameters *ip-address* — The IP or IPv6 address of the tertiary DNS server.

Values ipv4-address - a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x[-interface]
x:x:x:x:x:x:d.d.d.d[-interface]
x: [0..FFFF]H
d: [0..255]D
interface - 32 chars max, for link local addresses

ecmp

Syntax **ecmp** *max-ecmp-routes*
no ecmp

Context config>service>vprn

Description This command enables equal-cost multipath (ECMP) and configures the number of routes for path sharing. For example, the value of 2 means that 2 equal cost routes will be used for cost sharing.

ECMP groups form when the system routes to the same destination with equal cost values. Routing table entries can be entered manually (as static routes), or they can be formed when neighbors are discovered and routing table informationis exchanged by routing protocols. The system can balance traffic across the groups with equal costs.

ECMP can only be used for routes learned with the same preference and same protocol. See the discussion on preferences in the **static-route** command.

When more ECMP routes are available at the best preference than configured by the max-ecmp-routes parameter, then the lowest next-hop IP address algorithm is used to select the number of routes configured.

The **no** form of the command disables ECMP path sharing. If ECMP is disabled and multiple routes are available at the best preference and equal cost, the newly updated route is used.

Default no ecmp

Parameters *max-ecmp-routes* — Specifies the maximum number of routes for path sharing.

Values 0— 32

enable-bgp-vpn-backup

Syntax **enable-bgp-vpn-backup** [**ipv4**] [**ipv6**]
no enable-bgp-vpn-backup

Context config>service>vprn>bgp

Description This command allows BGP-VPN routes imported into the VPRN to be used as backup paths for IPv4 and/or IPv6 BGP-learned prefixes.

Parameters **ipv4 —** Allows BGP-VPN routes to be used as backup paths for IPv4 prefixes.

ipv6 — Allows BGP-VPN routes to be used as backup paths for IPv6 prefixes.

fib-priority

Syntax **fib-priority** {**high** | **standard**}

Context config>service>vprn

Description This command specifies the FIB priority for VPRN.

Parameters **high —**

standard —

grt-lookup

Syntax **grt-lookup**

Context config>service>vprn

Description This command provides the context under which all Global Route Table (GRT) leaking commands are configured. If all the supporting commands in the context are removed, this command will also be removed.

enable-grt

Syntax [**no**] **enable-grt**

Context config>service>vprn>grt-lookup

Description This command enables the functions required for looking up routes in the Global Route Table (GRT) when the lookup in the local VRF fails. If this command is enabled without the use of a static-route option (as subcommand to this parent), a lookup in the local VRF is preferred over the GRT. When the local VRF returns no route table lookup matches, the result from the GRT is preferred.

The no form of this command disables the lookup in the GRT when the lookup in the local VRF fails.

Default no enable-grt

export-grt

Syntax **export-grt** *policy-name* [*policy-name* ...(up to 5 max)]
no export-grt

Context config>service>vprn>grt-lookup

Description This command uses route policy to determine which routes are exported from the VRF to the GRT along with all the forwarding information. These entries will be marked as BGP-VPN routes in the GRT. Routes must be in the GRT in order for proper routing to occur from the GRT to the VRF.

Default no export-grt

export-limit

Syntax **export-limit** *num-routes*
no export-limit

Context config>service>vprn>grt-lookup
config>service>vprn>ospf
config>service>vprn>ospf3
config>service>vprn>rip

Description This command provides the ability to limit the total number of routes exported from the VRF to the GRT. The value zero (0) provides an override that disables the maximum limit. Setting this value to zero (0) will not limit the number of routes exported from the VRF to the GRT. Configuring a range of one (1) to 1000 will limit the number of routes to the specified value.

The **no** form of the command sets the export-limit to a default of five (5).

Default export-limit 5

Parameters *num-routes* — Specifies maximum number of routes that can be exported.

Values 0 — 1000

export-v6-limit

Syntax **export-v6-limit** *num-routes*
no export-v6-limit

Context config>service>vprn>grt-lookup

Description The export-limit range provides the ability to limit the total number of IPv6 routes exported from the VPRN to the GRT. The value “0” provides an override that disables the maximum limit. Setting this value to “0” will not limit the the number of routes exported from the VPRN to the GRT. Configuring a range of 1-1000 will limit the number of routes to the specified value.

The **no** form of the command sets the export-limit to a default of 5.

Default export-v6-limit 5

Parameters *num-routes* — Specifies maximum number of routes that can be exported.

Values 0 — 1000

allow-local-management

Syntax [**no**] **allow-local-management**

Context config>service>vprn>grt-lookup>enable-grt

Description When enabled, both IPv4 and IPv6 base interfaces shall respond to leaked traffic from the VPRN.

static-route

Syntax **static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**enable|disable**] **grt**
no static-route

Context config>service>vprn>grt-lookup>enable-grt

Description This command is a simplified version of the traditional static-route command pointing to the base routing instance. This instructs the route lookup function to look only in the GRT for a route matching destination static route and not look up the route in the local VPRN. The GRT keyword is a required parameter.

The no form casues the feature into the default mode of primary lookup for all routes in the local VPRN and failing a match in the local VPRN, the lookup result in the GRT will be used.

Parameters *ip-prefix/prefix-length* — Specifies the IPv4 prefix and prefix length.

Values ip-prefix: a.b.c.d (host bits must be 0)

ipv4-prefix-length: [0..32]

ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 — FFFF]H
d: [0 — 255]D
ipv6-prefix-length 0 — 128

netmask — Specifies the netmask.

Values a.b.c.d (network bits all 1 and host bits all 0)

preference — Specifies the preference.

Values 1..255

metric — Specifies the metric.

Values 0..65535

enable|disable — Keyword; specifies the state of the static-route.

grt — Keyword; Global Route Table lookup.

gsmp

Syntax **gsmp**

Context config>service>vprn

Description This command enables the context to configure GSMP connections maintained in this service.

Default not enabled

group

Syntax **[no] group *name***

Context config>service>vprn>gsmp

Description This command specifies a GSMP name. A GSMP group name is unique only within the scope of the service in which it is defined.

Parameters *name* — Specifies the group name up to 32 characters in length.

ancp

Syntax **ancp**

Context config>service>vprn>gsmp>group

Description This command configures ANCP parameters for this GSMP group.

dynamic-topology-discover

Syntax [**no**] **dynamic-topology-discover**

Context config>service>vprn>gsmp>group>ancp

Description This command enables the ANCP dynamic topology discovery capability.

The **no** form of this command disables the feature.

oam

Syntax [**no**] **oam**

Context config>service>vprn>gsmp>group>ancp

Description This command specifies whether or not the GSMP ANCP OAM capability should be negotiated at startup of the GSMP connection.

The **no** form of this command disables the feature.

hold-multiplier

Syntax **hold-multiplier** *multiplier*
no hold-multiplier

Context config>service>vprn>gsmp>group

Description This command configures the hold-multiplier for the GSMP connections in this group.

Parameters *multiplier* — Specifies the GSMP hold multiplier value.

Values 1 — 100

idle-filter

Syntax **idle-filter**
no idle-filter

Context config>service>vpls>gsmp
config>service>vprn>gsmp

Description This command when applied will filter out new subscriber's ANCP messages from subscriber with "DSL-line-state" IDLE

Default no idle-filter

keepalive

Syntax **keepalive** *seconds*
no keepalive

Context config>service>vprn>gsmp>group

Description This command configures keepalive values for the GSMP connections in this group.

Parameters *seconds* — Specifies the GSMP keepalive timer value in seconds.

Values 1 — 25

neighbor

Syntax [**no**] **neighbor** *ip-address*

Context config>service>vprn>gsmp>group

Description This command adds or removes a neighbor in this group.

Parameters *ip-address* — Specifies the IP address in dotted decimal notation.

local-address

Syntax **local-address** *ip-address*
no local-address

Context config>service>vprn>gsmp>group>neighbor

Description This command configures the source ip-address used in the connection towards the neighbor.

Parameters *ip-address* — Specifies the IP address in dotted decimal notation.

priority-marking

Syntax **priority-marking dscp** *dscp-name*
priority-marking prec *ip-prec-value*
no priority-marking

Context config>service>vprn>gsmp>group>neighbor

Description This command configures the type of priority marking to be used.

Parameters **dscp** *dscp-name* — Specifies the DSCP code-point to be used.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

prec *ip-prec-value* — Specifies the precedence value to be used.

Values 0 — 7

persistency-database

Syntax **persistency-database**
no persistency-database

Context config>service>vpls <service id>gsmp
config>service>vprn<service id>gsmp

Description This command enables the system to store DSL line information in memory. If the GSMP connection terminates, the DSL line information will remain in memory and accessible for Radius authentication and accounting.

Default no persistency-database

IGMP Commands

igmp

Syntax [**no**] **igmp**

Context config>service>vprn

Description This command enables the context to configure IGMP parameters.

The **no** form of the command disables IGMP.

Default disabled

group-interface

Syntax [**no**] **group-interface** *ip-int-name*
[**no**] **group-interface fwd-service** *service-id ip-int-name*

Context config>service>vprn>igmp

Description This command configures IGMP group interfaces.

The **no** form of the command reverts to the default.

Default none

Parameters *ip-int-name* — Specifies the name of the IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

fwd-service *service-id* — Specifies the service ID. This is only configured in the retailer VRF. This construct references the wholesaler service under which the group-interface (and the subscriber) is actually defined.

Values 1 — 2147483650, svc-name up to 64 char maximum

Default none

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context config>service>vprn>igmp>gr-if
config>service>vprn>igmp>if

Description This command enables the IGMP router alert check option.

The **no** form of the command disables the router alert check.

import

Syntax **import** *policy-name*
no import

Context config>service>vprn>igmp>gr-if
config>service>vprn>igmp>if

Description This command specifies the policy that is to be applied on this interface.

Parameters *policy-name* — Specify the policy to filter IGMP packets.

max-groups

Syntax **max-groups** *value*
no max-groups

Context config>service>vprn>igmp>gr-if
config>service>vprn>igmp>if

Description This command configures the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

The **no** form of the command removes the value.

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 — 16000

max-sources

Syntax **max-sources** [1..1000]
no max-sources

Context config>service>vprn>igmp>gr-if
config>service>vprn>igmp>if

Description This command specifies the maximum number of sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of sources, the sources that are already accepted are not deleted. Only new sources will not be allowed.

Parameters *sources* — Specifies the maximum number of sources for this interface.

Values 1 — 1000

max-grp-sources

Syntax **max-grp-sources** [1..32000]
no max-grp-sources

Context config>service>vprn>igmp>gr-if
config>service>vprn>igmp>if

Description This command configures the maximum number of group sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources will not be allowed.

The no form of the command reverts to the default.

Default 0

Parameters **1 — 32000 —** Specifies the maximum number of group source.

Values 1 — 32000

mcac

Syntax **mcac**

Context config>service>vprn>igmp>gr-if

Description This command enables the context to configure multicast CAC parameters.

mc-constraints

Syntax **mc-constraints**

Context config>service>vprn>igmp>gr-if

Description This command configures multicast CAC constraints.

policy

Syntax **policy** *policy-name*
no policy

Context config>service>vprn>igmp>gr-if

Description This command references the global channel bandwidth definition policy that is used for (H)mcac and HQoS Adjust.

HQoS Adjustment is supported only with redirection enabled. In other words, the policy from the redirected interface is used for HQoS Adjustment.

Hierarchical mcac (Hmcac) is supported only with redirection enabled. In Hmcac, the subscriber is checked first against its bandwidth limits followed by the check on the redirected interface against the bandwidth limits defined under the redirected interface. In the Hmcac case the channel definition policy must be referenced under the redirected interface level.

Parameters *policy-name* — Specifies the name of the global mcac channel definition policy defined under the hierarchy **configure>router>mcac>policy**.

Default No policy is referenced.

unconstrained-bw

Syntax **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
no unconstrained-bw

Context config>service>vprn>igmp>gr-if

Description This command configures unconstrained-bw for multicast cac policy on this interface.

The **no** form of the command

Parameters *bandwidth* — Specifies the bandwidth assigned for interface's multicast cac policy traffic in kilo-bits per second (kbps).

mandatory-bw *mandatory-bw* **—**

query-src-ip

Syntax **query-src-ip** *ip-address*
no query-src-ip

Context config>service>vprn>igmp>gr-if

Description This command configures the query source IP address for the group interface. This IP address overrides the source IP address configured at the router level.

The **no** form of the command removes the IP address.

Default none

Parameters *ip-address* — Sets the source IPv4 address for all subscriber’s IGMP queries.

sub-hosts-only

Syntax [**no**] **sub-hosts-only**

Context config>service>vprn>igmp>gr-if

Description This command enables the IGMP traffic from known hosts only.

The **no** form of the command disable the IGMP traffic from known hosts only

subnet-check

Syntax [**no**] **subnet-check**

Context config>service>vprn>igmp>gr-if

Description This command enables local subnet checking for IGMP.

The **no** form of the command disables local subnet checking for IGMP.

version

Syntax **version** *version*
no version

Context config>service>vprn>igmp>gr-if

Description This command configures the version of IGMP.

The **no** form of the command

Parameters *version* — Specifies the IGMP version.

Values 1, 2 or 3

grp-if-query-src-ip

Syntax **grp-if-query-src-ip** *ip-address*
no grp-if-query-src-ip

Context config>service>vprn>igmp

Description This command configures the query source IP address for all group interfaces.

The **no** form of the command removes the IP address.

Default none

interface

Syntax **interface** *ip-int-name*
no interface

Context config>service>vprn>igmp

Description This command enables the context to configure IGMP interface parameters.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 1 — 32 characters maximum

import

Syntax **import** *policy-name*
no import

Context config>service>vprn>igmp>if

Description This command imports a policy to filter IGMP packets. The **no** form of the command removes the policy association from the IGMP instance.

Default **no import** — No import policy specified.

Parameters *policy-name* — The import route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

max-groups

Syntax **max-groups** *value*
no max-groups

Context config>service>vprn>igmp>if

Description This command specifies the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

Default 0, no limit to the number of groups.

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 — 16000

mcac

Syntax **mcac**

Context config>service>vprn>if
config>service>vprn>pim>if

Description This command configures multicast CAC policy and constraints for this interface.

Default none

mc-constraints

Syntax **mc-constraints**

Context config>service>vprn>igmp>if>mcac
config>service>vprn>pim>if>mcac

Description This command enables the context to configure multicast CAC constraints.

Default none

level

Syntax **level** *level-id* **bw** *bandwidth*
no level *level-id*

Context config>service>vprn>igmp>if>mcac
config>service>vprn>pim>if>mcac

Description This command configures interface levels and associated bandwidth for multicast CAC policy.

Parameters *level-id* — Specifies an entry for the multicast CAC policy constraint level configured on this system.

Values 1 — 8

bandwidth — Specifies the bandwidth in kilobits per second (kbps) for the level.

Values 1 — 2147483647

number-down

Syntax **number-down** *number-lag-port-down*
no number-down

Context config>service>vprn>igmp>if>mcac>mc-constraints
config>service>vprn>pim>if>mcac>mc-constraints

Description This command configures the number of ports down and level for interface's multicast CAC policy.

Default not enabled

policy

Syntax **policy** *policy-name*
no policy

Context config>service>vprn>igmp>if>mcac
config>service>vprn>pim>if>mcac

Description This command configures the mulitcast CAC policy name.

Parameters *policy-name* — The multicast CAC policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

unconstrained-bw

Syntax **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
no unconstrained-bw

Context config>service>vprn>igmp>if>mcac
config>service>vprn>pim>if>mcac

Description This command configures the bandwidth for the interface's multicast CAC policy traffic. When disabled (**no unconstrained-bw**) there will be no checking of bandwidth constraints on the interface level. When enabled and a policy is defined, enforcement is performed. The allocated bandwidth for optional channels should not exceed the **unconstrained-bw** minus the **mandatory-bw** and the mandatory channels have to stay below the specified value for the **mandatory-bw**. After this interface check, the bundle checks are performed.

Parameters *bandwidth* — The bandwidth assigned for interface's MCAC policy traffic, in kilo-bits per second (kbps).

Values 0 — 2147483647

mandatory-bw *mandatory-bw* — Specifies the bandwidth pre-reserved for all the mandatory channels on a given interface in kilo-bits per second (kbps).

If the *bandwidth* value is 0, no mandatory channels are allowed. If *bandwith* is not configured, then all mandatory and optional channels are allowed.

If the value of *mandatory-bw* is equal to the value of *bandwidth*, then all the unconstrained bandwidth on a given interface is allocated to mandatory channels configured through multicast CAC policy on that interface and no optional groups (channels) are allowed.

The value of *mandatory-bw* should always be less than or equal to that of *bandwidth*, An attempt to set the value of *mandatory-bw* greater than that of *bandwidth*, will result in inconsistent value error.

Values 0 — 2147483647

static

Syntax **static**

Context config>service>vprn>igmp>if

Description This command tests forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Default none

group

Syntax [**no**] **group** *grp-ip-address*

Context config>service>vprn>igmp>if>static

Description This command adds a static multicast group either as a (*,G) or one or more (S,G) records. Use IGMP static group memberships to test multicast forwarding without a receiver host. When IGMP static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static IGMP group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static IGMP group entries do not generate join messages toward the RP.

Default none

Parameters *grp-ip-address* — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group. The address must be in dotted decimal notation

source

Syntax **source**

Context config>service>vprn>igmp>if>static>group

Description This command specifies a IPv4 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group is to receive multicast traffic from, and from the source(s) that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The source command in combination with the group is used to create a specific (S,G) static group entry.

Use the **no** form of the command to remove the source from the configuration.

Default none

Parameters *ip-address* — Specifies the IPv4 unicast address.

starg

Syntax **starg**

Context config>service>vprn>igmp>if>static>group

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the **no** form of the command to remove the starg entry from the configuration.

Default none

subnet-check

Syntax [**no**] **subnet-check**

Context config>service>vprn>igmp>if

Description This command enables subnet checking for IGMP messages received on this interface. All IGMP packets with a source address that is not in the local subnet are dropped.

Default enabled

version

Syntax **version** *version*
no version

Context config>service>vprn>igmp>if

Description This command specifies the IGMP version. If routers run different versions of IGMP, they will negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version. For IGMP to function correctly, all routers on a LAN should be configured to run the same version of IGMP on that LAN.

For IGMPv3, note that a multicast router that is also a group member performs both parts of IGMPv3, receiving and responding to its own IGMP message transmissions as well as those of its neighbors.

Default 3

Parameters *version* — Specifies the IGMP version number.

Values 1, 2, 3

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context config>service>vprn>igmp

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default 125

Parameters *seconds* — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 — 1024

query-last-member-interval

Syntax **query-last-member-interval** *seconds*

Context config>service>vprn>igmp

Description This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default 1

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 — 1024

query-response-interval

Syntax **query-response-interval** *seconds*

Context config>service>vprn>igmp

Description This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default 10

Parameters *seconds* — Specifies the the length of time to wait to receive a response to the host-query message from the host.

Values 1 — 1023

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context config>service>vprn>igmp

Description This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default 2

Parameters *robust-count* — Specifies the robust count value.

Values 2 — 10

ssm-translate

Syntax **igmp**

Context config>service>vprn>igmp

config>service>vprn>igmp>if

Description This command enables the context to configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the **source** command with **starg** command enabled.

grp-range

Syntax [**no**] **grp-range** *start end*

Context config>service>vprn>igmp>ssm-translate

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters *start* — An IP address that specifies the start of the group range.

end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the *start* value.

source

Syntax [**no**] **source** *ip-address*

Context config>service>vprn>igmp>ssm-translate>grp-range

Description This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters *ip-address* — Specifies the IP address that will be sending data.

igmp-host-tracking

Syntax **igmp-host-tracking**

Context config>service>vprn
config>service>vprn>sap

Description This command enables the context to configure IGMP host tracking parameters.

expiry-time

Syntax **expiry-time** *expiry-time*
no expiry-time

Context config>service>vprn>igmp-trk
config>service>vprn>sap>igmp-trk

Description This command configures the time that the system continues to track inactive hosts.

The **no** form of the command removes the values from the configuration.

Default no expiry-time

Parameters *expiry-time* — Specifies the time, in seconds, that this system continues to track an inactive host.

Values 1 — 65535

import

Syntax **import** *policy-name*
no import

Context config>service>vprn>sap>igmp-trk

Description This command associates an import policy to filter IGMP packets.

The **no** form of the command removes the values from the configuration.

Default n o import

Parameters *policy-name* — Specifies the import policy name.

max-num-groups

Syntax **max-num-groups** *max-num-groups*
no max-num-groups

Context config>service>vprn>sap>igmp-trk

Description This command configures the maximum number of multicast groups allowed to be tracked.

The **no** form of the command removes the values from the configuration.

Default no max-num-groups

Parameters *max-num-groups* — Specifies the maximum number of multicast groups allowed to be tracked.

Values 1 — 196607

max-num-sources

Syntax **max-num-sources** *max-num-sources*
no max-num-sources

Context config>service>vprn>sub-if>grp-if

Description This command specifies the maximum number of multicast sources allowed to be tracked per group.

The **no** form of the command reverts to the default.

Default no max-num-sources

Parameters *max-num-sources* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 — 1000

label-mode

Syntax **label-mode** {**vrf** | **next-hop**}
no label-mode

Context config>service>vprn

Description This command controls the method by which service labels are allocated to routes exported by the VPRN as BGP-VPN routes. The **vrf** option selects service label per VRF mode while the **next-hop** option selects service label per next-hop mode.

The **no** form of the command sets the mode to the default mode of service label per VRF.

Default no label-mode

Parameters **vrf —** Selects service label per VRF mode.

next-hop — Selects service label per next-hop mode.

maximum-ipv6-routes

Syntax **maximum-ipv6-routes** *number* [**log-only**] [**threshold** *percentage*]
no maximum-ipv6-routes

Context config>service>vprn

Description This command specifies the maximum number of remote IPv6 routes that can be held within a VPN routing/ forwarding (VRF) context. Note that **local**, **host**, **static** and **aggregate** routes are not counted.

Note that the VPRN service ID must be in a shutdown state in order to modify maximum-routes command parameters.

If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then the offending RIP peer (if applicable) is brought down (but the VPRN instance remains up). BGP peering will remain up but the exceeding BGP routes will not be added to the VRF.

The maximum route threshold can dynamically change to increase the number of supported routes even when the maximum has already been reached. Protocols will resubmit their routes which were initially rejected.

The **no** form of the command disables any limit on the number of routes within a VRF context. Issue the **no** form of the command only when the VPRN instance is shutdown.

Default 0 or disabled — The threshold will not be raised.

Parameters *number* — An integer that specifies the maximum number of routes to be held in a VRF context.

Values 1 — 2147483647

log-only — This parameter specifies that if the maximum limit is reached, only log the event. **log-only** does not disable the learning of new routes.

threshold *percentage* — The percentage at which a warning log message and SNMP trap should be set. There are two warnings, the first is a mid-level warning at the threshold value set and the second is a high-level warning at level between the maximum number of routes and the mid-level rate ([mid+max] / 2).

Values 0 — 100

maximum-routes

Syntax **maximum-routes** *number* [**log-only**] [**threshold** *percentage*]
no maximum-routes

Context config>service>vprn

Description This command specifies the maximum number of remote routes that can be held within a VPN routing/ forwarding (VRF) context. Note that **local**, **host**, **static** and **aggregate** routes are not counted.

Note that the VPRN service ID must be in a shutdown state in order to modify maximum-routes command parameters.

If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then the offending RIP peer (if applicable) is brought down (but the VPRN instance remains up). BGP peering will remain up but the exceeding BGP routes will not be added to the VRF.

The maximum route threshold can dynamically change to increase the number of supported routes even when the maximum has already been reached. Protocols will resubmit their routes which were initially rejected.

The **no** form of the command disables any limit on the number of routes within a VRF context. Issue the **no** form of the command only when the VPRN instance is shutdown.

Default 0 or disabled — The threshold will not be raised.

Parameters *number* — An integer that specifies the maximum number of routes to be held in a VRF context.

Values 1 — 2147483647

log-only — This parameter specifies that if the maximum limit is reached, only log the event. **log-only** does not disable the learning of new routes.

threshold *percentage* — The percentage at which a warning log message and SNMP trap should be set. There are two warnings, the first is a mid-level warning at the threshold value set and the second is a high-level warning at level between the maximum number of routes and the mid-level rate ([mid+max] / 2).

Values 0 — 100

multicast-info-policy

Syntax **multicast-info-policy** *policy-name*
no multicast-info-policy

Context config>service>vprn

Description This command configures multicast information policy.

Parameters *policy-name* — Specifies the policy n ame.

Values 32 chars max

mc-maximum-routes

Syntax **mc-maximum-routes** *number* [**log-only**] [**threshold** *threshold*]

Context config>service>vprn

Description This command specifies the maximum number of multicast routes that can be held within a VPN routing/forwarding (VRF) context. When this limit is reached, a log and SNMP trap are sent. If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then no new joins will be processed.

The **no** form of the command disables the limit of multicast routes within a VRF context. Issue the **no** form of the command only when the VPRN instance is shutdown.

Default no mc-maximum-routes

Parameters *number* — Specifies the maximum number of routes to be held in a VRF context.

Values 1 — 2147483647

log-only — Specifies that if the maximum limit is reached, only log the event. **log-only** does not disable the learning of new routes.

threshold *threshold* **—** The percentage at which a warning log message and SNMP trap should be sent.

Values 0 — 100

Default 10

ptp

Syntax [**no**] **ptp**

Context config>service>vprn

Description This command enables the context to configure PTP parameters for the VPRN service.

peer

peer

Syntax **peer** *ip-address*

Context config>system>ptp
configure>service>vprn>ptp

Description This command configures a remote PTP peer. It provides the context to configure parameters for the remote PTP peer.

Up to 20 remote PTP peers may be configured.

The **no** form of the command deletes the specified peer.

If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last peer cannot be deleted. This prevents the user from having PTP enabled without any peer configured and enabled.

Peers are created within the routing instance associated with the context of this command. All configured PTP peers must use the same routing instance.

Default none

Parameters *ip-address* — The IP address of the remote peer.

Values ipv4-address a.b.c.d

Parameters *ip-address* — The IP address of the remote peer.

Values ipv4-address a.b.c.d

peer-limit

Syntax **peer-limit** *limit*
no peer-limit

Context configure>system>ptp
configure>service>vprn>ptp

Description This command specifies an upper limit to the number of discovered peers permitted within the routing instance. This can be used to ensure that a routing instance does not consume all the possible discovered peers and blocking discovered peers in other routing instances.

If it is desired to reserve a fixed number of discovered peers per router instance, then all router instances supporting PTP should have values specified with this command and the sum of all the peer-limit values must not exceed the maximum number of discovered peers supported by the system.

If the user attempts to specify a peer-limit, and there are already more discovered peers in the routing instance than the new limit being specified, the configuration will not be accepted.

Default no limit

Parameters *limit* — Specifies the maximum number of discovered peers allowed in the routing instance.

Values 0 — 50

Default 1 (The maximum number of discovered peers supported by the system.)

reassembly-group

Syntax **reassembly-group** *nat-group-id*
no reassembly-group

Context configure>router
config>service>vprn

Description This command associate reassembly-group consisting of multiple ISAs with the

routing context in which the application requiring reassembly service resides.

Default no route-distinguisher

Parameters *nat-group-id* — Nat-group id. The nat-group contains up to 10 active ISAs.

asn:number — The ASN is a 2-byte value less than or equal to 65535. The assigned number can be any 32-bit unsigned integer value.

route-distinguisher

Syntax **route-distinguisher** [*ip-address*:*number* | *asn*:*number*]
no route-distinguisher

Context config>service>vprn

Description This command sets the identifier attached to routes the VPN belongs to. Each routing instance must have a unique (within the carrier's domain) route distinguisher associated with it. A route distinguisher must be defined for a VPRN to be operationally active.

Default no route-distinguisher

Parameters The route distinguisher is a 6-byte value that can be specified in one of the following formats:

ip-address:number — Specifies the IP address in dotted decimal notation. The assigned number must not be greater than 65535.

asn:number — The ASN is a 2-byte value less than or equal to 65535. The assigned number can be any 32-bit unsigned integer value.

router-id

Syntax **router-id** *ip-address*
no router-id

Context config>service>vprn
config>service>vprn>ospf
config>service>vprn>bgp

Description This command sets the router ID for a specific VPRN context.

If neither the router ID nor system interface are defined, the router ID from the base router context is inherited.

The **no** form of the command removes the router ID definition from the given VPRN context.

Default no router-id

Parameters *ip-address* — The IP address must be given in dotted decimal notation.

service-name

Syntax **service-name** *service-name*
no service-name

Context config>service>vprn

Description This command configures an optional service name, up to 64 characters in length, which adds a name identifier to a given service to then use that service name in configuration references as well as display and use service names in show commands throughout the system. This helps the service provider/administrator to identify and manage services within the 7750 SR, 7450 ESS and 7710 SR platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

Parameters *service-name* — Specifies a unique service name to identify the service. Service names may not begin with an integer (0-9).

sgt-qos

Syntax **sgt-qos**

Context config>service>vprn

Description This command enables the context to configure DSCP/Dot1p re-marking for self-generated traffic.

application

Syntax **application** *dscp-app-name* **dscp** {*dscp-value* | *dscp-name*}
application *dot1p-app-name* **dot1p** *dot1p-priority*
no application {*dscp-app-name* | *dot1p-app-name*}

Context config>service>vprn>sgt-qos

Description This command configures DSCP/Dot1p re-marking for self-generated traffic. When an application is configured using this command, then the specified DSCP name/value is used for all packets generated by this application within the router instance it is configured.

Using the value configured in this command:

- Sets the DSCP bits in the IP packet.
- Maps to the FC. This value will be signaled from the CPM to the egress forwarding complex.

- Based on this signaled FC the egress forwarding complex QoS policy sets the IEEE802.1 dot1P and LSP EXP bits.
- The Dot1P and the LSP EXP bits are set by the egress complex for all packets based on the signaled FC. This includes ARP and IS-IS packets that, due to their nature, do not carry DSCP bits.
- The DSCP value in the egress IP header will be as configured in this command. The egress QoS policy will not overwrite this value.

Only one DSCP name/value can be configured per application, if multiple entries are configured then the subsequent entry overrides the previous configured entry.

The **no** form of this command reverts back to the default value.

Parameters *dscp-app-name* — Specifies the DSCP application name.

Values ldp, rsvp, bgp, rip, msdp, pim, ospf, igmp, mld, telnet, tftp, ftp, ssh, snmp, snmp-notification, syslog, icmp, traceroute, tacplus, dns, ntp, radius, cflowd, dhcp, bootp, ndis, vrrp, srrp

dscp-value — Specifies a value when this packet egresses the respective egress policy should provide the mapping for the DSCP value to either LSP-EXP bits or IEEE 802.1p (Dot1P) bits as appropriate otherwise the default mapping applies.

Values 0 — 63

dscp-name — Specifies the DSCP name.

Values none, be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dot1p-priority — Specifies the Dot1P priority.

Values 0 — 7

dot1p-app-name — Specifies the Dot1P application name.

Values arp, isis

dscp

Syntax **dscp** *dscp-name* **fc** *fc-name*
no dscp *dscp-name*

Context config>service>vprn>sgt-qos

Description This command creates a mapping between the DiffServ Code Point (DSCP) of the self generated traffic and the forwarding class.

Self generated traffic that matches the specified DSCP will be assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all sixty-four DiffServ code points to the forwarding class. For undefined code points, packets are assigned to the forwarding class specified under the default-action command.

All DSCP names that defines a DSCP value must be explicitly defined.

The **no** form of this command removes the DiffServ code point to forwarding class association. The default-action then applies to that code point value.

Default none

Parameters *dscp-name* — The name of the DiffServ code point to be associated with the forwarding class. DiffServ code point can only be specified by its name and only an existing DiffServ code point can be specified. The software provides names for the well known code points.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc *fc-name* **—** Specifies the forwarding class name. All packets with DSCP value or MPLS EXP bits that is not defined will be placed in this forwarding class.

Default None, the fc name must be specified

Values be, l2, af, l1, h2, ef, h1, nc

single-sfm-overload

Syntax **single-sfm-overload** [**holdoff-time** *holdoff-time*]
no single-sfm-overload

Context config>service>vprn

Description This command, if enabled, will cause the IGP protocols (either IS-IS or OSPF) for the service to enter an overload state when the node only has a single SFM functioning.

The **no** form of this command causes the overload state to be cleared.

Default no single-sfm-overload

Parameters *holdoff-time* — This parameter specifies the delay between the detection of a single SFM and enacting the overload state.

Values 1—600 seconds

Default 0 seconds

snmp-community

Syntax **snmp-community** *community-name* [**version** *SNMP-version*]
no snmp-community [*community-name*]

Context config>service>vprn

Description This command sets the SNMP community name to be used with the associated VPRN instance.

If an SNMP community name is not specified, then SNMP access is not allowed.

The **no** form of the command removes the SNMP community name from the given VPRN context.

Default None — The SNMP community must be explicitly specified.

Parameters *community-name* — Specifies one or more SNMP community names.

version *SNMP-version* — Specifies the SNMP version.

Values **v1**, **v2c**, **both**

source-address

Syntax **source-address**

Context config>service>vprn

Description This command enables the context to specify the source address and application that should be used in all unsolicited packets.

application

Syntax **application** *app* [*ip-int-name*|*ip-address*]
no application *app*

Context config>service>vprn>source-address

Description This command specifies the source address and application.

Parameters *app* — Specify the application name.

Values telnet, ssh, traceroute, ping

ip-int-name | *ip-address* — Specifies the name of the IP interface or IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

application6

Syntax **application6** *app ipv6-address*

Context config>service>vprn>source-address

Description This command specifies the IPv6 source address and application.

Parameters *app* — Specify the application name.

Values telnet, ssh, traceroute, ping

ipv6-address — Specifies the name of the IPv6 address.

static-route

Syntax [**no**] **static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**community** *comm-id*] [**enable** | **disable**] {**next-hop** *ip-int-name* | *ip-address* [**mcast-family**] | **ipsec-tunnel** *ipsec-tunnel-name*} [**bfd-enable** | {**cpe-check** *cpe-ip-address* [**interval** *seconds*] [**drop-count** *count*] [**log**]}]

[**no**] **static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**community** *comm-id*] [**enable** | **disable**] **indirect** *ip-address* [**cpe-check** *cpe-ip-address* [**interval** *seconds*][**drop-count** *count*] [**log**]]

[**no**] **static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**community** *comm-id*] [**enable** | **disable**] **black-hole** [**mcast-family**]

Context config>service>vprn

Description This command creates a static route. A static route can have a directly-connected interface as a next-hop (specified using the IP interface name or an IP address of the interface), or an indirect IP address as a next-hop or a black-hole next-hop (specifying a discard action).

The no form of the command deletes the static route entry. If a static route needs to be removed when multiple static routes exist to the same destination, then as many parameters to uniquely identify the static route must be entered.

If a CPE connectivity check target address is already being used as the target address in a different static route, then cpe-check parameters must match. If they do not, the new configuration command will be rejected.

If a static-route command is issued with no cpe-check target but the destination prefix/netmask and next-hop matches a static route that did have an associated cpe-check, the cpe-check test will be removed from the associated static route.

Default No static routes are defined**.**

Parameters *ip-prefix* — The destination address of the aggregate route in dotted decimal notation.

Values

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 — 32
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 — FFFF]H d: [0 — 255]D
ipv6-prefix-length	0 — 128

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

ip-int-name — The name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed with

ip-address — The IP address of the IP interface. The *ip-addr* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x[-interface]

x:x:x:x:x:x:d.d.d.d[-interface]
x: [0..FFFF]H
d: [0..255]D
interface: 32 characters maximum, mandatory for link local addresses

community *comm-id* **—** This configuration option associates a BGP community with the static route. The community can be matched in route policies and is automatically added to BGP routes exported from the static route.

Values	comm-id	asn:comm-val | well-known-comm
	asn	0 — 65535
	comm-val	0 — 65535
	well-known-comm	no-advertise, no-export, no-export-subconfed

enable — Static routes can be administratively enabled or disabled. Use the **enable** parameter to re-enable a disabled static route. In order to enable a static route, it must be uniquely identified by the IP address, mask, and any other parameter that is required to identify the exact static route.

The administrative state is maintained in the configuration file.

Default enable

disable — Static routes can be administratively enabled or disabled. Use the **disable** parameter to disable a static route while maintaining the static route in the configuration. In order to enable a static route, it must be uniquely identified by the IP address, mask, and any other parameter that is required to identify the exact static route.

The administrative state is maintained in the configuration file.

Default enable

interval *seconds* — This optional parameter specifies the interval between ICMP pings to the target IP address.

Values 1 —255 seconds

Default 1 seconds

drop-count *count* — This optional parameter specifies the number of consecutive ping-replies that must be missed to declare the CPE down and to de-active the associated static route.

Values Value range: 1 —255

Default 3

log — This optional parameter enables the ability to log transitions between active and in-active based on the CPE connectivity check. Events should be sent to the system log, syslog and SNMP traps.

next-hop [*ip-address* | *ip-int-name*] **—** Specifies the directly connected next hop IP address used to reach the destination. If the next hop is over an unnumbered interface, the *ip-int-name* of the unnumbered interface (on this node) can be configured.

The **next-hop** keyword and the **indirect** or **black-hole** keywords are mutually exclusive. If an identical command is entered (with the exception of either the **indirect** or **black-hole** parameters), then this static route will be replaced with the newly entered command, and unless specified, the respective defaults for preference and metric will be applied.

The *ip-addr* configured here can be either on the network side or the access side on this node. This address must be associated with a network directly connected to a network configured on this node.

ipsec-tunnel *ipsec-tunnel-name* **—** specifies an IPSec tunnel name up to 32 characters in length.

indirect *ip-address* **—** Specifies that the route is indirect and specifies the next hop IP address used to reach the destination.

The configured *ip-addr* is not directly connected to a network configured on this node. The destination can be reachable via multiple paths. The static route remains valid as long as the address configured as the indirect address remains a valid entry in the routing table. Indirect static routes cannot use an ip-prefix/mask to another indirect static route.

The **indirect** keyword and the **next-hop** or **black-hole** keywords are mutually exclusive. If an identical command is entered (with the exception of either the **next-hop** or **black-hole** parameters), then this static route will be replaced with the newly entered command and unless specified the respective defaults for preference and metric will be applied.

The *ip-addr* configured can be either on the network or the access side and is normally at least one hop away from this node.

black-hole — Specifies a black hole route meaning that if the destination address on a packet matches this static route it will be silently discarded.

The **black-hole** keyword is mutually exclusive with either the **next-hop** or **indirect** keywords. If an identical command is entered, with exception of either the **next-hop** or **indirect** parameters, then the static route is replaced with the new command, and unless specified, the respective defaults for **preference** and **metric** are applied.

preference *preference* — The preference of this static route (as opposed to the routes from different sources such as BGP or OSPF), expressed as a decimal integer. When modifying the **preference** value of an existing static route, unless specified, the metric will not change.

If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of which route to use is determined by the configuration of the ECMP command.

Default 5

Values 1 — 255

metric *metric* — The cost metric for the static route, expressed as a decimal integer. This value is used when importing this static route into other protocols such as OSPF. This value is also used to determine the static route to install in the forwarding table: When modifying the metrices of an existing static route, unless specified, the preference will not change.

If there are multiple static routes with the same preference but unequal metrices, the lower cost (metric) route is installed. If there are multiple static routes with equal preference and metrics then ECMP rules apply. If there are multiple routes with unequal preferences, then the lower preference route is installed.

Default 1

Values 0 — 65535

tag — Adds a 32-bit integer tag to the static route. The tag is used in route policies to control distribution of the route into other protocols.

Values 1..4294967295

bfd-enable — Associates the state of the static route to a BFD session between the local system and the configured nexthop. This keyword cannot be configured if the nexthop is **indirect** or a **blackhole** keywords are specified.

cpe-check *target-ip-address* **—** This parameter specifies the IP address of the target CPE device. ICMP pings will be sent to this target IP address. This parameter must be configured to enable the CPE connectivity feature for the associated static route. The target-ip-address cannot be in the same subnet as the static route subnet itself to avoid possible circular references. This option is mutually exclusive with BFD support on a given static route.

Default no cpe-check enabled

mcast-family — Enables submission of the IPv4 static route into IPv4 multicast RTM.

Values mcast-ipv4

type

Syntax **type** [**hub** |**subscriber-split-horizon**]
no type

Context config>service>vprn>

Description This command designates the type of VPRN instance being configured for hub and spoke topologies. Use the **no** form to reset to the default of a fully meshed VPRN.

Default no type

Parameters **hub —** Specifies a hub VPRN which allows all traffic from the hub SAPs to be routed to the destination directly, while all traffic from spoke VPRNs or network interfaces can only be routed to a hub SAP.

subscriber-split-horizon — Controls the flow of traffic for wholesale subscriber applications.

vrf-export

Syntax **vrf-export** *policy* [*policy...*]
no vrf-export

Context config>service>vprn

Description This command specifies the export policies to control routes exported from the local VPN routing/forwarding (VRF) to other VRFs on the same or remote PE routers (via MP-BGP).

You can specify up to fifteen (15) policy names.

The **no** form of the command removes all route policy names from the export list.

Default None — No routes are exported from the VRF by default.

Parameters *policy* — The route policy statement name.

vrf-import

Syntax **vrf-import** *policy* [*policy...*]
no vrf-import

Context config>service>vprn

Description This command sets the import policies to control routes imported to the local VPN routing/forwarding (VRF) from other VRFs on the same or remote PE routers (via MP-BGP). Up to fifteen (15) names may be specified.

BGP-VPN routes imported with a vrf-import policy will use the BGP preference value of 170 when imported from remote PE routers, or retain the protocol preference value of the exported route when imported from other VRFs on the same router, unless the preference is changed by the policy.

The **no** form of the command removes all route policy names from the import list

Default None — No routes are accepted into the VRF by default.

Parameters *policy* — The route policy statement name.

vrf-target

Syntax **vrf-target** {**ext-community** | **export** *ext-community* | **import** *ext-community*}
no vrf-target

Context config>service>vprn

Description This command facilitates a simplified method to configure the route target to be added to advertised routes or compared against received routes from other VRFs on the same or remote PE routers (via MP-BGP).

BGP-VPN routes imported with a vrf-target statement will use the BGP preference value of 170 when imported from remote PE routers, or retain the protocol preference value of the exported route when imported from other VRFs in the same router.

Specified **vrf-import** or **vrf-export** policies override the **vrf-target** policy.

The no form of the command removes the vrf-target

Default no vrf-target

Parameters *ext-comm* — An extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values <ext-community> : target:{<ip-addr:comm-val>|
<2byte-asnumber:ext-comm-val>|<4byte-asnumber:comm-val>}

ip-addr	a.b.c.d
comm-val	[0..65535]
2byte-asnumber	[0..65535]

ext-comm-val	[0..4294967295]
4byte-asnumber	[0..4294967295]

import *ext-community* **—** Specify communities allowed to be accepted from remote PE neighbors.

export *ext-community* **—** Specify communities allowed to be sent to remote PE neighbors.

Router L2TP Commands

l2tp

Syntax **l2tp**
no l2tp

Context config>service>vprn

Description This command enables the context to configure L2TP parameters. L2TP extends the PPP model by allowing Layer 2 and PPP endpoints to reside on different devices interconnected by a packet-switched network.

avp-hiding

Syntax **avp-hiding** *sensitive* | *always*
no avp-hiding

Context config>service>vprn>l2tp

Description This command configures Attribute Value Pair (AVP) hiding. This capability can be used to avoid the passing of sensitive data, such as user passwords, as cleartext in an AVP.

The **no** form of the command returns the value to **never** allow AVP hiding.

Parameters *avp-hiding* — Specifies the method to be used for the authentication of the tunnels in this L2TP group.

Default no avp-hiding

Values sensitive — AVP hiding is used only for sensitive information (such as username/password).
always — AVP hiding is always used.

calling-number-format

Syntax **calling-number-format** *ascii-spec*
no calling-number-format

Context config>service>vprn>l2tp

Description This command what string to put in the Calling Number AVP, for L2TP control messages related to a session in this L2TP protocol instance.

Parameters *ascii-spec* — Specifies the L2TP calling number AVP.

Values ascii-spec char-specification ascii-spec
char-specification ascii-char | char-origin

ascii-char a printable ASCII character
char-origin %origin
origin S | c | r | s | l
S - system name, the value of TIMETRA-CHASSIS-MIB::tmnxChassisName
c - Agent Circuit Id
r - Agent Remote Id
s - SAP ID, formatted as a character string
l - Logical Line ID

challenge

Syntax **challenge** *always*
no challenge

Context config>service>vprn>l2tp

Description This command configures the use of challenge-response authentication.

The **no** form of the command reverts to the default **never** value.

Parameters *always* — Specifies that the challenge-response authentication is always used.

Default no challenge

Values always

destruct-timeout

Syntax **destruct-timeout** *destruct-timeout*
no destruct-timeout

Context config>service>vprn>l2tp

Description This command configures the period of time that the data of a disconnected tunnel will persist before being removed.

The **no** form of the command removes the value from the configuration.

Default no destruct-timeout

Parameters *destruct-timeout* — [Specifies the automatic removal of dynamic L2TP sessions, in seconds, that are no longer active.

Default no destruct-timeout

Values 60 — 86400

exclude-avps

Syntax **exclude-avps calling-number**

no exclude-avps

Context config>service>vprn>l2tp

Description This command configures the L2TP AVPs to exclude.

ipcp-subnet-negotiation

Syntax [**no**] **ipcp-subnet-negotiation**

Context configure>router>l2tp>group>ppp
configure>router>l2tp>group>tunnel>ppp
configure>service>vprn>l2tp>group>ppp
configure>service>vprn>l2tp>group>tunnel>ppp

Description Enables IPCP negotiation for PPPoE hosts. If not enabled (default setting), the current behavior will apply even if subnet is allocated to the host. Enables IPCP negotiation for PPPoE hosts. If not enabled (default setting), the current behavior will apply even if subnet is allocated in the host.

peer-address-change-policy

Syntax **peer-address-change-policy** {**accept | ignore | reject**}

Context config>service>vprn>l2tp

Description This command configures the reaction to a change of tunnel peer address in this router.

receive-window-size

Syntax **receive-window-size** *[4..1024]*
no receive-window-size

Context config>service>vprn>l2tp

Description This command configures the L2TP receive window size.

session-limit

Syntax **session-limit** *session-limit*
no session-limit

Context config>service>vprn>l2tp

Description This command configures the L2TP session limit of this router.

Parameters *session-limit* — Specifies the session limit.

Values 1..131071

group

Syntax **group** *tunnel-group-name* [**create**]
no group *tunnel-group-name*

Context config>service>vprn>l2tp

Description This command configures an L2TP tunnel group.

Parameters *tunnel-group-name* — Specifies a name string to identify a L2TP group up to 63 characters in length.

create — This keyword is mandatory when creating a tunnel group name. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

session-limit

Syntax **session-limit** *session-limit*
no session-limit

Context config>service>vprn>l2tp

Description This command configures the L2TP session limit for the router. L2TP is connection-oriented. The L2TP Network Server (LNS) and LAC maintain state for each call that is initiated or answered by an LAC. An L2TP session is created between the LAC and LNS when an end-to-end PPP connection is established between a remote system and the LNS. Datagrams related to the PPP connection are sent over the tunnel between the LAC and LNS. There is a one to one relationship between established L2TP sessions and their associated calls.

Parameters *session-limit* — Specifies the number of sessions allowed.

Default no session-limit

Values 1 — 131071

avp-hiding

Syntax **avp-hiding** *sensitive* | *always*
no avp-hiding

Context config>service>vprn>l2tp>group

Description This command configures Attribute Value Pair (AVP) hiding. This capability can be used to avoid the passing of sensitive data, such as user passwords, as cleartext in an AVP.

The **no** form of the command returns the value to **never** allow AVP hiding.

Parameters *avp-hiding* — Specifies the method to be used for the authentication of the tunnels in this L2TP group.

Default no avp-hiding

Values sensitive — AVP hiding is used only for sensitive information (such as username/password).
always — AVP hiding is always used.

challenge

Syntax **challenge** *always*
no challenge

Context config>service>vprn>l2tp>group

Description This command configures the use of challenge-response authentication.

The **no** form of the command reverts to the default **never** value.

Parameters *always* — Specifies when challenge-response is to be used for the authentication of the tunnels in this L2TP group.

Default no challenge

Values always

destruct-timeout

Syntax **destruct-timeout** *destruct-timeout*
no destruct-timeout

Context config>service>vprn>l2tp>group
config>service>vprn>l2tp>group>tunnel

Description This command configures the period of time that the data of a disconnected tunnel will persist before being removed.

The **no** form of the command removes the value from the configuration.

Default no destruct-timeout

Parameters *destruct-timeout* — [Specifies the automatic removal of dynamic L2TP sessions, in seconds, that are no longer active.

Default no destruct-timeout

Values 60 — 86400

hello-interval

Syntax **hello-interval** *hello-interval*
no hello-interval

Context config>service>vprn>l2tp>group

Description This command configures the time interval between two consecutive tunnel Hello messages. The Hello message is an L2TP control message sent by either peer of a LAC-LNS control connection. This control message is used as a keepalive for the tunnel.

The **no** form of the command removes the interval from the configuration.

Default 60

Parameters *hello-interval* — Specifies the time interval, in seconds, between two consecutive tunnel Hello messages.

Default no hello-interval

Values 60 — 3600

idle-timeout

Syntax **idle-timeout** *idle-timeout*
no idle-timeout

Context config>service>vprn>l2tp>group

Description This command configures the period of time that an established tunnel with no active sessions will persist before being disconnected.

Enter the **no** form of the command to maintain a persistent tunnel.

The **no** form of the command removes the idle timeout from the configuration.

Default no idle-timeout

Parameters *idle-timeout* — Specifies the idle timeout value, in seconds until the group is removed.

Default no idle-timeout

Values 0 — 3600

lns-group

Syntax **lns-group** *lns-group-id*
no lns-group

Context config>service>vprn>l2tp>group

Description This command configures the ISA LNS group.

Parameters *lns-group-id* — Specifies the LNS group ID.

Values 1..4

local-address

Syntax **local-address** *ip-address*

no local-address

Context config>service>vprn>l2tp>group>tunnel

Description This command configures the local address.

Parameters *ip-address* — Specifies the IP address used during L2TP authentication.

local-name

Syntax **local-name** *host-name*
no local-name

Context config>service>vprn>l2tp>group
config>service>vprn>l2tp>group>tunnel

Description This command creates the local host name used by this system for the tunnels in this L2TP group during the authentication phase of tunnel establishment. It can be used to distinguish tunnels.

The **no** form of the command removes thename from the configuration.

Default local-name

Parameters *host-name* — Specifies the host name, up to 64 characters in length, that the router will use to identify itself during L2TP authentication.

Default no local-name

max-retries-estab

Syntax **max-retries-estab** *max-retries*
no max-retries-estab

Context config>service>vprn>l2tp>group
config>service>vprn>l2tp>group>tunnel

Description This command configures the number of retries allowed for this L2TP tunnel while it is established, before its control connection goes down.

The **no** form of the command removes the value from the configuration.

Default no max-retries-estab

Parameters *max-retries* — Specifies the maximum number of retries for an established tunnel.

Default no max-retries-estab

Values 2 — 7

max-retries-not-estab

Syntax **max-retries-not-estab** *max-retries*

no max-retries-not-estab

Context config>service>vprn>l2tp>group
config>service>vprn>l2tp>group>tunnel

Description This command configures the number of retries allowed for this L2TP tunnel while it is not established, before its control connection goes down.

The **no** form of the command removes the value from the configuration.

Default no max-retries-not-estab

Parameters *max-retries* — Specifies the maximum number of retries for non-established tunnels.

Default no max-retries-not-estab

Values 2 — 7

password

Syntax **password** *password* [**hash** | **hash2**]
no password

Context config>service>vprn>l2tp>group
config>service>vprn>l2tp>group>tunnel

Description This command configures the password between L2TP LAC and LNS

The no form of the command removes the password.

Default no password

Parameters *password* — Configures the password used for challenge/response calculation and AVP hiding. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the hash2 keyword is specified.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

Default no password

ppp

Syntax **ppp**

Context config>service>vprn>l2tp>group

Description This command configures PPP for the L2TP tunnel group.

authentication

Syntax **authentication** {**chap**|**pap**|**pref-chap**}

Context config>service>vprn>l2tp>group>ppp

Description This command configures the PPP authentication protocol to negotiate.

authentication-policy

Syntax **authentication-policy** *auth-policy-name*
no authentication-policy

Context config>service>vprn>l2tp>group>ppp

Description This command configures the authentication policy.

Parameters *auth-policy-name* — Specifies the authentication policy name.

Values 32 chars max

default-group-interface

Syntax **default-group-interface** *ip-int-name* **service-id** *service-id*
no default-group-interface

Context config>service>vprn>l2tp>group>ppp

Description This command configures the default group interface.

Parameters *ip-int-name* — Specifies the interface name.

Values 32 chars max

service-id — Specifies the service ID.

Values 1..2147483648

svc-name — Specifies the service name (instead of service ID).

Values 64 chars max

keepalive

Syntax **keepalive** *seconds* [**hold-up-multiplier** *multiplier*]
no keepalive

Context config>service>vprn>l2tp>group>ppp

Description This command configures the PPP keepalive interval and multiplier.

Parameters *seconds* — Specifies in seconds the interval.

Values 10..300

multiplier — Specifies the multiplier.

Values 1..5

mtu

Syntax **mtu** *mtu-bytes*
no mtu

Context config>service>vprn>l2tp>group>ppp

Description This command configures the maximum PPP MTU size.

Parameters *mtu-bytes* — Specifies, in bytes, the maximum PPP MTU size.

Values 512..9212

proxy-authentication

Syntax [**no**] **proxy-authentication**

Context config>service>vprn>l2tp>group>ppp

Description This command configures the use of the authentication AVPs received from the LAC.

proxy-lcp

Syntax [**no**] **proxy-lcp**

Context config>service>vprn>l2tp>group>ppp

Description This command configures the use of the proxy LCP AVPs received from the LAC.

user-db

Syntax **user-db** *local-user-db-name*
no user-db

Context config>service>vprn>l2tp>group>ppp

Description This command configures the local user database to use for PPP PAP/CHAP authentication.

Parameters *local-user-db-name* — Specifies the local user database name.

Values 32 chars max

session-assign-method

Syntax **session-assign-method** *weighted*
no session-assign-method

Context config>service>vprn>l2tp>group

Description This command specifies how new sessions are assigned to one of the set of suitable tunnels that are available or could be made available.

Default no session-assign-method

Parameters *weighted* — specifies that the sessions are shared between the available tunnels. If necessary, new tunnels are set up until the maximum number is reached. The distribution aims at an equal ratio of the actual number of sessions to the maximum number of sessions.

Default no session-assign-method. All new sessions are placed by preference in existing tunnels.

Values weighted — Enables weighted preference to tunnels in the group.

session-limit

Syntax **session-limit** *session-limit*
no session-limit

Context config>service>vprn>l2tp>group
config>service>vprn>l2tp>group>tunnel

Description This command configures the session limit. The value controls how many L2TP session will be allowed within a given context (system, group, tunnel).

The no form of the command removes the value from the configuration.

Default no session-limit

Parameters *session-limit* — Specifies the allowed number of sessions within the given context.

Values 1 — 131071

Router L2TP Tunnel Commands

tunnel

Syntax **tunnel** *tunnel-name* [**create**]
no tunnel *tunnel-name*

Context config>service>vprn>l2tp>group

Description This command configures an L2TP tunnel. A tunnel exists between a LAC-LNS pair and consists of a Control Connection and zero or more L2TP sessions. The tunnel carries encapsulated PPP datagrams and control messages between the LAC and the L2TP Network Server (LNS).

Parameters *tunnel-name* — Specifies a valid string to identify a L2TP up to 32 characters in length.

create — mandatory while creating a new tunnel

auto-establish

Syntax [**no**] **auto-establish**

Context config>service>vprn>l2tp>group>tunnel

Description This command specifies if this tunnel is to be automatically set up by the system.

Default no auto-establish

avp-hiding

Syntax **avp-hiding** {**never | sensitive | always**}
no avp-hiding

Context config>service>vprn>l2tp>group>tunnel

Description This command configures Attribute Value Pair (AVP) hiding. This capability can be used to avoid the passing of sensitive data, such as user passwords, as cleartext in an AVP.

Note that it is recommended that sensitive information not be sent in clear text.

The **no** form of the command removes the parameter of the configuration and indicates that the value on group level will be taken.

Default no avp-hiding

Parameters *avp-hiding* — Specifies the method to be used for the authentication of the tunnel.

Values never — AVP hiding is not used.
sensitive — AVP hiding is used only for sensitive information (such as username/password).
always — AVP hiding is always used.

challenge

Syntax **challenge** *challenge-mode*
no challenge

Context config>service>vprn>l2tp>group>tunnel

Description This command configures the use of challenge-response authentication.

The **no** form of the command removes the parameter from the configuration and indicates that the value on group level will be taken.

Default no challenge

Parameters *challenge-mode* — Specifies when challenge-response is to be used for the authentication of the tunnel.

Values always — Always allows the use of challenge-response authentication.
never — Never allows the use of challenge-response authentication.

hello-interval

Syntax **hello-interval** *hello-interval*
hello-interval infinite
no hello-interval

Context config>service>vprn>l2tp>group>tunnel

Description This command configures the number of seconds between sending Hellos for a L2TP tunnel. The no form removes the parameter from the configuration and indicates that the value on group level will be taken.

Parameters *hello-interval* — Specifies the time interval, in seconds, between two consecutive tunnel Hello messages.

Values 60 — 3600

infinite — Specifies that no hello messages are sent.

idle-timeout

Syntax **idle-timeout** *idle-timeout*
idle-timeout infinite
no idle-timeout

Context config>service>vprn>l2tp>group>tunnel

Description This command configures the idle timeout to wait before being disconnect. The no form indicates that the parameter will be removed from the configuration and that the value specified on group level will be taken.

Parameters *idle-timeout* — Specifies the idle timeout, in seconds.

Values 0 — 3600

infinite — Specifies that the tunnel will not be closed when idle.

peer

Syntax **peer** *ip-address*
no peer

Context config>service>vprn>l2tp>group>tunnel

Description This command configures the peer address.

The **no** form of the command removes the IP address from the tunnel configuration.

Default no peer

Parameters *ip-address* — Sets the LNS IP address for the tunnel.

preference

Syntax **preference** *preference*
no preference

Context config>service>vprn>l2tp>group>tunnel

Description This command configures a preference number that indicates the relative preference assigned to a tunnel when using a weighted session assignment.

The **no** form of the command removes the preference value from the tunnel configuration.

Default no preference

Parameters *preference* — Specifies the tunnel preference number with its group. The value 0 corresponds to the highest preference.

Values 0 — 16777215

remote-name

Syntax **remote-name** *host-name*
no remote-name

Context config>service>vprn>l2tp>group>tunnel

Description This command configures a string to be compared to the host name used by the tunnel peer during the authentication phase of tunnel establishment.

Parameters *host-name* — Specifies a remote host name for the tunnel up to 64 characters in length.

Router DHCP Configuration Commands

dhcp

Syntax **dhcp**

Context config>service>vprn

Description This command enables the context to configure DHCP parameters.

dhcp6

Syntax **dhcp6**

Context config>service>vprn

Description This command enables the context to configure DHCP6 parameters.

local-dhcp-server

Syntax **local-dhcp-server** *server-name* [**create**]
no local-dhcp-server *server-name*

Context config>service>vprn>dhcp
config>service>vprn>dhcp6
config>service>vprn>if
config>service>vprn>nw-if

Description This command instantiates a local DHCP server. A local DHCP server can serve multiple interfaces but is limited to the routing context it was which it was created.

Default none

Parameters *server-name* — Specifies the name of local DHCP server.

create — Keyword used to create the server name. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

failover

Syntax **failover**

Context config>service>vprn>dhcp

Description This command enables the context to configure failover parameters.

ignore-mclt-on-takeover

Syntax **ignore-mclt-on-takeover**
no ignore-mclt-on-takeover

Context config>service>vprn>dhcp>server>failover

Description With this flag enabled, the 'remote' IP address/prefix can be taken over immediately upon

entering the PARTNER-DOWN state of the intercommunication link, without having to wait for the MCLT to expire. Note that by setting this flag, the lease times of the existing DHCP clients, while the intercommunication link is in the PARTNER-DOWN state, will still be reduced to the MCLT over time and all new lease times will be set to MCLT this behavior remain the same as originally intended for MCLT.

Some deployments require that the 'remote' IP address/prefix range starts delegating new IP addresses/prefixes upon the failure of the intercommunication link, without waiting for the intercommunication link to transition from the COMM-INT state into the PARTNER-DOWN state and the MCLT to expire while in PARTNER-DOWN state.

This can be achieved by enabling the ignore-mclt-on-takeover flag and by configuring the partner-down-delay to 0.

Enabling this functionality must be exercised with caution. One needs to keep in mind that the partner-down-delay and MCLT timers were originally introduced to prevent IP address duplication in cases where DHCP redundant nodes transition out-of-sync due to the failure of intercommunication link. These timers (partner-down-delay and MCLT) would ensure that during their duration, the new IP addresses/prefixes are delegated only from one node – the one with local IP address-range/prefix. The drawback is of course that the new IP address delegation is delayed and thus service is impacted.

But if one could ensure that the intercommunication link is always available, then the DHCP nodes would stay in sync and the two timers would not be needed. This is why it is of utmost importance that in this mode of operation, the intercommunication link is well protected by providing multiple paths between the two DHCP nodes. The only event that should cause intercommunication link to fail is the entire nodal failure. This failure is acceptable since in this case only one DHCP node is available to provide new IP addresses/prefixes.

Default no ignore-mclt-on-takeover

maximum-client-lead-time

Syntax **maximum-client-lead-time** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no maximum-client-lead-time

Context config>service>vprn>dhcp>server>failover

Description Maximum-client-lead-time (MCLT) is the maximum time that a DHCP server can extend client's lease time beyond the lease time currently known by the DHCP partner node. In dual-homed environment, the initial lease time for all DHCP clients is by default restricted to MCLT. Consecutive DHCP renews are allowed to extend the lease time beyond the MCLT.

The MCLT is a safeguard against IP address/prefix duplication in cases of a lease synchronization failure when local-remote failover model is deployed

Once the intercommunication link failure between the redundant DHCP servers is detected, the DHCP IP address range configured as remote will not be allowed to start delegating new leases until the MCLT + partner-down-delay intervals expire. This is to ensure that the new lease that was delegated from the 'local' IP address-range/prefix on one node, but was never synchronized due to the intercommunication link failure, will expire before the same IP address/prefix is allocated from the remote IP address-range/prefix on the other node.

However, the already existing (and synchronized) lease times can be renewed from the remote IP address range at any time, regardless of the state of the intercommunication link (operational or failed).

Lease synchronization failure can be caused either by a node failure, or a failure of the link over which the DHCP leases are synchronized (intercommunication link). Synchronization failure detection can take up to 3 seconds.

During the failure, the DHCP lease time for the new clients will be restricted to MCLT while for the existing clients the lease time will over time (by consecutive DHCP renews) be gradually reduced to the MCLT.

Default 10 minutes

Parameters **hrs** *hours* — Specifies the hour parameter of the MCLT.

Values 1 — 23

min *minutes* — Specifies the minute parameter of the MCLT.

Values 1 — 59

sec *seconds* — Specifies the seconds parameter of the MCLT.

Values 1 — 59

partner-down-delay

Syntax **partner-down-delay** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no partner-down-delay

Context config>service>vprn>dhcp>server>failover

Description Since the DHCP lease synchronization failure can be caused by the failure of the intercommunication link (and not necessary the entire node), there is a possibility the redundant DHCP servers become isolated in the network. In other words, they can serve DHCP clients but they cannot synchronize the lease. This can lead to duplicate assignment of IP addresses, since the servers have configured overlapping IP address ranges but they are not aware of each other's leases.

The purpose of the partner-down-delay is to prevent the IP lease duplication during the intercommunication link failure by not allowing new IP addresses to be assigned from the remote IP address range. This timer is intended to provide the operator with enough time to remedy the failed situation and to avoid duplication of IP addresses/prefixes during the failure.

During the partner-down-delay time, the prefix designated as remote will be eligible only for renewals of the existing DHCP leases that have been synchronized by the peering node. Only after the sum of the partner-down-delay and the maximum-client-lead-time will the prefix designated as

remote be eligible for delegation of the new DHCP leases. When this occurs, we say that the remote IP address range has been taken over.

It is possible to expedite the takeover of a remote IP address range so that the new IP leases can start being delegated from that range shortly after the intercommunication failure is detected. This can be achieved by configuring the partner-down-delay timer to 0 seconds, along with enabling the ignore-mclt-on-takeover CLI flag. Caution must be taken before enabling this functionality. It is safe to bypass safety timers (partner-down-delay + MCLT) only in cases where the operator is certain that the intercommunication between the nodes has failed due to the entire node failure and not due to the intercommunication (MCS) link failure. Failed intercommunication due to the nodal failure would ensure that only one node is present in the network for IP address delegation (as opposed to two isolated nodes with overlapping IP address ranges where address duplication can occur). For this reason, the operator MUST ensure that there are redundant paths between the nodes to ensure uninterrupted synchronization of DHCP leases.

In access-driven mode of operation, partner-down-delay has no effect.

Default 23 hours, 59minutes, and 59 seconds.

Parameters **hrs** *hours* — Specifies the hour parameter of the partner down delay feature.

Values 1 — 23

min *minutes* — Specifies the minute parameter of the partner down delay feature.

Values 1 — 59

sec *seconds* — Specifies the seconds parameter of the partner down delay feature.

Values 1 — 59

peer

Syntax **peer** *ip-address* **tag** *sync-tag-name*
no peer *ip-address*

Context config>service>vprn>dhcp>server>failover

Description DHCP leases can be synchronized per DHCP server. The pair of synchronizing servers is identified by a tag. The synchronization information is carried over the Multi-Chassis Synchronization (MCS) link between the two peers. MCS link is a logical link (IP, or MPLS).

MCS runs over TCP, port 45067 and it is using either data traffic or keepalives to detect failure on the communication link between the two nodes. In the absence of any MCS data traffic for more than 0.5sec, MCS will send its own keepalive to the peer. If a reply is NOT received within 3sec, MCS will declare its operation state as DOWN and the DB Sync state as out-of-sync. MCS will consequently notify its clients (DHCP Server being one of them) of this. It can take up to 3 seconds before the DHCP client realizes that the inter-chassis communication link has failed.

Note that the inter-chassis communication link failure does not necessarily assume the same failed fate for the access links. In other words the two redundant nodes can become isolated from each other in the network. This would occur in cases where only the intercommunication (MCS) link fails. It is of utmost importance that this MCS link be highly redundant.

Parameters *ip-address* — Specifies the IPv4 address of the peer

sync-tag *sync-tag* — Specifies a synchronization tag to be used while synchronizing DHCP server or pools.

startup-wait-time

Syntax [**no**] **startup-wait-time** [**min** *minutes*] [**sec** *seconds*]

Context configure>service>vprn>dhcp6>server>failover
configure>service>vprn>dhcp6>server>pool

Description This command enables startup-wait-time during which each peer waits after the initialization process before assuming the active role for the prefix designated as local or access-driven. This is to avoid transient issues during the initialization process.

Default 2 minutes

Parameters **min** *minutes* — Specifies the minute parameter of the startup wait time feature.

Values 1 — 10

sec *seconds* — Specifies the seconds parameter of the startup wait time feature.

Values 1 — 59

ignore-rapid-commit

Syntax [**no**] **ignore-rapid-commit**

Context config>service>vprn>dhcp6>server

Description This command specifies whether the Rapid Commit Option (RCO) sent by the DHCPv6 client is processed.

If enabled and the client has included an RCO in the solicit, the server ignores the option and processes the remainder of the message as if no RCO were present.

The **no** form of the command disables ignore-rapid-commit.

lease-hold-time

Syntax **lease-hold-time** [**days** *days*][**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-hold-time

Context config>service>vprn>dhcp6>server

Description This command configures the time to remember this lease.

Parameters [**days** *days*][**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] — S the lease hold time.

Values		
	days:	[0..3650]
	hours:	[0..23]

minutes:	[0..59]
seconds:	[0..59

force-renews

Syntax [**no**] **force-renews**

Context config>service>vprn>dhcp>server

Description This command enables the sending of sending forcerenew messages.

The **no** form of the command disables the sending of forcerenew messages.

Default no disable-force-renews

pool

Syntax **pool** *pool-name* [**create**]
no pool *pool-name*

Context config>service>vprn>dhcp>server

Description This command configures a DHCP address pool on the router.

Default none

Parameters *pool name* — Specifies the name of this IP address pool. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters.

create — Keyword used to create the entity. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

max-lease-time

Syntax **max-lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no max-lease-time

Context config>service>vprn>dhcp>server>pool

Description This command configures the maximum lease time.

The **no** form of the command returns the value to the default.

Default 10 days

Parameters *time* — Specifies the maximum lease time.

Values

days :	0 — 3650
hours	0 — 23
minutes:	0 — 59
seconds	0 — 59

min-lease-time

Syntax **min-lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no min-lease-time

Context config>service>vprn>dhcp>server>pool

Description This command configures the minimum lease time.

The **no** form of the command returns the value to the default.

Default 10 minutes

Parameters *time* — Specifies the minimum lease time.

Values

days :	0 — 3650
hours	0 — 23
minutes:	0 — 59
seconds	0 — 59

minimum-free

Syntax **minimum-free** *minimum-free* [**percent**] [**event-when-depleted**]
no minimum-free

Context config>service>vprn>dhcp>server>pool

Description This command configures the minimum number of free addresses.

The **no** form of the command reverts to the default.

Default 1

Parameters *minimum-free* — Specifies the desired minimum number of free addresses in this pool. If the actual number of free addresses in this pool falls below this configured minimum, a notification is generated.

Values 0 — 255

percent — Indicates the value indicates a percentage.

event-when-depleted — This parameter enables a system-generate event when all available addresses in the pool/subnet of local DHCP server are depleted.

offer-time

Syntax **offer-time** [**min** *minutes*] [**sec** *seconds*]
no offer-time

Context config>service>vprn>dhcp>server>pool

Description This command configures the offer time.

The **no** form of the command returns the value to the default.

Default 1 minute

Parameters *time* — Specifies the offer time.

Values

minutes:	0 — 10
seconds	0 — 59

options

Syntax **options**

Context config>service>vprn>dhcp>server>pool

Description This command enables the context to configure pool options. The options defined here can be overruled by defining the same option in the local user database.

Default none

custom-option

Syntax **custom-option** *option-number* **address** *ip-address* [*ip-address*...(up to 4 max)] (DHCP only)
custom-option *option-number* **address** *ipv6-address* [*ipv6-address*...(up to 4 max)] (**DHCP6 only**)
custom-option *option-number* **domain** *domain-string*
custom-option *option-number* **hex** *hex-string*
custom-option *option-number* **string** *ascii-string*
no custom-option *option-number*

Context config>service>vprn>dhcp>server>pool>options
config>service>vprn>dhcp>server>pool>subnet>options

Description This command configures specific DHCP options. The options defined here can overrule options in the local user database.

The **no** form of the removes the option from the configuration.

Default none

Parameters *option-number* — specifies the option number that the DHCP server uses to send the identification strings to the DHCP client.

Values 1 — 254

address *ip-address* **—** Specifies the IP address of this host.

domain *domain-string* **— — hex** *hex-string* **—** Specifies the hex value of this option.

Values 0x0..0xFFFFFFFF...(maximum 254 hex nibbles)

string *ascii-string* **—** Specifies the value of this option.

Values Up to 127 characters maximum.

dns-server

Syntax **dns-server** *ip-address* [*ip-address*...(up to 4 max)](**DHCP only**)
dns-server *ipv6-address* [*ipv6-address*...(up to 4 max)] (**DHCP6 only**)

Context config>service>vprn>dhcp>server>pool>options

Description This command configures the IP address of the DNS server.

Default none

Parameters *ip-address* — The IP address of the DNS server. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

domain-name

Syntax **domain-name** *domain-name*
no domain-name

Context config>service>vprn>dhcp>server>pool>options

Description This command configures the default domain for a DHCP client that the router uses to complete unqualified hostnames (without a dotted-decimal domain name).

The **no** form of the command removes the name from the configuration.

Default none

Parameters *domain-name* — Specifies the domain name for the client.

Values Up to 127 characters

renew-timer

Syntax **renew-timer** [**days** *days*][**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no renew-timer

Context config>service>vprn>dhcp6>server>pool>prefix

Description This command configures the renew-timer (T1), the time at which the client contacts the server from which the addresses in the IA_NA or IA_PD were obtained to extend the lifetimes of the addresses or prefixes assigned to the client.

Default 1800

Parameters *seconds* — Specifies the time duration relative to the current time, expressed in units of seconds. A value of zero leaves the renew-time at the discretion of the client.

Values 0-604,800

rebind-timer

Syntax **rebind-timer** [**days** *days*][**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no rebind-timer

Context config>service>vprn>dhcp6>server>pool>prefix

Description This command configures the rebind-timer (T2), the time at which the client contacts any available server to extend the lifetimes of the addresses or prefixes assigned to the client.

Default 2880

Parameters *seconds* — T2 is a time duration relative to the current time. A value of zero leaves the rebind-time at the discretion of the client.

Values 0-1,209,600

Parameters [**days** *days*][**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] — Specifies the rebind timer.

Values		
	days:	[0..3650]
	hours:	[0..23]
	minutes:	[0..59]
	seconds:	[0..59

prefix

Syntax **prefix** *ipv6-address/prefix-length* [**failover** {**local**|**remote**}] [**pd**] [**wan-host**] [**create**]
no prefix *ipv6-address/prefix-length*

Context config>service>vprn>dhcp6>server>pool

Description This command allows a list of prefixes(using the prefix command multiple times) to be routed to hosts associated with this pool. Each prefix will be represented in the associated FIB with a reference to the pool. Prefixes are defined as being for prefix delegation (pd) or use on a WAN interface or host (wan-host).

Default Failover local.

Parameters *ipv6-address* — Specifies the 128-bit IPv6 address.

Values 128-bit hexadecimal IPv6 address in compressed form

prefix-length — Specifies the length of any associated aggregate prefix.

Values 32-63

failover — This command designates a IPv6 prefx as local, remote or access-driven. This is used when multi-chassis synchronization is enabled.

local — An IPv6 prefix designated as local is used for new lease grants or to renew the existing lease grants. Local prefix designation should be always paired with the remote designation of the same prefix on the peering node.
The IPv6 prefix configured as local on one node can only be configured as remote on the other

node. No other combination is allowed between the two nodes for an IPv6 prefix that is configured as local.
The dhcpv6 relay could point to both IPv6 DHCP server addresses - the one hosting the local IPv6 prefix and the one hosting the corresponding remote IPv6 prefix. Under normal circumstances the new lease will always be allocated from the local IPv6 prefix while the leases can be renewed from either IPv6 prefix (local or remote). Under network failure, the remote IPv6 prefix can be taken over according to the intercommunication link state transitions and associated timers.

remote — An IPv6 prefix designated as remote is used only to renew the existing DHCP leases. The new leases will be delegated from it only after the maximum-client-lead-time + partner-down-delay time elapses. At that point we say that the remote IPv6 prefix has been taken over.
To ensure faster takeover, the partner-down-delay can be set to 0 and the MCLT time can be ignored. Extra caution should be exercised when enabling this mode of operation, as described in the configuration guides.
The IPv6 prefix configured as remote on one node can only be configured as local on the other node. No other combination is allowed between the two nodes for an IP address ranges that is configured as remote.

access-driven — An IPv4 prefix designated as access-driven is used for new lease grants or to renew the existing lease grants regardless of the state of the intercommunication link (operational or failed). In this mode of operation the IPv6 prefix is actively shared between the two 7x50 DHCPv6 server nodes. This can be used on both DHCPv6 servers only in cases where the access protection mechanism (SRRP or MC-LAG) will ensure that there is only a single active path for DHCPv6 clients using the same IPv6 prefix available to one of the redundant 7x50 DHCPv6 nodes.
The IPv6 prefix configured as access-driven on one node can only be configured as access-driven on the other node. No other combination is allowed between the two nodes for an IPv6 prefix that is configured as access-driven.
There MUST be no crosslinks between the DHCPv6 servers that have IPv6 address ranges configured in access-driven failover mode. In other words, each node must have the dhcp-relay pointing to the IPv6 address of the local DHCPv6 server. This IPv6 address must be the same on both nodes. For example, both DHCPv6 servers should have a loopback address configured with the same IPv6 address (IPv4 or IPv6) and a DHCPv6 server associated with this loopback address. Those IPv6 addresses MUST not be advertised outside of each box. The DHCPv6 relay in each node would point to its local DHCPv6 server via this loopback IPv6 address.

pd — Specifies that this aggregate is used by IPv6 ESM hosts for DHCPv6 prefix-delegation.

wan-host — Specifies that this aggregate is used by IPv6 ESM hosts for local addressing or by a routing gateway's WAN interface.

preferred-lifetime

Syntax **preferred-lifetime** [**days** *days*][**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no preferred-lifetime

Context config>service>vprn>dhcp6>server>pool>prefix

Description The preferred lifetime for the IPv6 prefix or address in the option, expressed in units of seconds. When the preferred lifetime expires, any derived addresses are deprecated.

Default 3600

Parameters *time* — Specifies the preferred lifetime.

Values

days:	0 — 3650
hours:	0 — 23
minutes:	0 — 59
seconds	0 — 59

valid-lifetime

Syntax **valid-lifetime** [**days** *days*][**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no valid-lifetime

Context config>service>vprn>dhcp6>server>pool>prefix

Description The valid lifetime for the IPv6 prefix or address in the option, expressed in units of seconds.

Default 86,400

Parameters *time* — Specifies the valid lifetime.

Values

days:	0 — 3650
hours:	0 — 23
minutes:	0 — 59
seconds	0 — 59

use-link-address

Syntax **use-link-address** [**scope** *scope*]
no use-link-address

Context config>service>vprn>dhcp6>server

Description This command specifies whether the GI address selects a single subnet or a pool.

The **no** form of the command reverts to the default.

Default subnet

Parameters **scope** *scope* — Specifies the scope of the IP address selection.

Values subnet, pool

user-ident

Syntax **user-ident** *user-ident*
no user-ident

Context config>service>vprn>dhcp6>server

Description This command specifies which method is used by the local DHCP server to uniquely identify a user.

The **no** form of the command reverts to the default.

Default duid

Parameters *user-ident* — Configures the user identification method.

Values duid, interface-id, interface-id-link-local

lease-rebind-time

Syntax **lease-rebind-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-rebind-time

Context config>service>vprn>dhcp>server>pool>options

Description This command configures the time the client transitions to a rebinding state.

The **no** form of the command removes the time from the configuration.

Default none

Parameters *time* — Specifies the lease rebind time.

Values		
	days:	0 — 3650
	hours:	0 — 23
	minutes:	0 — 59
	seconds	0 — 59

lease-renew-time

Syntax **lease-renew-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-renew-time

Context config>service>vprn>dhcp>server>pool>options

Description This command configures the time the client transitions to a renew state.

The **no** form of the command removes the time from the configuration.

Default none

Parameters *time* — Specifies the lease renew time.

Values		
	days:	0 — 3650
	hours:	0 — 23
	minutes:	0 — 59
	seconds	0 — 59

lease-time

Syntax **lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-time

Context config>service>vprn>dhcp>server>pool>options

Description This command configures the amount of time that the DHCP server grants to the DHCP client permission to use a particular IP address.

The **no** form of the command removes the lease time parameters from the configuration.

Default none

Parameters *time* — Specifies the lease time.

Values

days :	0 — 3650
hours	0 — 23
minutes:	0 — 59
seconds	0 — 59

netbios-name-server

Syntax **netbios-name-server ip-address** [*ip-address*...(up to 4 max)]
no netbios-name-server

Context config>service>vprn>dhcp>server>pool>options

Description This command configures up to four Network Basic Input/Output System (NetBIOS) name server IP addresses.

Default none

Parameters *ip-address* — The IP address of the NetBIOS name server. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

netbios-node-type

Syntax **netbios-node-type** *netbios-node-type*
no netbios-node-type

Context config>service>vprn>dhcp>server>pool>options

Description This command configures the Network Basic Input/Output System (NetBIOS) node type.

Default none

Parameters *netbios-node-type* — Specifies the netbios node type.

Values B — Broadcast node uses broadcasting to query nodes on the network for the owner of a NetBIOS name.
P — Peer-to-peer node uses directed calls to communicate with a known NetBIOS name server for the IP address of a NetBIOS machine name.
M — Mixed node uses broadcasted queries to find a node, and if that fails, queries

a known P-node name server for the address.
H — Hybrid node is the opposite of the M-node action so that a directed query is executed first, and if that fails, a broadcast is attempted.

server

Syntax **server** *server-name*
no server

Context configure>service>ies>sub-if>grp-if>local-address-assignment
configure>service>ies>sub-if>local-address-assignment
configure>service>vprn>sub-if>grp-if>local-address-assignment
configure>service>vprn>sub-if>local-address-assignment

Description This command designates a local 7x50 DHCPv4 server for local pools management where IPv4 addresses for PPPoXv4 clients will be allocated without the need for the internal 7x50 DHCP relay-agent. Those addresses will be tied to PPPoX sessions and they will be de-allocated when the PPPoX session is terminated.

Default none

Parameters *server-name* — Specifies the name of the local 7x50 DHCP server.

client-application

Syntax **client-application [ppp-v4]**
no client-application

Context configure>service>ies>sub-if>grp-if>local-address-assignment
configure>service>ies>sub-if>local-address-assignment
configure>service>vprn>sub-if>grp-if>local-address-assignment
configure>service>vprn>sub-if>local-address-assignment

Description This command enables local 7x50 DHCP Server pool management for PPPoXv4 clients. A pool of IP addresses can be shared between IPoE clients that rely on DHCP protocol (lease renewal process) and PPPoX clients where address allocation is not dependent on DHCP messaging but instead an IP address allocation within the pool is tied to the PPPoX session.

Default none

Parameters **ppp-v4 —**

default-pool

Syntax **default-pool** *pool-name*
no default-pool

Context configure>service>ies>sub-if>grp-if>local-address-assignment

configure>service>ies>sub-if>local-address-assignment
configure>service>vprn>sub-if>grp-if>local-address-assignment
configure>service>vprn>sub-if>local-address-assignment

Description This command references a default DHCP address pool for local PPPoX pool management in case that the pool-name is not retuned via Radius or LUDB.

Default none

Parameters *pool-name* — Specifies the name of the local 7x50 DHCP server pool.

delayed-enable

Syntax **delayed-enable** *seconds* **[init-only]**
no delayed-enable

Context configure>service>ies>sub-if>local-address-assignment
configure>service>vprn>sub-if>local-address-assignment

Description This command will render the subscriber-interface non operation for the given amount of time once the node is rebooted or once the interface is enabled (no-shutdown). The purpose of this timer is to stall the operation of the subscriber-interface until the MCS database is synchronized.

A typical use case for this timer would be to prevent IP lease duplication for PPPoE clients using local PPPoXv4/v6 pools in redundant DHCPv4/v6 server configuration. Since there is no classical DHCP lease state maintained for local PPPoXv4/v6 pools, the IP addresses will not be synchronized via DHCP Server. Instead they will be synchronized via PPPoX clients whose state is maintained in 7x50. Once the PPPoX subscriber host is synchronized between the two 7x50 nodes, the respective IP address lease will be updated in the respective local pool.

One artifact of this behavior (IP address assignment in local DHCP pools is synchronized via PPPoX clients and not via DHCP server synchronization mechanism) is that during the node boot, the DHCP server must wait for the completion of PPPoX subscriber synchronization via MCS so that it learns which addresses/prefixes are already allocated on the peering node. Since the DHCP server can theoretically start assigning IP addresses before the PPPoX sync is completed, a duplicate address assignment my occur. For example an IP address lease can be granted via DHCP local pools while PPPoX sync is still in progress. Once the PPPoX sync is completed, the DHCP server may discover that the granted IP lease has already been allocated by the peering node. The most recent lease will be kept and the other will be removed from both systems. To prevent this scenario, a configurable timer is set to an arbitrary value that will render sub-if non-operational until the timer expires. The purpose of this timer is to allow the PPPoX sync to complete before subscribers under the sub-intf can be served.

Default none

Parameters *second* — Specifies in seconds.

Values [1..1200]

subnet

Syntax **subnet** {*ip-address*/*mask* | *ip-address netmask*} [**create**]
no subnet {*ip-address*/*mask* | *ip-address netmask*}

Context config>service>vprn>dhcp>server>pool

Description This command creates a subnet of IP addresses to be served from the pool. The subnet cannot include any addresses that were assigned to subscribers without those addresses specifically excluded. When the subnet is created no IP addresses are made available until a range is defined.

Default none

Parameters *ip-address* — Specifies the base IP address of the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

mask — The subnet mask in dotted decimal notation. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

create — Keyword used to create the entity. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

address-range

Syntax **address-range** *start-ip-address end-ip-address* **[failover {local | remote | access-driven}]**
no address-range *start-ip-address end-ip-address*

Context config>service>vprn>dhcp>server>pool>subnet

Description This command configures a range of IP addresses to be served from the pool. All IP addresses between the start and end IP addresses will be included (other than specific excluded addresses).

The only two valid failover combinations between the two redundant DHCP nodes are:

- local - remote
- access-driven - access-driven

Default Failover local

Parameters *start-ip-address* — Specifies the start address of this range to include. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

end-ip-address — Specifies the end address of this range to include. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

failover — This command designates an address range as local, remote or access-driven. This is used when multi-chassis synchronization is enabled.

local — An IPv4 address-range designated as local is used for new lease grants or to renew the existing lease grants. Local address-range designation should be always paired with the remote

designation of the same address-range on the peering node.
The IP address range configured as local on one node can only be configured as remote on the other node. No other combination is allowed between the two nodes for an IP address ranges that is configured as local.
The dhcp relay could point to both IP DHCP server addresses - the one hosting the local IP address range and the one hosting the corresponding remote IP address range. Under normal circumstances the new lease will always be allocated from the local IP address range while the leases can be renewed from either IP address range (local or remote). Under network failure, the remote IP address range can be taken over according to the intercommunication link state transitions and associated timers.

remote — An IPv4 address-range designated as remote is used only to renew the existing DHCP leases. The new leases will be delegated from it only after the maximum-client-lead-time + partner-down-delay time elapses. At that point we say that the remote IP address range has been taken over.
To ensure faster takeover, the partner-down-delay can be set to 0 and the MCLT time can be ignored. Extra caution should be exercised when enabling this mode of operation, as described in the configuration guides.
The IP address range configured as remote on one node can only be configured as local on the other node. No other combination is allowed between the two nodes for an IP address ranges that is configured as remote.

access-driven — An IPv4 address-range designated as access-driven is used for new lease grants or to renew the existing lease grants regardless of the state of the intercommunication link (operational or failed). In this mode of operation the IP address-range is actively shared between the two 7x50 DHCP server nodes. This can be used on both DHCP servers only in cases where the access protection mechanism (SRRP or MC-LAG) will ensure that there is only a single active path for DHCP clients using the same IP address range available to one of the redundant 7x50 DHCP nodes.
The IP address range configured as access-driven on one node can only be configured as access-driven on the other node. No other combination is allowed between the two nodes for an IP address ranges that is configured as access-driven.
There MUST be no crosslinks between the DHCP servers that have IP address ranges configured in access-driven failover mode. In other words, each node must have the dhcp-relay pointing to the IP address of the local DHCP server. This IP address must be the same on both nodes. For example, both DHCP servers should have a loopback address configured with the same IP address (IPv4 or IPv6) and a DHCP server associated with this loopback address. Those IP addresses MUST not be advertised outside of each box. The DHCP relay in each node would point to its local DHCP server via this loopback IP address.

drain

Syntax [**no**] drain

Context config>service>vprn>dhcp>server>pool>subnet

Description This command subnet draining which means no new leases can be assigned from this subnet and existing leases are cleaned up upon renew/rebind.

The **no** form of the command means the subnet is active and new leases can be assigned from it.

exclude-addresses

Syntax [**no**] **exclude-addresses** *start-ip-address* [*end-ip-address*]

Context config>service>vprn>dhcp>server>pool>subnet

Description This command specifies a range of IP addresses that excluded from the pool of IP addresses in this subnet.

Default none

Parameters *start-ip-address* — Specifies the start address of this range to exclude. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

end-ip-address — Specifies the end address of this range to exclude. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

maximum-declined

Syntax **maximum-declined** *maximum-declined*
no maximum-declined

Context config>service>vprn>dhcp>server>pool>subnet

Description This command configures the maximum number of declined addresses allowed.

Default 64

Parameters *maximum-declined* — Specifies the maximum number of declined addresses allowed.

Values 0 — 4294967295

minimum-free

Syntax **minimum-free** *minimum-free* [**percent**] [**event-when-depleted**]
no minimum-free

Context config>service>vprn>dhcp>server>pool>subnet

Description This command configures the minimum number of free addresses in this subnet. If the actual number of free addresses in this subnet falls below this configured minimum, a notification is generated.

Default 1

Parameters *minimum-free* — Specifies the minimum number of free addresses in this subnet.

Values 0 — 255

percent — Indicates the value indicates a percentage.

event-when-depleted — This parameter enables a system-generate event when all available addresses in the pool/subnet of local DHCP server are depleted.

default-router

Syntax **default-router** *ip-address* [*ip-address*...(up to 4 max)]
no default-router

Context config>service>vprn>dhcp>server>pool>subnet

Description This command configures the IP address of the default router for a DHCP client. Up to four IP addresses can be specified.

The **no** form of the command removes the address(es) from the configuration.

Default none

Parameters *ip-address* — Specifies the IP address of the default router. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

subnet-mask

Syntax **subnet-mask** *ip-address*
no subnet-mask

Context config>service>vprn>dhcp>server>pool>subnet

Description This command specifies the subnet-mask option to the client. The mask can either be defined (for supernetting) or taken from the pool address.

The **no** form of the command removes the address from the configuration.

Default none

Parameters *ip-address* — Specifies the IP address of the subnet mask. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

use-gi-address

Syntax [**no**] **use-gi-address**

Context config>service>vprn>dhcp>server

Description This command enables the use of gi-address matching. If the gi-address flag is enabled, a pool can be used even if a subnets is not found. If the local-user-db-name is not used, the gi-address flag is used and addresses are handed out by GI only. If a user must be blocked from getting an address the server maps to a local user database and configures the user with no address.

A pool can include multiple subnets. Since the GI is shared by multiple subnets in a subscriber-interface the pool may provide IP addresses from any of the subnets included when the GI is matched to any of its subnets. This allows a pool to be created that represents a sub-int.

Default no use-gi-address

use-pool-from-client

Syntax [**no**] **use-pool-from-client**

Context config>service>vprn>dhcp>server
config>service>vprn>dhcp6>server

Description This command specifies if the IP address pool to be used by this server is the pool indicated by the vendor-specific sub-option 13 of the DHCP Option 82.

When enabled, the pool indicated by the sub-option 13 is to be used.

The **no** form of the command indicates that the pool selection is specified by the value of **use-gi-address** setting.

user-db

Syntax **user-db** *local-user-db-name*
no user-db

Context config>service>vprn>dhcp>server

Description This command configures a local user database for authentication.

Default not enabled

Parameters *local-user-db-name* — Specifies the name of a local user database.

Multicast VPN Commands

mvpn

Syntax **mvpn**

Context config>service>vprn

Description This command enables the context to configure MVPN-related parameters for the IP VPN.

auto-discovery

Syntax [**no**] **auto-discovery** [**default | mdt-safi**]

Context config>service>vprn>mvpn

Description This command enables MVPN membership auto-discovery through BGP. When auto-discovery is enabled, PIM peering on the inclusive provider tunnel is disabled.

The **no** form of the command disables MVPN membership auto-discovery through BGP.

Default enabled

default — Enable AD route exchange based on format defined in draft-ietf-l3vpn-2547bis-mcast-10.

mdt-safi — Enable AD route exchange based on mdt-safi format defined in draft-rosen-vpn-mcast-15.

c-mcast-signaling

Syntax **c-mcast-signaling** {**bgp** | **pim**}
no c-mcast-signaling

Context config>service>vprn>mvpn

Description This command specifies BGP or PIM, for PE-to-PE signaling of CE multicast states. When this command is set to PIM and neighbor discovery by BGP is disabled, PIM peering will be enabled on the inclusive tree.

Changes may only be made to this command when the mvpn node is shutdown.

The **no** form of the command reverts it back to the default.

Default mcast-signaling bgp

Parameters **bgp —** Specifies to use BGP for PE-to-PE signaling of CEmulticast states. Auto-discovery must be enabled.

pim — Specifies to use PIM for PE-to-PE signaling of CE multicast states.

intersite-shared

Syntax **intersite-shared**
no intersite-shared

Context config>service>vprn>mvpn

Description This command specifies whether to use inter-site shared C-trees or not.

Default intersite-shared

mdt-type

Syntax **mdt-type {**sender-receiver **|** sender-only **|** receiver-only}

Context config>service>vprn>mvpn

Description This command allows restricting MVPN instance per PE node to a specific role. By default, MVPN instance on a given PE node assumes the role of being a sender as well as receiver. This creates a mesh of MDT/PMSI across all PE nodes from this PE.

This command provides an option to configure either a sender-only or receiver only mode per PE node. Restricting the role of a PE node avoids creating full mesh of MDT/PMSI across all PE nodes that are participating in MVPN instance

The **no** version of this command restores the default (sender-receiver).

Default mdt-type sender-receiver

Parameters **sender-receiver —** MVPN has both sender and receivers connected to PE node

sender-only — MVPN has only senders connected to PE node

receiver-only — MVPN has only receivers connected to PE node

provider-tunnel

Syntax **provider-tunnel**

Context config>service>vprn>mvpn

Description This command enables context to configure tunnel parameters for the MVPN.

inclusive

Syntax **inclusive**

Context config>service>vprn>mvpn>pt

Description This command enables the context for specifying inclusive provider tunnels

mldp

Syntax **mldp**
no mldp

Context config>service>vprn>mvpn>provider-tunnel>inclusive

Description This command enables use of mLDP LSP for the provider tunnel.

Default no mldp

shutdown

Syntax **shutdown**
no shutdown

Context config>service>vprn>mvpn>provider-tunnel>inclusive>mldp

Description This command administratively disables and enables use of mLDP LSP for the provider tunnel.

Default no shutdown

pim

Syntax **pim** {**asm** | **ssm**} *grp-ip-address*
no pim

Context config>service>vprn>mvpn>pt>inclusive

Description This command specifies the PIM mode to use, ASM or SSM, for PIM-based inclusive provider tunnels and the multicast group address to use. Also enables the context for specifying parameters for PIM peering on the inclusive provider tunnel.

Note that auto-discovery must be enabled in order for SSM to operate.

The **no** form of the command removes the pim context including the statements under the context.

Default no pim

Parameters **asm** — Specifies to use PIM ASM for inclusive provider tunnels.

ssm — Specifies to u PIM SSM for inclusive provider tunnels.

group-address — Specifies the multicast group address to use.

hello-interval

Syntax **hello-interval** *hello-interval*
no hello-interval

Context config>service>vprn>mvpn>provider-tunnel>inclusive>pim

Description This command specifies the interval at which PIM hello messages are transmitted on the PIM inclusive provider tunnel.

The **no** form of this command reverts to the default value.

Default 30 seconds

Parameters *hello-interval* — Specifies the hello interval, in seconds. A 0 (zero) value disables the sending of hello messages.

Values 0 — 255

hello-multiplier

Syntax **hello-multiplier** *deci-units*
no hello-multiplier

Context config>service>vprn>mvpn>provider-tunnel>inclusive>pim

Description This command specifies the hello multiplier. The hello-multiplier in conjunction with the hello-interval determines the hold time for a PIM neighbor.

Hold time = (hello-interval * hello-multiplier) / 10.

The **no** form of the command reverts the value to the default.

Default 35

Parameters *deci-units* — Specifies the value, in multiples of 0.1, for the formula used to calculate the hold time

Values 20 — 100

improved-assert

Syntax [**no**] **improved-assert**

Context config>service>vprn>mvpn>provider-tunnel>inclusive>pim

Description This command enables improved assert procedure on the PIM inclusive provider tunnel.

The **no** form of the command disables improved assert procedure.

Default enabled

three-way-hello

Syntax [**no**] **three-way-hello**

Context config>service>vprn>mvpn>provider-tunnel>inclusive>pim

Description This command enables PIM three-way hello on the inclusive provider tunnel.

The no form of the command disables the PIM three-way hello.

Default disabled

tracking-support

Syntax [**no**] **tracking-support**

Context config>service>vprn>mvpn>provider-tunnel>inclusive>pim

Description This command enables the setting of the T bit in the LAN Prune Delay option of the hello message. This indicates the router's capability to disable Join message suppression.

The no form of the command disables the setting.

Default disabled

rsvp

Syntax **rsvp**
no rsvp

Context config>service>vprn>mvpn>provider-tunnel>inclusive

Description This command enables the context for specifying RSVP P2MP LSP for the provider tunnel. The **no** form of the command removes the rsvp context including all the statements in the context.

Default no rsvp

enable-bfd-root

Syntax **enable-bfd-root** [**transmit-interval**] [**multiplier** *multiplier*]
no enable-bfd-root

Context config>service>vprn>mvpn>provider-tunnel>inclusive>rsvp

Description This command enables unidirectional multi-point BFD session on a sender (Root) PE node for upstream fast failure detection over RSVP-TE P2MP LSP.

Parameters **transmit-interval —** Sets the transmit interval, in milliseconds.

Default 100

Values 10 — 100,000

multiplier *multiplier* — Sets the multiplier for the BFD session.

Default 3

Values 3 — 20

enable-bfd-leaf

Syntax [**no**] **enable-bfd-leaf**

Context config>service>vprn>mvpn>provider-tunnel>inclusive>rsvp

Description This command enables unidirectional multi-point BFD session on a receiver (leaf) PE node for upstream fast failure detection over RSVP-TE P2MP LSP.

lsp-template

Syntax **lsp-template**
no lsp-template

Context Context config>service>vprn>mvpn>provider-tunnel>inclusive>rsvp

Description This command specifies the use of automatically created P2MP LSP as the provider tunnel. The P2MP LSP will be signaled using the parameters specified in the template, such as bandwidth constraints, etc.

Default none

shutdown

Syntax **shutdown**
no shutdown

Context config>service>vprn>mvpn>provider-tunnel>inclusive>rsvp>lsp-template

Description This command administratively disables and enables use of RSVP P2MP LSP for the provider tunnel.

Default no shutdown

selective

Syntax **selective**

Context config>service>vprn>mvpn>provider-tunnel

Description This command enables the context to specify selective provider tunnel parameters.

Default none

auto-discovery-disable

Syntax [**no**] **auto-discovery-disable**

Context config>service>vprn>mvpn>provider-tunnel>selective

Description This command disables C-trees to P-tunnel binding auto-discovery through BGP so it is signaled using PIM join TLVs.

This command requires the **c-mcast-signaling** parameter to be set to PIM.

The **no** form of the command enables multicast VPN membership auto-discovery through BGP.

Default no auto-discovery-disable

data-delay-interval

Syntax **data-delay-interval** *value*
no data-delay-interval

Context config>service>vprn>mvpn>provider-tunnel>selective

Description This command specifies the interval, in seconds, before a PE router connected to the source switches traffic from the inclusive provider tunnel to the selective provider tunnel.

The no form of the command reverts the value to the default.

Default 3 seconds

Parameters *value* — Specifies the data delay interval, in seconds.

Values 3 — 180

data-threshold

Syntax **data-threshold** {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*} *s-pmsi-threshold*
data-threshold *c-grp-ipv6-addr/prefix-length s-pmsi-threshold*
no data-threshold {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*}
no data-threshold *c-grp-ipv6-addr/prefix-length*

Context config>service>vprn>mvpn>provider-tunnel>selective

Description This command specifies the data rate threshold that triggers the switch from the inclusive provider tunnel to the selective provider tunnel for C-(S,G) within the group range. Multiple statements are allowed in the configuration.

The **no** form of the command removes the values from the configuration.

Default none

Parameters *group-address/mask* — Specifies a multicast group address and netmask length.

c-grp-ip-addr/mask | *c-grp-ip-addr netmask* — Specifies an IPv4 multicast group address and netmask length or network mask.

c-grp-ipv6-addr/prefix-length — Specifies an IPv6 multicast group address and prefix length.

s-pmsi-threshold — Specifies the rate, in kilobits per second (kbps). If the rate for a C-(S,G) within the specified group range exceeds the threshold, traffic for the C-(S,G) will be switched to the selective provider tunnel.

Values

c-grp-ip-addr	: multicast group address a.b.c.d
mask	[4..32]
netmask	: a.b.c.d (network bits all 1 and host bits all 0)
s-pmsi-threshold	: [1..4294967294](threshold in kbps)
c-grp-ipv6-addr	: multicast ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x [0..FFFF]H d [0..255]D
prefix-length	[1..128]

join-tlv-packing-disable

Syntax [**no**] **join-tlv-packing-disable**

Context config>service>vprn>mvpn>provider-tunnel>selective>pim

Description This command enables packing of MDT join TLVs into a single PDU to improve efficiency, if multiple Join TLVs are available at the time of transmission.

The no form of the command disables packing of MDT join TLVs into a single PDU.

Default no join-tlv-packing-disable

pim-asm

Syntax [**no**] **pim-asm** {*grp-ip-address/mask* | *grp-ip-address netmask*}

Context config>service>vprn>mvpn>provider-tunnel>selective

Description This command specifies the range of PIM-ASM groups to use on the sender PE to setup ASM multicast tree for draft Rosen based Data MDT.

rsvp

Syntax **[no] rsvp**

Context config>service>vprn>mvpn>provider-tunnel>inclusive
config>service>vprn>mvpn>provider-tunnel>selective

Description This command enables use of P2MP RSVP as inclusive or selective provider tunnel.

Default no rsvp

lsp-template

Syntax **[no] lsp-template** *lsp-template-name*

Context config>service>vprn>mvpn>provider-tunnel>inclusive
config>service>vprn>mvpn>provider-tunnel>selective>rsvp

Description This command specifies the use of automatically created P2MP LSP as the inclusive or selective provider tunnel. The P2MP LSP will be signaled using the parameters specified in the template, such as bandwidth constraints, etc.

Default no lsp-template

mldp

Syntax **[no] mldp**

Context config>service>vprn>mvpn>provider-tunnel>inclusive
config>service>vprn>mvpn>provider-tunnel>selective

Description This command enables use of P2MP mLDP LSP as inclusive or selective PMSI tunnels.

Default no mldp

maximum-p2mp-spmsi

Syntax [**no**] **maximum-p2mp-spmsi**

Context config>service>vprn>mvpn>provider-tunnel>selective

Description This command specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnels for the mVPN. Once the limit is reached, no more RSVP P2MP S-PMSI or LDP P2MP S-PMSI is created and traffic over the data-threshold will stay on I-PMSI.

Default 10

Parameters *number* — specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnel for the mVPN.

Values 1-4k

Default 10

shutdown

Syntax [**no**] **shutdown**

Context config>service>vprn>mvpn>provider-tunnel>inclusive>rsvp>lsp-template
config>service>vprn>mvpn>provider-tunnel>inclusive>mldp
config>service>vprn>mvpn>provider-tunnel>selective>rsvp>lsp-template
config>service>vprn>mvpn>provider-tunnel>selective>mldp

Description This command administratively disables/enables use of P2MP RSVP LSP template or mLDP LSP for inclusive or selective PMSI tunnels.

Default no shutdown

enable-asm-mdt

Syntax [**no**] **enable-asm-mdt**

Context config>service>vprn>mvpn>provider-tunnel>selective

Description This command enables Data MDT with PIM-ASM mode on the receiver PE node. PIM-ASM or PIM-SSM operation mode is derived based on the locally configured SSM range on the node.

If asm-mode is disabled using this command, then PIM-SSM mode is enabled for all groups, independent of the configured SSM range on the node.

pim-ssm

Syntax **pim-ssm** {*grp-ip-address/mask* | *grp-ip-address netmask*}
no pim-ssm

Context config>service>vprn>mvpn>provider-tunnel>selective

Description This command specifies the PIM SSM groups to use for the selective provider tunnel.

Parameters *group-address/mask* — Specifies a multicast group address and netmask length.

umh-pe-backup

Syntax **umh-pe-backup**

Context config>service>vprn>mvpn

Description This command enables context to configure primary and standby upstream PE association for the MVPN.

umh-pe

Syntax **umh-pe** *ip-address* **standby** *ip-address*
no umh-pe *ip-address*

Context config>service>vprn>mvpn>umh-pe-backup

Description This command assigns a standby PE to each primary PE that must be selected as an alternative PE in case the UFD session on tunnel from primary PE is detected down. Standby for a PE cannot be modified without shutting down the MVPN instance.

If a primary PE is not assigned a standby PE then the UMH selection would fall back to the default method.

umh-selection

Syntax **umh-selection** {**highest-ip**|**hash-based**|**tunnel-status**|**unicast-rt-pref**}
no umh-selection

Context config>service>vprn>mvpn

Description This command specifies which UMH selection mechanism to use, highest IP address, hash based or provider tunnel status.

The **no** form of the command resets it back to default.

Default umh-selection highest-ip

Parameters **highest-ip —** Specifies that the highest IP address is selected as UMH.

hash-based — Specifies that the UMH selection is based on the hash based procedures.

tunnel-status — Specifies that UMH selection is based on the state of the tunnel as well as the available unicast routes through the tunnel.

unicast-rt-pref — When selected, best unicast route will decide which UMH is chosen. Note that, all PE routers shall prefer the same route to the UMH for the UMH selection criterion (for example BGP path selection criteria must not influence one PE to choose different UMH from another PE).

vrf-export

Syntax **vrf-export** {**unicast** | *policy-name* [*policy-name*...(up to 16 max)]}
no vrf-export

Context config>service>vprn>mvpn

Description This command specifies the export policy (up to 16) to control MVPN routes exported from the local VRF to other VRFs on the same or remote PE routers.

Default vrf-export unicast

Parameters **unicast —** Specifies to use unicast VRF export policy for the MVPN.

policy — Specifies a route policy name.

vrf-import

Syntax **vrf-import** {**unicast** | *policy-name* [*policy-name*...(up to 16 max)]}
no vrf-import

Context config>service>vprn>mvpn

Description This command specifies the import policy (up to 16) to control MVPN routes imported to the local VRF from other VRFs on the same or remote PE routers.

Default vrf-import unicast

Parameters **unicast —** Specifies to use a unicast VRF import policy for the MVPN.

policy — Specifies a route policy name.

vrf-target

Syntax **vrf-target** {**unicast** | *ext-community* | **export unicast** | *ext-community* | **import unicast** | *ext-community*}
no vrf-target

Context config>service>vprn>mvpn

Description This command specifies the route target to be added to the advertised routes or compared against the received routes from other VRFs on the same or remote PE routers. vrf-import or vrf-export policies override the vrf-target policy.

The **no** form of the command removes the vrf-target.

Default no vrf-target

Parameters **unicast —** Specifies to use unicast vrf-target ext-community for the multicast VPN.

ext-comm — An extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values target:{*ip-address*:*comm-val* |*2byte-asnumber:ext-comm-val*|*4byte-asnumber:comm-val*}

ip-address:	a.b.c.d
comm-val:	0 — 65535
2byte-asnumber:	1 — 65535
4byte-asnumber	0 — 4294967295

import *ext-community* **—** Specify communities allowed to be accepted from remote PE neighbors.

export *ext-community* **—** Specify communities allowed to be sent to remote PE neighbors.

export

Syntax **export** {**unicast** | *ext-community*}

Context config>service>vprn>mvpn>vrf-target

Description This command specifies communitities to be sent to peers.

Parameters **unicast —** Specifies to use unicast vrf-target ext-community for the multicast VPN.

ext-comm — An extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values target:{*ip-address*:*comm-val* |*2byte-asnumber:ext-comm-val*|*4byte-asnumber:comm-val*}

ip-address:	a.b.c.d
comm-val:	0 — 65535

2byte-asnumber:	1 — 65535
4byte-asnumber	0 — 4294967295

import

Syntax **import** {**unicast** | *ext-community*}

Context config>service>vprn>mvpn>vrf-target

Description This command specifies communitities to be accepted from peers.

Parameters **unicast —** Specifies to use unicast vrf-target ext-community for the multicast VPN.

ext-comm — An extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values target:{*ip-address*:*comm-val* |*2byte-asnumber:ext-comm-val*|*4byte-asnumber:comm-val*}

ip-address:	a.b.c.d
comm-val:	0 — 65535
2byte-asnumber:	1 — 65535
4byte-asnumber	0 — 4294967295

Network Time Protocol Commands

ntp

Syntax [**no**] **ntp**

Context config>service>vprn

Description This command enables the context to configure Network Time Protocol (NTP) and its operation. This protocol defines a method to accurately distribute and maintain time for network elements. Furthermore this capability allows for the synchronization of clocks between the various network elements. Use the no form of the command to stop the execution of NTP and remove its configuration.

Default none

authenticate

Syntax [**no**] **authenticate**

Context config>service>vprn>ntp

Description This command enables authentication for the NTP server.

authentication-check

Syntax [**no**] **authentication-check**

Context config>service>vprn>ntp

Description This command provides the option to skip the rejection of NTP PDUs that do not match the authentication key-id, type or key requirements. The default behavior when authentication is configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key-id, type or key.

When **authentication-check** is enabled, NTP PDUs are authenticated on receipt. However, mismatches cause a counter to be increased, one counter for type and one for key-id, one for type, value mismatches. These counters are visible in a show command.

The **no** form of this command allows authentication mismatches to be accepted; the counters however are maintained.

Default authentication-check — Rejects authentication mismatches.

authentication-key

Syntax **authentication-key** *key-id* {**key** *key*} [**hash** | **hash2**] **type** {**des** | **message-digest**}
no authentication-key *key-id*

Context config>service>vprn>ntp

Description This command sets the authentication key-id, type and key used to authenticate NTP PDUs sent to or received by other network elements participating in the NTP protocol. For authentication to work, the authentication key-id, type and key value must match.

The **no** form of the command removes the authentication key.

Default none

Parameters *key-id* — Configure the authentication key-id that will be used by the node when transmitting or receiving Network Time Protocol packets.

Entering the authentication-key command with a key-id value that matches an existing configuration key will result in overriding the existing entry.

Recipients of the NTP packets must have the same authentication key-id, type, and key value in order to use the data transmitted by this node. This is an optional parameter.

Default None

Values 1 — 255

key — The authentication key associated with the configured key-id, the value configured in this parameter is the actual value used by other network elements to authenticate the NTP packet.

The key can be any combination of ASCII characters up to 8 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash — Specifies the key is entered in an encrypted form. If the hash or hash2 parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables then the key value alone, this means that hash2 encrypted variable can’t be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

type — This parameter determines if DES or message-digest authentication is used.

This is a required parameter; either DES or message-digest must be configured.

Values des — Specifies that DES authentication is used for this key
message-digest — Specifies that MD5 authentication in accordance with RFC 2104 is used for this key.

broadcast

Syntax **broadcast** {**interface** *ip-int-name*} [**key-id** *key-id*] [**version** *version*] [**ttl** *ttl*]
no broadcast {**interface** *ip-int-name*}

Context config>service>vprn>ntp

Description This command configures the node to transmit NTP packets on a given interface. Broadcast and multicast messages can easily be spoofed, thus, authentication is strongly recommended.

The **no** form of this command removes the address from the configuration.

Parameters *ip-int-name* — Specifies the local interface on which to transmit NTP broadcast packets. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 32 character maximum

key-id *key-id* **—** Identifies the configured authentication key and authentication type used by this node to receive and transmit NTP packets to and from an NTP server and peers. If an NTP packet is received by this node both authentication key and authentication type must be valid otherwise the packet will be rejected and an event/trap generated.

Values 1 — 255

Default none

version *version* **—** Specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all versions will be accepted.

Values 1 — 4

Default 4

ttl *ttl* **—** Specifies the IP Time To Live (TTL) value.

Values 1 — 255

Default none

Redundant Interface Commands

redundant-interface

Syntax [**no**] **redundant-interface** *ip-int-name*

Context config>service>vprn

Description This command configures a redundant interface.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

address

Syntax **address** {*ip-address/mask* | *ip-address netmask*} [**remote-ip** *ip-address*]
no address

Context config>service>vprn>redundant-interface

Description This command assigns an IP address mask or netmask and a remote IP address to the interface.

Parameters *ip-address/mask* — Assigns an IP address/IP subnet format to the interface.

ip-address netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

Assigns an IP address netmask to the interface.

remote-ip *ip-address* — Assigns a remote IP to the interface.

SDP Commands

spoke-sdp

Syntax [**no**] **spoke-sdp** *sdp-id*

Context config>service>vprn

Description This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge "port" where flooded traffic received on the spoke SDP is replicated on all other "ports" (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a VPRN service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end 7750 SR devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default No *sdp-id* is bound to a service.

Special Cases **VPRN —** Several SDPs can be bound to a VPRN service. Each SDP must be destined to a different 7750 SR router. If two *sdp-id* bindings terminate on the same 7750 SR, an error occurs and the second SDP binding is rejected.

Parameters *sdp-id* — The SDP identifier. Allowed values are integers in the range of 1 and 17407 for existing SDPs.

vc-id — The virtual circuit identifier.

Values 1 — 4294967295

spoke-sdp

Syntax **spoke-sdp** *sdp-id* [:*vc-id*] *vc-type* {**ether**|**ipipe**} [**create**]
no spoke-sdp *sdp-id* [:*vc-id*] *vc-type* {**ether**|**ipipe**} [**create**]

Context config>service>vprn>if

Description This command binds a service to an existing Service Distribution Point (SDP).

A spoke SDP is treated like the equivalent of a traditional bridge "port" where flooded traffic received on the spoke SDP is replicated on all other "ports" (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end 7750 SR devices can participate in the service.

Class-based forwarding is not supported on a spoke SDP used for termination on an IES or VPRN services. All packets are forwarded over the default LSP.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default none

Special Cases **VPRN —** Several SDPs can be bound to a VPRN service. Each SDP must be destined to a different 7750 SR router. If two sdp-id bindings terminate on the same 7750 SR, an error occurs and the second SDP is binding is rejected.

sdp-id — The SDP identifier.

Values 1 — 17407

vc-id — The virtual circuit identifier.

Values 1 — 4294967295

vc-type — The encapsulation and pseudowire type for the spoke SDP.

Values ether—Ethernet pseudowire.
ipipe—IP pseudowire.

Default ether

egress

Syntax **egress**

Context config>service>vprn>if>spoke-sdp
config>service>vprn>red-if>spoke-sdp

Description This command configures an SDP context.

hash-label

Syntax [**no**] **hash-label**

Context config>service>vprn
config>service>vprn>spoke-sdp
config>service>vprn>if>spoke-sdp

Description This command enables the use of the hash label on a VLL, VPLS, or VPRN service bound to LDP or RSVP SDP as well as to a VPRN service using the autobind mode with the with the ldp, rsvp-te, or mpls options. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option..

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to 1 to indicate that.

In order to allow for applications whereby the egress LER infers the presence of the Hash Label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label will always be in the range [524,288 - 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note however that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets that are generated in CPM and forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The **no** form of this command disables the use of the hash label.

Default no hash-label

ingress

Syntax **ingress**

Context config>service>vprn>if>spoke-sdp
config>service>vprn>red-if>spoke-sdp

Description This command configures the SDP context.

qos

Syntax **qos** *network-policy-id* **fp-redirect-group** *queue-group-name* **instance** *instance-id*
no qos

Context configure>service>apipe>spoke-sdp>ingress
configure>service>cpipe>spoke-sdp>ingress
configure>service>epipe>spoke-sdp>ingress
configure>service>fpipe>spoke-sdp>ingress
configure>service>ipipe>spoke-sdp>ingress
config>service>vpls>spoke-sdp>ingress
config>service>vpls>mesh-sdp>ingress
config>service>pw-template>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>ies>interface>spoke-sdp>ingress

Description This command is used to redirect pseudowire packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress pseudowire rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more pseudowires to the same instance of policers, which are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress pseudowire shaping feature consists of the following steps:

1. Create an ingress queue-group template and configure policers for each FC that needs to be redirected and optionally, for each traffic type (unicast or multicast).
2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface to which the pseudowire packets can be received. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.
3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the ingress context of a spoke-SDP inside a service, or to the ingress context of a pseudowire template, and specify the redirect queue-group name.
5. One or more spoke-SDPs can have their FCs redirected to use policers in the same policer queue-group instance.

The following are the constraints and rules of this provisioning model when used in the ingress pseudowire rate-limiting feature:

1. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.
2. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the

association is failed at the time the user associates the ingress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

3. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   a When a pseudowire packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per-FP ingress shared queues referred to as *policer-output-queues*.
   b When a pseudowire packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the pseudowire packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.
4. If a network QoS policy is applied to the ingress context of a pseudowire, any pseudowire FC which is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.
5. If no network QoS policy is applied to the ingress context of the pseudowire, then all packets of the pseudowire will feed:
   a the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP. This is the default behavior.
   b a queue-group policer followed by the per-FP ingress shared queues referred to as *policer-output-queues* if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group (csc-policing). The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from an R-VPLS spoke-SPD, which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP is used.

When a pseudowire is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the pseudowire. This is true regardless of wether an instance of the named policer queue-group exists on the ingress FP on which the pseudowire packet is received. The user can apply a QoS filter matching the dot1.p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload IP header if the user enabled the **ler-use-dscp** option and the pseudowire terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface on which the pseudowire packet is received.

The **no** version of this command removes the redirection of the pseudowire to the queue-group.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 — 65535

fp- redirect-group *queue-group-name* **—** Specifies the name of the queue group template up to 32 characters in length.

ingress-instance *instance-id* **—** Specifies the identification of a specific instance of the queue-group.

Values 1 — 16384

vc-label

Syntax **vc-label** *egress-vc-label*
no vc-label [*egress-vc-label*]

Context config>service>vprn>if>spoke-sdp>egress
config>service>vprn>red-if>spoke-sdp>egress

Description This command configures the egress VC label.

Parameters *vc-label* — A VC egress value that indicates a specific connection.

Values 16 — 1048575

vc-label

Syntax **vc-label** *ingress-vc-label*
no vc-label [*ingress-vc-label*]

Context config>service>vprn>if>spoke-sdp>ingress
config>service>vprn>red-if>spoke-sdp>ingress

Description This command configures the ingress VC label.

Parameters *vc-label* — A VC ingress value that indicates a specific connection.

Values 2048 — 18431

egress

Syntax **egress**

Context config>service>vprn>network-interface

Description This command enables the context to configure egress network filter policies for the interface.

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
no filter [**ip** *ip-filter-id*] [**ipv6** *ipv6-filter-id*]

Context config>service>vprn>network-interface>egress
config>service>vprn>if>spoke-sdp>egress
config>service>vprn>if>spoke-sdp>ingress
config>service>vprn>red-if>spoke-sdp>ingress
config>service>vprn>red-if>spoke-sdp>egress
config>service>vprn>nw-if>egress

Description This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface. An IP filter policy can be associated with spoke SDPs. Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria.

The filter command is used to associate a filter policy with a specified ip-filter-id with an ingress or egress SAP. The ip-filter-id must already be defined before the filter command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use scope command within the filter definition to change the scope to local or global. The default scope of a filter is local.

Parameters **ip** *ip-filter-id* — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 — 65535

qos

Syntax **qos** *network-policy-id* **port-redirect-group** *queue-group-name* [**instance** *instance-id*]
no qos [*network-policy-id*]

Context configure>service>apipe>spoke-sdp>egress
configure>service>cpipe>spoke-sdp>egress
configure>service>epipe>spoke-sdp>egress
configure>service>fpipe>spoke-sdp>egress
configure>service>ipipe>spoke-sdp>egress
config>service>vpls>spoke-sdp>egress
config>service>vpls>mesh-sdp>egress
config>service>pw-template>egress
config>service>vprn>interface>spoke-sdp>egress
config>service>ies>interface>spoke-sdp>egress

Description This command is used to redirect pseudowire packets to an egress port queue-group for the purpose of shaping.

The egress pseudowire shaping provisioning model allows the mapping of one ore more pseudowires to the same instance of queues, or policers and queues, which are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only or policers and queues for each FC that needs to be redirected.
2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface on which the pseudowire packets can be forwarded. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the egress context of a spoke-SPD inside a service or to the egress context of a pseudowire template and specify the redirect queue-group name.

One or more spoke-SPDs can have their FCs redirected to use queues only or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:

1. When a pseudowire FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface on which the pseudowire packet is forwarded. This queue can be a queue-group queue, or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a pseudowire packet.
2. When a pseudowire FC is redirected to use a queue or a policer, and a queue in a queue-group and the queue-group name exists, but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the pseudowire packet is forwarded on.
3. When a pseudowire FC is redirected to use a queue, or a policer and a queue in a queue-group, and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports which have network IP interfaces. The handling of this is dealt with in the data path as follows:
    a When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.
    b When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the pseudowire packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

4. If a network QoS policy is applied to the egress context of a pseudowire, any pseudowire FC, which is not explicitly redirected in the network QoS policy, will have the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the pseudowire is redirected to exists and the redirection succeeds, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP is performed; according to the relevant mappings of the (FC, profile) in the egress context of the network QoS policy applied to the pseudowire. This is true regardless, wether an instance of the queue-group exists or not on the egress port to which the pseudowire packet is forwarded. If the packet profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet DEI/dot1.p and the tunnel DEI/dot1.p/EXP, but the DSCP is not modified by the policer operation.

When the queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface to which the pseudowire packet is forwarded.

The **no** version of this command removes the redirection of the pseudowire to the queue-group.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 — 65535

port-redirect-group *queue-group-name* **—** This optional parameter specifies that the *queue-group-name* will be used for all egress forwarding class redirections within the network QoS policy ID. The specified *queue-group-name* must exist as a port egress queue group on the port associated with the IP interface.

egress-instance *instance-id* **—** Specifies the identification of a specific instance of the queue-group.

Values 1 — 16384

Interface Commands

interface

Syntax **interface** *ip-int-name*
no interface *ip-int-name*

Context config>service>vprn

Description This command creates a logical IP routing interface for a Virtual Private Routed Network (VPRN). Once created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.

The **interface** command, under the context of services, is used to create and maintain IP routing interfaces within VPRN service IDs. The **interface** command can be executed in the context of an VPRN service ID. The IP interface created is associated with the service core network routing instance and default routing table. The typical use for IP interfaces created in this manner is for internet access.

Interface names are case sensitive and must be unique within the group of defined IP interfaces defined for **config router interface** and **config service vprn interface**. Interface names must not be in the dotted decimal notation of an IP address. For example, the name "1.1.1.1" is not allowed, but "int-1.1.1.1" is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.

The available IP address space for local subnets and routes is controlled with the **config router service-prefix** command. The **service-prefix** command administers the allowed subnets that can be defined on service IP interfaces. It also controls the prefixes that may be learned or statically defined with the service IP interface as the egress interface. This allows segmenting the IP address space into **config router** and **config service** domains.

When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, there are no default IP interface names defined within the system. All VPRN IP interfaces must be explicitly defined. Interfaces are created in an enabled state.

The **no** form of this command removes IP the interface and all the associated configuration. The interface must be administratively shutdown before issuing the **no interface** command.

For VPRN services, the IP interface must be shutdown before the SAP on that interface may be removed. VPRN services do not have the **shutdown** command in the SAP CLI context. VPRN service SAPs rely on the interface status to enable and disable them.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and config service vprn interface commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If *ip-int-name* already exists within the service ID, the context will be changed to maintain that IP interface. If *ip-int-name* already exists within another service ID or is an IP interface defined within the **config router** commands, an error will occur and context will not be changed to that IP interface. If *ip-int-name* does not exist, the interface is created and context is changed to that interface for further command processing.

active-cpm-protocols

Syntax [**no**] **active-cpm-protocols**

Context config>service>vprn>if

Description This command enables CPM protocols on this interface.

address

Syntax **address** *ip-address/mask* | *ip-address netmask*} [**broadcast** [**all-ones** | **host-ones**]
no address

Context config>service>vprn>if
config>service>vprn>nw-if

Description Assigns an IP address, IP subnet, and broadcast address format to a VPRN IP router interface. Only one IP address can be associated with an IP interface.

An IP address must be assigned to each VPRN IP interface. An IP address and a mask are used together to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the 7750 SR.

The local subnet that the **address** command defines must be part of the services address space within the routing context using the **config router service-prefix** command. The default is to disallow the complete address space to services. Once a portion of the address space is allocated as a service prefix, that portion can be made unavailable for IP interfaces defined within the **config router interface** CLI context for network core connectivity with the **exclude** option in the **config router service-prefix** command.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

Use the **no** form of this command to remove the IP address assignment from the IP interface. When the **no address** command is entered, the interface becomes operationally down.

Address	Admin state	Oper state
No address	up	down
No address	down	down
1.1.1.1	up	up
1.1.1.1	down	down

The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an adminstratively up state and an address is assigned, it becomes operationally up and the protocol interfaces and the MPLS LSPs associated with that IP interface will be reinitialized.

ip-address — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

/ — The forward slash is a parameter delimiter and separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-address*, the "/" and the *mask-length* parameter. If a forward slash is not immediately following the *ip-address*, a dotted decimal mask must follow the prefix.

mask-length — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-address* from the *mask-length* parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. Allowed values are integers in the range 0 – 30. Note that a mask length of 32 is reserved for system IP addresses.

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that will be used in a logical 'AND' function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

broadcast — The optional **broadcast** parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is **host-ones** which indictates a subnet broadcast address. Use this parameter to change the broadcast address to **all-ones** or revert back to a broadcast address of **host-ones**.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed.

This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (**all-ones**) or the valid subnet broadcast address (**host-ones**) will be received by the IP interface.

Default host-ones

all-ones — The **all-ones** keyword following the **broadcast** parameter specifies the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

host-ones — The **host-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and the *mask-length* or *mask* with all the host bits set to binary one. This is the default broadcast address used by an IP interface.

The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

allow-directed-broadcasts

Syntax [**no**] **allow-directed-broadcasts**

Context config>service>vprn>if
config>service>vprn>nw-if

Description This command controls the forwarding of directed broadcasts out of the IP interface.

A directed broadcast is a packet received on a local router interface destined for the subnet broadcast address on another IP interface. The **allow-directed-broadcasts** command on an IP interface enables or disables the transmission of packets destined to the subnet broadcast address of the egress IP interface.

When enabled, a frame destined to the local subnet on this IP interface will be sent as a subnet broadcast out this interface. Care should be exercised when allowing directed broadcasts as it is a well-known mechanism used for denial-of-service attacks.

When disabled, directed broadcast packets discarded at this egress IP interface will be counted in the normal discard counters for the egress SAP.

By default, directed broadcasts are not allowed and will be discarded at this egress IP interface.

The **no** form of this command disables the forwarding of directed broadcasts out of the IP interface.

Default **no allow-directed-broadcasts** — Directed broadcasts are dropped.

bfd

Syntax **bfd** *transmit-interval* [**receive** *receive-interval*] [**multiplier** *multiplier*] [**echo-receive** *echo-interval*] [**type cpm-np**]
no bfd

Context config>service>vprn>if
config>service>vprn>if>ipv6
config>service>vprn>nw-if

Description This command specifies the BFD parameters for the associated IP interface. If no parameters are defined the default value are used.

The multiplier specifies the number of consecutive BFD messages that must be missed from the peer before the BFD session state is changed to down and the upper level protocols (OSPF, IS-IS, BGP or PIM) is notified of the fault.

The **no** form of the command removes BFD from the associated IGP protocol adjacency.

Important notes: On the 7750-SR, the *transmit-interval,* **receive** ***receive-interval***, and **echo-receive** *echo-interval* values can only be modified to a value less than 100 when:

1. The **type cpm-np option** is explicitly configured.
2. The service is shut down (**shutdown**)
3. The interval is specified 10 — 100000.
4. The service is re-enabled (**no shutdown**)

To remove the **type cpm-np** option, re-issue the **bfd** command without specifying the **type** parameter.

Default no bfd

Parameters *transmit-interval* — Sets the transmit interval for the BFD session.

Values 10 — 100000
10 — 100000 (see Important Notes above)

Default 100

receive ***receive-interval*** **—** Sets the receive interval for the BFD session.

Values 10 — 100000
10 — 100000 (see Important Notes above)

Default 100

multiplier ***multiplier*** **—** Set the multiplier for the BFD session.

Values 3— 20

Default 3

echo-receive *echo-interval* **—** Sets the minimum echo receive interval, in milliseconds, for the BFD session.

Values 100 — 100000
10 — 100000 (see Important Notes above)

Default 100

type cpm-np — Specifies that BFD sessions associated with this interface will be created on the CPM network processor to allow for fast timers down to 10ms granularity.

cflowd

Syntax **cflowd** {**acl** | **interface**} [**direction**]
no cflowd

Context config>service>vprn>if
config>service>vprn>nw-if

Description This command enables cflowd to collect traffic flow samples through a router for analysis.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When cflowd is enabled at the interface level, all packets forwarded by the interface are subjected to analysis according to the cflowd configuration.

If cflowd is enabled without either egress-only or both specified or with the ingress-only keyword specified, then only ingress sampling will be enabled on the associated IP interface.

Default no cflowd

Parameters **acl —** *cflowd* configuration associated with a filter.

interface — *cflowd* configuration associated with an IP interface.

direction — Specifies the direction to collect traffic flow samples.

Values ingress-only — Enables ingress sampling only on the associated interface.
egress-only — Enables egress sampling only on the associated interface.
both — Enables both ingress and egress cflowd sampling.

cpu-protection

Syntax **cpu-protection** *policy-id*
no cpu-protection

Context config>service>vprn>if
config>service>vprn>nw-if

Description This command assigns an existing CPU protection policy to the associated service interface. For these interface types, the per-source rate limit is not applicable.The CPU protection policies are configured in the **config>sys>security>cpu-protection>policy** *cpu-protection-policy-id* context.

If no CPU protection policy is assigned to a service interface, then a the default policy is used to limit the overall-rate.

The **no** form of the command removes CPU protection policy association from the interface, resulting in no default rate limiting of control packets.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

none (for video-interfaces (where applicable), shown as **no cpu-protection** in CLI)

The configuration of **no cpu-protection** returns the interface/SAP to the default policies as shown above.

Parameters *policy-id* — Specifies an existing CPU protection policy.

Values 1 — 255

cpu-protection

Syntax **cpu-protection** *policy-id* [**mac-monitoring**]
no cpu-protection

Context config>service>vprn>if
config>service>vprn>if>sap

Description This command assigns an existing CPU protection policy to the associated service group interface SAP, interface or MSAP policy. The CPU protection policies are configured in the **config>sys>security>cpu-protection>policy** *cpu-protection-policy-id* context.

If no CPU protection policy is assigned to a service group interface SAP, then a the default policy is used to limit the overall-rate.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

none (for video-interfaces (where applicable), shown as **no cpu-protection** in CLI)

The configuration of **no cpu-protection** returns the interface/SAP to the default policies as shown above.

Parameters *policy-id* — Specifies an existing CPU protection policy.

Values 1 — 255

mac-monitoring — When specified, the per MAC rate limiting should be performed, using the per-source-rate from the associated cpu-protection policy.

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context config>service>vprn>if>nw-if

Description This command assigns a Distributed CPU Protection (DCP) policy to the network interface. Only a valid created DCP policy can be assigned to a SAP or a network interface (note that this rule does not apply to templates such as an msap-policy)

Default no dist-cpu-protection

delayed-enable

Syntax **delayed-enable** *seconds*
no delayed-enable

Context config>service>vprn>if

Description This command creates a delay to make the interface operational by the specified number of seconds

The value is used whenever the system attempts to bring the interface operationally up.

Parameters *seconds* — Specifies a delay, in seconds, to make the interface operational.

Values 1 — 1200

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context config>service>vprn>if

Description This command configures the IP maximum transmit unit (packet) for this interface.
The **no** form of the command returns the default value.

Default no ip-mtu

ipcp

Syntax **ipcp**

Context config>service>vprn>if

Description This command creates allows access to the IPCP context within the interface configuration. Within this context, IPCP extensions can be configured to define such things as the remote IP address and DNS IP address to be signaled via IPCP on the associated PPP interface.

This command is only applicable if the associated SAP/port is a PPP/MLPPP interface.

Default none

dns

Syntax **dns ip-address** [**secondary** *ip-address*]
dns secondary *ip-address*
no dns [*ip-address*] [**secondary** *ip-address*]

Context config>service>vprn>if>ipcp

Description This command defines the dns address(es) to be assigned to the far-end of the associated PPP/MLPPP link via IPCP extensions.

This command is only applicable if the associated SAP/port is a PPP/MLPPP interface with an IPCP encapsulation.

The **no** form of the command deletes either the specified primary DNS address, secondary DNS address or both addresses from the IPCP extension peer-ip-address configuration.

Default no dns

Parameters *ip-address* — This parameter specifies a unicast IPv4 address for the primary DNS server to be signaled to the far-end of the associate PPP/MLPPP link via IPCP extensions.

secondary *ip-address* — This parameter specifies a unicast IPv4 address for the secondary DNS server to be signaled to the far-end of the associate PPP/MLPPP link via IPCP extensions.

peer-ip-address

Syntax **peer-ip-address** *ip-address*
no peer-ip-address

Context config>service>vprn>if>ipcp

Description This command defines the remote IP address to be assigned to the far-end of the associated PPP/MLPPP link via IPCP extensions.

This command is only applicable if the associated SAP/port is a PPP/MLPPP interface with an IPCP encapsulation.

The interface must be shut down to modify the IPCP configuration.

The **no** form of the command deletes the IPCP extension peer-ip-address configuration.

Default no peer-ip-address (0.0.0.0)

Parameters *ip-address* — Specifies a unicast IPv4 address to be signaled to the far-end of the associated PPP/MLPPP link by IPCP extensions.

ipv6

Syntax [**no**] **ipv6**

Context config>service>vprn>if

Description This command configures an IPv6 interface.

address

Syntax **address** *ipv6-address/mask* [**eui-64**] [**preferred**]
no address *ipv6-address/prefix-length*

Context config>service>vprn>if>ipv6

Description This command assigns an IPv6 address to the VPRN interface.

Parameters *ipv6-address/prefix-length* — Specifies the IPv6 address on the interface.

Values

ipv6-address/prefix:	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x [0 — FFFF]H d [0 — 255]D
	prefix-length	1 — 128

eui-64 — When the **eui-64** keyword is specified, a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. The 64-bit interface identifier is derived from MAC address on Ethernet interfaces. For interfaces without a MAC address, for example ATM interfaces, the Base MAC address of the chassis is used.

preferred — specifies that the IPv6 address is the preferred IPv6 address for this interface. Preferred address is an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses maybe used as the source (or destination) address of packets sent from (or to) the interface. Preferred address doesn't go through the DAD process.

dhcp6-relay

Syntax [**no**] **dhcp6-relay**

Context config>service>vprn>if>ipv6

Description This command configures DHCPv6 relay parameters for the VPRN interface.

dhcp6-server

Syntax [**no**] dhcp6-server

Context config>service>vprn>if>ipv6

Description This command configures DHCPv6 server parameters for the VPRN interface.

icmp6

Syntax **icmp6**

Context config>service>vprn>if>ipv6

Description This command configures ICMPv6 for the interface.

local-proxy-nd

Syntax [**no**] **local-proxy-nd**

Context config>service>vprn>if>ipv6

Description This command enables or disables neighbor discovery on the interface.

neighbor

Syntax **neighbor** *ipv6-address mac-address*

no neighbor *ipv6-address*

Context config>service>vprn>if>ipv6

Description This command configures IPv6-to-MAC address mapping on the interface.

Parameters *ipv6-address* — Specifies the IPv6 address on the interface.

Values ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0 — FFFF]H
d [0 — 255]D

mac-address — Specifies the 48-bit MAC address for the static ARP in the form *aa***:***bb***:***cc***:***dd***:***ee***:***ff* or *aa***-***bb***-***cc***-***dd***-***ee***-***ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

proxy-nd-policy

Syntax **proxy-nd-policy** *policy-name* [*policy-name*...*(up to 5 max*)]
no proxy-nd-policy

Context config>service>vprn>if>ipv6

Description This command configures a proxy neighbor discovery policy for the interface.

Parameters *policy-name* — Specifies the existing policy name(s).

local-proxy-arp

Syntax [**no**] **local-proxy-arp**

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command enables local proxy ARP. When local proxy ARP is enabled on an IP interface, the system responds to all ARP requests for IP addresses belonging to the subnet with its own MAC address, and thus will become the forwarding point for all traffic between hosts in that subnet. When local-proxy-arp is enabled, ICMP redirects on the ports associated with the service are automatically blocked.

Default no local-proxy-arp

loopback

Syntax [**no**] **loopback**

Context config>service>vprn>if
config>service>vprn>nw-if

Description This command specifies that the associated interface is a loopback interface that has no associated physical interface. As a result, the associated interface cannot be bound to a SAP.

When using mtrace/mstat in a Layer 3 VPN context then the configuration for the VPRN should have a loopback address configured which has the same address as the core instance's system address (BGP next-hop).

Default None

mac

Syntax [**no**] **mac** *ieee-mac-address*

Context config>service>vprn>if
config>service>vprn>if>vrrp
config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command assigns a specific MAC address to a VPRN IP interface.

The **no** form of this command returns the MAC address of the IP interface to the default value.

Default The physical MAC address associated with the Ethernet interface that the SAP is configured on.

Parameters *ieee-mac-address* — Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa*-*bb*-*cc*-*dd*-*ee*-*ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

ntp-broadcast

Syntax [**no**] **ntp-broadcast**

Context config>service>vprn>nw-if

Description This command enables receiving of NTP/SNTP broadcasts on the interface/

monitor-oper-group

Syntax **monitor-oper-group** *name*
no monitor-oper-group

Context config>service>vprn>if

Description This command specifies the operational group to be monitored by the object under which it is configured. The oper-group name must be already configured under the config>service context before its name is referenced in this command.

The **no** form of the command removes the association from the configuration.

Default no monitor-oper-group

Parameters *name* — Specifies a character string of maximum 32 ASCII characters identifying the group instance.

proxy-arp

Syntax [**no**] **proxy-arp**

Context config>service>vprn>nw-if

Description This command enables proxy ARP on the interface.

Default no proxy-arp

proxy-arp-policy

Syntax [**no**] **proxy-arp-policy** *policy-name* [*policy-name*...(up to 5 max)]

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command enables a proxy ARP policy for the interface.

The no form of this command disables the proxy ARP capability.

Default no proxy-arp

Parameters *policy-name* — The export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

qos-route-lookup

Syntax **qos-route-lookup** [**source** | **destination**]
no qos-route-lookup

Context config>service>vprn>if
config>service>vprn>if>ipv6
config>service>vprn>sub-if>group-interface
config>service>vprn>sub-if>grp-if>ipv6

Description This command enables QoS classification of the ingress IP packets on an interface based on the QoS information associated with routes in the forwarding table.

If the optional **destination** parameter is specified and the destination address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos

policy associated with the IP interface. If the destination address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network QoS policy.

If the optional **source** parameter is specified and the source address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the source address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network QoS policy.

If neither the optional **source** or **destination** parameter is present, then the default is **destination** address matching.

The functionality enabled by the qos-route-lookup command can be applied to IPv4 packets or IPv6 packets on an interface, depending on whether it is present at the interface context (applies to IPv4) or the interface>ipv6 context (applies to IPv6). The ability to specify source address based QoS lookup is not supported for IPv6.

The **no** form of the command reverts to the default.

Default destination

Parameters **source —** Enables QoS classification of incoming IP packets based on the source address matching a route with QoS information.

destination — Enables QoS classification of incoming IP packets based on the destination address matching a route with QoS information.

redundant-interface

Syntax **redundant-interface** *red-ip-int-name*
no redundant-interface

Context config>service>vprn
config>service>vprn>sub-if>grp-if

Description This command configures a redundant interface used for dual homing.

Parameters *red-ip-int-name* — Specifies the redundant IP interface name.

remote-proxy-arp

Syntax [**no**] **remote-proxy-arp**

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command enables remote proxy ARP on the interface.

Remote proxy ARP is similar to proxy ARP. It allows the router to answer an ARP request on an interface for a subnet that is not provisioned on that interface. This allows the router to forward to the

other subnet on behalf of the requester. To distinguish remote proxy ARP from local proxy ARP, local proxy ARP performs a similar function but only when the requested IP is on the receiving interface.

Default no remote-proxy-arp

secondary

Syntax **secondary** {*ip-address/mask* | *ip-address netmask*} [**broadcast all-ones** | **host-ones**] [**igp-inhibit**]
no secondary {*ip-address/mask* | *ip-address netmask*}

Context config>service>vprn>if
config>service>vprn>nw-if

Description This command assigns an secondary IP address/IP subnet/broadcast address format to the interface.

Default none

Parameters *ip-address* — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that will be used in a logical 'AND' function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

broadcast — The optional **broadcast** parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is **host-ones** which indictates a subnet broadcast address. Use this parameter to change the broadcast address to **all-ones** or revert back to a broadcast address of **host-ones**.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed. This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (**all-ones**) or the valid subnet broadcast address (**host-ones**) will be received by the IP interface. *(Default: host-ones)*

all-ones — The **all-ones** keyword following the **broadcast** parameter specifies the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

host-ones — The **host-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and the *mask-length* or *mask* with all the host bits set to binary one. This is the default used by an IP interface. The **broadcast** parameter within the **address** command does not have a negate feature, which is

usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

igp-inhibit — The optional **igp-inhibit** parameter signals that the given secondary IP interface should not be recognized as a local interface by the running IGP. For OSPF and IS-IS, this means that the specified secondary IP interfaces will not be injected and used as passive interfaces and will not be advertised as internal IP interfaces into the IGP's link state database. For RIP, this means that these secondary IP interfaces will not source RIP updates.

static-arp

Syntax **static-arp** *ieee-mac-address unnumbered*
no static-arp ***unnumbered***

Context config>service>vprn>if
config>service>vprn>nw-if

Description This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. This static ARP will appear in the core routing ARP table. A static ARP can only be configured if it exists on the network attached to the IP interface. If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address will be replaced with the new MAC address.

The **no** form of this command removes a static ARP entry.

Default none

Parameters *ip-address* — Specifies the IP address for the static ARP in IP address dotted decimal notation.

ieee-mac-address — Specifies the 48-bit MAC address for the static ARP in the form *aa***:***bb***:***cc***:***dd***:***ee***:***ff* or *aa***-***bb***-***cc***-***dd***-***ee***-***ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

unnumbered — Specifies the static ARP MAC for an unnumbered interface. Unnumbered interfaces support dynamic ARP. Once this command is configured, it overrides any dynamic ARP.

static-tunnel-redundant-next-hop

Syntax **static-tunnel-redundant-next-hop** *ip-address*
no static-tunnel-redundant-next-hop

Context config>service>vprn>if

Description This command specifies redundant next-hop address on public or private IPsec interface (with public or private tunnel-sap) for static IPsec tunnel. The specified next-hop address will be used by standby node to shunt traffic to master in case of it receives them.

The next-hop address will be resolved in routing table of corresponding service.

The no form of the command removes the address from the interface configuration.

Default none

Parameters *ip-address* — Specifies the static ISA tunnel redundant next-hop address.

strip-label

Syntax **[no] strip-label**

Context config>service>vprn>nw-if

Description This command forces packets to be stripped of all (max 5) MPLS labels before the packets are handed over for possible filter (PBR) processing.

If the packets do not have an IP header ediately following the MPLS label stack after the strip, they are discarded. Only MPLS encapsulated IP, IGP shortcuts and VPRN over MPLS packets will be processed.

This command is only supported on:

- Optical ports
- IOM3-XP cards
- Null/Dot1q encaps
- Network ports
- IPv4

The **no** form removes the strip-label command.

In order to associate an interface that is configured with the strip-label parameter with a port, the port must be configured as single-fiber for the command to be valid.

Default no strip-label

tos-marking-state

Syntax **tos-marking-state** {**trusted** | **untrusted**}
no tos-marking-state

Context config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command is used to alter the default trusted state to a non-trusted state. When unset or reverted to the trusted default, the ToS field will not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set, in which case the egress network interface treats all VPRN and network IP interface as untrusted.

When the ingress interface is set to untrusted, all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface. The egress network remarking rules also apply to the ToS field of IP packets routed using IGP shortcuts (tunneled to a remote next-hop). However, the tunnel QoS markings are always derived

from the egress network QoS definitions.
Egress marking and remarking is based on the internal forwarding class and profile state of the packet once it reaches the egress interface. The forwarding class is derived from ingress classification functions. The profile of a packet is either derived from ingress classification or ingress policing.

The default marking state for network IP interfaces is trusted. This is equivalent to declaring no tos-marking-state on the network IP interface. When undefined or set to tos-marking-state trusted, the trusted state of the interface will not be displayed when using show config or show info unless the detail parameter is given. The **save config** command will not store the default tos-marking-state trusted state for network IP interfaces unless the detail parameter is also specified.

The **no** tos-marking-state command is used to restore the trusted state to a network IP interface. This is equivalent to executing the tos-marking-state trusted command.

Default trusted

Parameters **trusted —** The default prevents the ToS field to not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set.

untrusted — Specifies that all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface.

ipv6

Syntax [**no**] **ipv6**

Context config>service>vprn>sub-if
config>service>vprn>sub-if>group-if

Description This command configures IPv6 parameters.

allow-unmatching-prefixes

Syntax [**no**] **allow-unmatching-prefixes**

Context config>service>vprn>sub-if

Description This command allows address assignment to PPPoX hosts in cases where the assigned address falls outside the range of the configured subnets below the subscriber interface. Alternatively, if the interface is configured as unnumbered, this command cannot be enabled.

Default no allow-unmatching-prefixes

allow-unmatching-prefixes

Syntax [**no**] **allow-unmatching-prefixes**

Context configure>service>vprn>sub-if>ipv6>
configure>service>ies>sub-if>ipv6>

Description This command allows address assignment to IPv6 hosts in cases where the assigned address or the prefix falls outside of the range of the configured IPv6 subscriber-prefixes under the **configure>service>vprn/ies>sub-if>ipv6** hierarchy.

Unnumbered PPPoEv6 does not mean that the PPPoEv6 hosts do not have an IPv6 address or prefix assigned. It only means that the IPv6 address range (out of which the address or prefix is assigned to the host) does not have to be known in advance via configuration under the **subscriber-interface>ipv6>subscriber-prefixes** node

Default no allow-unmatching-prefixes

delegated-prefix-length

Syntax **delegated-prefix-length** *bits*
delegated-prefix-length variable
no delegated-prefix-length

Context configure>router>subscriber-interface>ipv6
configure>service>vprn>subscriber-interface>ipv6

Description This command configures the subscriber-interface level setting for delegated prefix length. The delegated prefix length for a subscriber- interface can be either set to a fixed value that is explicitly configured under the subscriber-interface CLI hierarchy or a variable value that can be obtained from various sources. This command can be changed only when no IPv6 prefixes are configured under the subscriber-interface.

Default no delegated-prefix-length This means that the delegated prefix length is 64.

Parameters *bits* — The delegated prefix length in bits. This value will beapplicable to the entire subscriber-interface. In case that the delegated prefix length is also supplied via other means (LUDB, Radius or DHCP Server), such supplied value must match the value configured under the subscriber-interface. Otherwise the prefix instantiation in 7x50 will fail.

Values 48 — 64

variable — The delegated prefix value can be of any length between 48..64. The value itself can vary between the prefixes and it will be provided at the time of prefix instantiation. The order of priority for the source of the delegated prefix length is:

- LUDB
- Radius
- DHCPv6 server

dhcp6

Syntax [**no**] **dhcp6**

Context config>service>vprn>sub-if>grp-if>ipv6

Description This command allows access to the DHCP6 context within the group interface configuration. Within this context, DHCP6 parameters can be configured.

Default no dhcp6

option

Syntax [**no**] **option**

Context config>service>vprn>sub-if>grp-if>ipv6

Description This command enables the context to configure DHCPv6 relay information options.

The **no** form of the command disables DHCPv6 relay information options.

interface-id

Syntax **interface-id**
interface-id ascii-tuple
interface-id ifindex
interface-id sap-id
interface-id string
no interface-id

Context config>service>vprn>sub-if>grp-if>ipv6>dhcp6>option

Description This command enables the sending of interface ID options in the DHCPv6 relay packet.

The **no** form of the command disables the sending of interface ID options in the DHCPv6 relay packet

Parameters **ascii-tuple —** Specifies that the ASCII-encoded concatenated tuple will be used which consists of the access-node-identifier, service-id, and interface-name, separated by "|".

ifindex — Specifies that the interface index will be used. (The If Index of a router interface can be displayed using the command **show>router>if>detail .**)

sap-id — Specifies that the SAP identifier will be used.

string — Specifies a string of up to 32 characters long, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

remote-id

Syntax [**no**] **remote-id**

Context config>service>vprn>sub-if>grp-if>ipv6>dhcp6>option

Description This command enables the sending of remote ID option in the DHCPv6 relay packet.

The client DHCP Unique Identifier (DUID) is used as the remote ID.

The **no** form of the command disables the sending of remote ID option in the DHCPv6 relay packet.

proxy-server

Syntax [**no**] **proxy-server**

Context config>service>vprn>sub-if>grp-if>ipv6>dhcp6

Description This command allows access to the DHCP6 proxy server context. Within this context, DHCP6 proxy server parameters of the group interface can be configured

Default no proxy-server.

renew-timer

Syntax **renew-timer** *seconds*
no renew-timer

Context config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server

Description This command configures the renew-timer (T1), the time at which the client contacts the server from which the addresses in the IA_NA or IA_PD were obtained to extend the lifetimes of the addresses or prefixes assigned to the client.

Default 1800

Parameters *seconds* — Specifies the time duration relative to the current time, expressed in units of seconds. A value of zero leaves the renew-time at the discretion of the client.

Values 0 — 604,800

rebind-timer

Syntax **rebind-timer** *seconds*
no rebind-timer

Context config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server

Description This command configures the rebind-timer (T2), the time at which the client contacts any available server to extend the lifetimes of the addresses or prefixes assigned to the client.

Default 2880

Parameters *seconds* — T2 is a time duration relative to the current time. A value of zero leaves the rebind-time at the discretion of the client.

Values 0 — 1,209,600

preferred-lifetime

Syntax **preferred-lifetime** [*seconds* | **infinite**]
no preferred-lifetime

Context config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server

Description The preferred lifetime for the IPv6 prefix or address in the option, expressed in units of seconds. When the preferred lifetime expires, any derived addresses are deprecated.

Default 3600

Parameters *seconds* — Specifies a decimal time interval in seconds.

Values 600 — 424967295

infinite — Specifies a 0xffffffff value, Dec = 4294967295

valid-lifetime

Syntax **valid-lifetime** [*seconds* **| infinite**]
no valid-lifetime

Context config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server

Description The valid lifetime for the IPv6 prefix or address in the option, expressed in units of seconds.

Default 86,400

Parameters *seconds* — Specifies a decimal time interval in seconds.

Values 600 — 424967295

infinite — Specifies a 0xffffffff value, Dec = 4294967295

client-applications

Syntax **client-applications** [**dhcp**] [**pppoe**]
no client-applications

Context config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server

Description This command configures the client host types to which the DHCP6 proxy server is allowed to assign addresses.

Parameters **dhcp —** Specifies IP over Ethernet hosts.

pppoe — Specifies PPP over Ethernet hosts.

router-advertisements

Syntax [**no**] **router-advertisements**

Context config>service>vprn>sub-if>group-if>ipv6

Description This command enables Router Advertisement transmission on this group interface.

Default router-advertisements

current-hop-limit

Syntax **current-hop-limit** *hop-count*
no current-hop-limit

Context config>service>vprn>sub-if>group-if>ipv6>router-ad

Description This command specifies the hop-limit advertised to hosts in router advertisements.

Default 64

Parameters *hop-count* — Specifies the current hop limit (decimal) inserted into router advertisements.

Values 0 — 255

managed-configuration

Syntax [**no**] **managed-configuration**

Context config>service>vprn>sub-if>group-if>ipv6>router-ad

Description This command sets the managed address configuration flag. This flag indicates that DHCPv6 is available for address configuration in addition to any address auto-configured using stateless address auto-configuration. See RFC 3315, Dynamic Host Configuration Protocol (DHCP) for IPv6.

Default no managed-configuration

max-advertisement-interval

Syntax **max-advertisement-interval** *seconds*
no max-advertisement-interval

Context config>service>vprn>sub-if>group-if>ipv6>router-ad

Description This command configures the maximum interval between sending router advertisement messages.

Default 1800

Parameters *seconds* — Specifies the maximum interval in seconds between sending router advertisement messages.

Values 900 — 1800

min-advertisment-interval

Syntax **min-advertisement-interval** *seconds*

no min-advertisement-interval

Context config>service>vprn>sub-if>group-if>ipv6>router-ad

Description This command configures the minimum interval between sending router advertisement messages.

Default 900

Parameters *seconds* — Specifies the minimum interval, in seconds, between sending router advertisement messages.

Values 900 — 1350

mtu

Syntax **mtu** *bytes*
no mtu

Context config>service>vprn>sub-if>group-if>ipv6>router-ad

Description This command configures the MTU for the nodes to use to send packets on the link.

Default no mtu

Parameters *bytes* — Specifies the MTU for the nodes to use to send packets on the link.

Values 1280 — 9212

other-stateful-configuration

Syntax [**no**] **other-stateful-configuration**

Context config>service>vprn>sub-if>group-if>ipv6>router-ad

Description This command sets the "Other configuration" flag. This flag indicates that DHCPv6 is available for auto-configuration of other (non-address) information such as DNS-related information or information on other servers in the network. See RFC 3736, Stateless Dynamic Host Configuration Protocol (DHCP) for IPv6.

Default no other-stateful-configuration

prefix-options

Syntax [**no**] **prefix-options**

Context config>service>vprn>sub-if>group-if>ipv6>router-ad

Description This command configures router advertisement parameters for IPv6 prefixes returned via RADIUS Framed-IPv6-Prefix. All prefixes will inherit these configuration parameters.

Default no prefix-options

autonomous

Syntax [**no**] **autonomous**

Context config>services>vprn>sub-if>group-if>ipv6>router-ad>prefix-op

Description This command specifies whether the prefix can be used for stateless address auto-configuration.

Default no autonomous

preferred-lifetime

Syntax **preferred-lifetime** [*seconds* | **infinite**]
no preferred-lifetime

Context config>service>vprn>sub-if>group-if>ipv6>router-ad>prefix-op
config>service>vprn>sub-if>group-if>ipv6>dhcp6>proxy-server

Description This command configures the remaining length of time in seconds that this prefix will continue to be preferred, such as, time until deprecation. The address generated from a deprecated prefix should not be used as a source address in new communications, but packets received on such an interface are processed as expected.

Default 3600

Parameters *seconds* — Specifies a decimal time interval in seconds.

Values 0-4,294,967,295

infinite — Sepcifies a 0xffffffff value. Dec = 4,294,967,295.

valid-lifetime

Syntax **valid-lifetime** [*seconds* | **infinite**]
no valid-lifetime

Context config>service>vprn>sub-if>group-if>ipv6>router-ad>prefix-op
config>service>vprn>sub-if>group-if>ipv6>dhcp6>proxy-server

Description This command specifies the length of time, in seconds, that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity. The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

Default 86400

Parameters *seconds* — Specifies a decimal time interval in seconds.

Values 0-4,294,967,295

infinite — Sepcifies a 0xffffffff value. Dec = 4,294,967,295.

reachable-time

Syntax **reachable-time** *milliseconds*
no reachable-time

Context config>services>vprn>sub-if>group-if>ipv6>router-ad

Description This command configures how long this router should be considered reachable by other nodes on the link after receiving a reachability confirmation.

Default no reachable-time

Parameters *milliseconds* — The length of time the router should be considered reachable for default router selection.

Values 0-3,600,000

retransmit-time

Syntax **retransmit-time** *milliseconds*
no retransmit-time

Context config>services>vprn>sub-if>group-if>ipv6>router-ad

Description This command configures the retransmission frequency of neighbor solicitation messages.

Default no retransmit-time

Parameters *milliseconds* — Specifies how often the retransmission should occur.

Values 0-1,800,000

router-lifetime

Syntax **router-lifetime** *seconds*
router-lifetime no-default-router
no router-lifetime

Context config>services>vprn>sub-if>group-if>ipv6>router-ad

Description This command sets the router lifetime. A value of zero indicates this router should not be used by hosts as a default router.

Default 4500

Parameters *seconds* — Specifies how long this router is valid for default router selection.

Values 2700-9000

renew-timer

Syntax **renew-timer** *seconds*
no renew-timer

Context config>services>vprn>sub-if>group-if>ipv6>dhcpv6

Description This command configures the renew-timer (T1). The time at which the client contacts the server from the addresses in the IA_NA or IA_PD were obtained to extend the lifetimes of the addresses or prefixes assigned to the client.

Default 1800

Parameters *seconds* — Time duration relative to the current time expressed in units of seconds. A value of zero (0) leaves the renew-time at the discretion of the client.

Values 0-604,800

rebind-timer

Syntax **rebind-timer** *seconds*
no rebind-timer

Context config>services>vprn>sub-if>group-if>ipv6>dhcpv6

Description This command configures the rebind-timer (T2), the time at which the client contacts any available server to extend the lifetimes of the addresses or prefixes assigned to the client.

Default 2880

Parameters *seconds* — T2 is a time duration relative to the current time expressed in units of seconds. A value of zero (0) leaves the rebind-time at the discretion of the client.

Values 0-1,209,600

delegated-prefix-length

Syntax [**no**] **delegated-prefix-length** *prefix-length*

Context config>service>vprn>sub-if>ipv6

Description This command defines the prefix-length used for all DHCPv6 prefix delegations on this subscriber interface.

Parameters *prefix-length* — Specifies the prefix length in use on this subscriber interface for DHCPv6 IA_PD.

Values 48..64

Default 64

subscriber-prefixes

Syntax **subscriber-prefixes**

Context config>service>vprn>sub-if>ipv6

Description This command specifies aggregate off-link subscriber prefixes associated with this subscriber interface. Individual prefixes are specified under the prefix context list aggregate routes in which the next-hop is indirect via the subscriber interface.

prefix

Syntax **prefix** *ipv6-address/prefix-length* [**pd**] [**wan-host**]
no prefix *ipv6-address/prefix-length*

Context config>service>vprn>sub-if>ipv6>sub-prefixes

Description This command allows a list of prefixes(using the prefix command multiple times) to be routed to hosts associated with this subscriber interface. Each prefix will be represented in the associated FIB with a reference to the subscriber interface. Prefixes are defined as being for prefix delegation (pd) or use on a WAN interface or host (wan-host).

Parameters *ipv6-address* — Specifies the 128-bit IPv6 address.

Values 128-bit hexadecimal IPv6 address in compressed form

prefix-length — Specifies the length of any associated aggregate prefix.

Values 32-63

pd — Specifies that this aggregate is used by IPv6 ESM hosts for DHCPv6 prefix-delegation.

wan-host — Specifies that this aggregate is used by IPv6 ESM hosts for local addressing or by a routing gateway's WAN interface.

private-retail-subnets

Syntax [**no**] **private-retail-subnets**

Context config>service>vprn>sub-if

Description This command controls the export of subnets to the forwarding service. When this attribute is configured, subnets defined on this retail subscriber interface will no longer be exported to the associated wholesale VPRN and will remain private to the retail VPRN. This is useful in a PPPoE business service context as it allows retail services to use overlapping IP address spaces even if these services are associated with the same wholesale service.

PPPoE sessions are actually terminated in the retail service although their traffic transits on a SAP belonging to the wholesale service. This configuration is incompatible, however, with IPoE host management (DHCP, static-host and ARP-host) as these host types require that the retail subnets are exported to the wholesale VPRN. Thus, if PPPoE sessions need to coexist with IPoE hosts, this attribute should not be configured on this retail interface.

This command will fail if the subscriber interface is not associated with a wholesale service.

If the retail VPRN is of the type **hub**, this attribute is mandatory. Then, it will be enabled by default and it will not be possible to deconfigure it.

unnumbered

Syntax **unnumbered** [*ip-int-name* | *ip-address*]
no unnumbered

Context config>service>vprn>if
config>service>vprn>nw-if

Description This command configures the interface as an unnumbered interface. Unnumbered IP interface is supported on a Sonet/SDH access port with the PPP, ATM, or Frame Relay encapsulation. It is not supported on a TDM port or channel.

Parameters *ip-int-name* — Specifies the name of an IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-address — Specifies an IP address.

qos

Syntax **qos** *network-policy-id* **port-redirect-group** *queue-group-name* **egress-instance** *instance-id* **fp- redirect-group** *queue-group-name* **ingress-instance** *instance-id*
no qos

Context config>service>vprn>nw-if

Description This command associates a network Quality of Service (QoS) policy with a network IP interface. Only one network QoS policy can be associated with an IP interface at one time. Attempts to associate a second QoS policy return an error.

Associating a network QoS policy with a network interface is useful for the following purposes:

- To apply classification rules for determining the forwarding-class and profile of ingress packets on the interface.
- To associate ingress packets on the interface with a queue-group instance applied to the ingress context of the interface's forwarding plane (FP). (This is only applicable to interfaces on IOM3 and later cards.) The referenced ingress queue-group instance may have policers defined in order to rate limit ingress traffic on a per-forwarding class (and forwarding type: unicast vs. multicast) basis.
- To perform 802.1p, DSCP, IP precedence and/or MPLS EXP re-marking of egress packets on the interface.
- To associate egress packets on the interface with a queue-group instance applied to the egress context of the interface's port. The referenced egress queue-group instance may have policers and/or queues defined in order to rate limit egress traffic on a per-forwarding class basis.

The **no** form of the command removes the network QoS policy association from the network IP interface, and the QoS policy reverts to the default.

Default **no qos**

Parameters *network-policy-id* — An existing network policy ID to associate with the IP interface.

Values 1 — 65535

port-redirect-group *queue-group-name* **—** This optional parameter specifies the egress queue-group used for all egress forwarding-class redirections specified within the network QoS policy ID. The specified *queue-group-name* must exist as an egress queue group applied to the egress context of the port associated with the IP interface.

egress-instance *instance-id* **—** Since multiple instances of the same egress queue-group can be applied to the same port this optional parameter is used to specify which particular instance to associate with this particular network IP interface.

Values 1 — 16384

fp- redirect-group *queue-group-name* **—** This optional parameter specifies the ingress queue-group used for all ingress forwarding-class redirections specified within the network QoS policy ID. The specified queue-group-name must exist as an ingress queue group applied to the ingress context of the forwarding plane associated with the IP interface.

ingress-instance *instance-id* **—** Since multiple instances of the same ingress queue-group can be applied to the same forwarding plane this parameter is required to specify which particular instance to associate with this particular network IP interface.

Values 1 — 16384

urpf-check

Syntax **[no] urpf-check**

Context config>service>vprn>if
config>service>vprn>nw-if
config>service>vprn>interface>ipv6
config>service>vprn>sub-if>grp-if

Description This command enables unicast RPF (uRPF) check on this interface.

The **no** form of the command disables unicast RPF (uRPF) Check on this interface.

Default disabled

mode

Syntax **mode** {**strict** | **loose** | **strict-no-ecmp**}
no mode

Context config>service>vprn>if>urfp-check
config>service>vprn>nw-if>urfp-check
config>service>vprn>sub-if>grp-if>urpf-check

Description This command specifies the mode of unicast RPF check.

The **no** form of the command reverts to the default (strict) mode.

Default strict

Parameters **strict —** When specified, uRPF checks whether incoming packet has a source address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

loose — In **loose** mode, uRPF checks whether incoming packet has source address with a corresponding prefix in the routing table. However, the loose mode does not check whether the interface expects to receive a packet with a specific source address prefix. This object is valid only when **urpf-check** is enabled.

strict-no-ecmp — When a packet is received on an interface in this mode and the SA matches an ECMP route the packet is dropped by uRPF.

DHCP Commands

dhcp

Syntax **dhcp**

Context config>service>vprn>if
config>service>vprn>nw-if
config>service>vprn>subscriber-interface
config>service>vprn>sub-if>grp-if

Description This command enables the context to configure DHCP parameters.

client-applications

Syntax **client-applications dhcp**
client-applications pppoe
client-applications dhcp pppoe
no client-applications

Context config>service>vprn>sub-if>grp-if>dhcp

Description This command enables the clients that will try to contact the DHCP server(s).

The **no** form of the command removes the server client type from the configuration.

Parameters **dhcp —** Specifies that the DHCP relay will forward requests to the DHCP server(s).

pppoe — Specifies that PPPoE will attempt to request an IP address for a PPPoE client from the DHCP server(s)ly assigned to PPPoE node.

action

Syntax **action** {**replace** | **drop** | **keep**}
no action

Context config>service>vprn>if>dhcp>option
config>service>vprn>nw-if>dhcp>option
config>service>vprn>sub-if>grp-if>dhcp>option

Description This command configures the processing required when the SR-Series router receives a DHCP request that already has a Relay Agent Information Option (Option 82) field in the packet.

The **no** form of this command returns the system to the default value.

Default Per RFC 3046, *DHCP Relay Agent Information Option* , section 2.1.1, *Reforwarded DHCP requests*, the default is to keep the existing information intact. The exception to this is if the giaddr of the

received packet is the same as the ingress address on the router. In that case the packet is dropped and an error is logged.

Parameters **replace —** In the upstream direction (from the user), the existing Option 82 field is replaced with the Option 82 field from the router. In the downstream direction (towards the user) the Option 82 field is stripped (in accordance with RFC 3046).

drop — The packet is dropped, and an error is logged.

keep — The existing information is kept in the packet and the router does not add any additional information. In the downstream direction the Option 82 field is not stripped and is sent on towards the client.

The behavior is slightly different in case of Vendor Specific Options (VSOs). When the keep parameter is specified, the router will insert his own VSO into the Option 82 field. This will only be done when the incoming message has already an Option 82 field.

If no Option 82 field is present, the router will not create the Option 82 field. In this in that case, no VSO will be added to the message.

circuit-id

Syntax **circuit-id** [**ascii-tuple** | **ifindex** | **sap-id** | **vlan-ascii-tuple**]
no circuit-id

Context config>service>vprn>if>dhcp>option
config>service>vprn>nw-if>dhcp>option
config>service>vprn>sub-if>grp-if>dhcp>option

Description When enabled, the router sends the interface index (If Index) in the **circuit-id** suboption of the DHCP packet. The If Index of a router interface can be displayed using the command **show>router>interface>detail**. This option specifies data that must be unique to the router that is relaying the circuit.

If disabled, the **circuit-id** suboption of the DHCP packet will be left empty.

The **no** form of this command returns the system to the default.

Default circuit-id

Parameters **ascii-tuple —** Specifies that the ASCII-encoded concatenated tuple will be used which consists of the access-node-identifier, service-id, and interface-name, separated by "|".

ifindex — Specifies that the interface index will be used. The If Index of a router interface can be displayed using the command **show>router>interface>detail**.

sap-id — Specifies that the SAP ID will be used.

vlan-ascii-tuple — Specifies that the format will include VLAN-id and dot1p bits in addition to what is included in ascii-tuple already. The format is supported on dot1q and qinq ports only. Thus, when the Option 82 bits are stripped, dot1p bits will be copied to the Ethernet header of an outgoing packet.

filter

Syntax **filter** *filter-id*
no filter

Context config>service>vprn>sub-if>grp-if>dhcp

Description This command configures the DHCP filter for this interface.

Parameters *filter-id* — Specifies the filter policy. The filter ID must already exist within the created IP filters.

Values 1 — 65535

gi-address

Syntax **gi-address** *ip-address* [*src-ip-addr*]
no gi-address

Context config>service>vprn>if>dhcp
config>service>vprn>nw-if>dhcp
config>service>vprn>sub-if>dhcp
config>service>vprn>sub-if>grp-if>dhcp

Description This command configures the gateway interface address for the DHCP relay. A subscriber interface can include multiple group interfaces with multiple SAPs. The GI address is needed, when the router functions as a DHCP relay, to distinguish between the different subscriber interfaces and potentially between the group interfaces defined.

Default no gi-address

Parameters *ip-address* — Specifies the host IP address to be used for DHCP relay packets.

src-ip-address — Specifies the source IP address to be used for DHCP relay packets.

lease-populate

Syntax **lease-populate** [*nbr-of-leases*]
lease-populate [*nbr-of-leases*] **route-populate** [**pd**] **na** [**ta**]
lease-populate [*nbr-of-leases*] **route-populate pd** [**na**] [**ta**] [**exclude**]
lease-populate [*nbr-of-leases*] **route-populate** [**pd**] [**na**] **ta**
no lease-populate

Context config>service>vprn>if>ipv6
config>service>vprn>if>ipv6>dhcp-relay

Description This command specifies the maximum number of DHCPv6 lease states allocated by the DHCPv6 relay function, allowed on this interface.

Optionally, by specifying “route-populate” parameter, system could:

- Create routes based on the IA_PD/IA_NA/IA_TA prefix option in relay-reply message.

- Create black hole routes based on OPTION_PD_EXCLUDE in IA_PD in relay-reply message.

These routes could be redistributed into IGP/BGP by using route-policy, following protocol types that could be used in "from protocol":

- dhcpv6-pd
- dhcpv6-na
- dhcpv6-ta
- dhcpv6-pd-excl

Parameters *nbr-of-entries* — Defines the number lease state table entries allowed for this interface. If this parameter is omitted, only a single entry is allowed. Once the maximum number of entries has been reached, subsequent lease state entries are not allowed and subsequent DHCPv6 ACK messages are discarded.

Values 1 — 8000

route-populate —

Values pd/na/ta — Create route based on specified option.

exclude — Create blackhole route based on OPTION_PD_EXCLUDE.

neighbor-resolution

Syntax [**no**] **neighbor-resolution**

Context config>service>vprn>if>ipv6>dhcp6-relay

Description This command enables neighbor resolution with DHCPv6 relay.

The **no** form of the command disables neighbor resolution.

match-circuit-id

Syntax [**no**] **match-circuit-id**

Context config>service>vprn>sub-if>grp-if>dhcp

Description This command enables Option 82 circuit ID on relayed DHCP packet matching. For routed CO, the group interface DHCP relay process is stateful. When packets are relayed to the server the virtual router ID, transaction ID, SAP ID, and client hardware MAC address of the relayed packet are tracked.

When a response is received from the server the virtual router ID, transaction ID, and client hardware MAC address must be matched to determine the SAP on which to send the packet out. In some cases, the virtual router ID, transaction ID, and client hardware MAC address are not guaranteed to be unique.

When the **match-circuit-id** command is enabled we use this as part of the key to guarantee correctness in our lookup. This is really only needed when we are dealing with an IP aware DSLAM that proxies the client hardware MAC address.

Default no match-circuit-id

option

Syntax [**no**] **option**

Context config>service>vprn>if>dhcp
config>service>vprn>nw-if>dhcp
config>service>vprn>sub-if>dhcp
config>service>vprn>sub-if>grp-if>dhcp

Description This command enables DHCP Option 82 (Relay Agent Information Option) parameters processing and enters the context for configuring Option 82 sub-options.

The **no** form of this command returns the system to the default.

Default no option

copy-82

Syntax [**no**] **copy-82**

Context config>service>vprn>nw-if>dhcp>option

Description This command enables the copy-82 option.

The **no** form of the command disables the option.

remote-id

Syntax **remote-id** [**mac** | **string** *string*]
no remote-id

Context config>service>vprn>sub-if>grp-if>dhcp>option
config>service>vprn>nw-if>dhcp>option

Description When enabled, the router sends the MAC address of the remote end (typically the DHCP client) in the **remote-id** suboption of the DHCP packet. This command identifies the host at the other end of the circuit. If disabled, the **remote-id** suboption of the DHCP packet will be left empty.

The **no** form of this command returns the system to the default.

Default remote-id

Parameters **mac** — This keyword specifies the MAC address of the remote end is encoded in the suboption.

string *string* — Specifies the remote-id.

vendor-specific-option

Syntax [**no**] **vendor-specific-option**

Context config>service>vprn>if>dhcp>option
config>service>vprn>nw-if>dhcp>option
config>service>vprn>sub-if>grp-if>dhcp>option

Description This command configures the Alcatel-Lucent vendor specific suboption of the DHCP relay packet.

client-mac-address

Syntax [**no**] **client-mac-address**

Context config>service>vprn>if>dhcp>option
config>service>vprn>nw-if>dhcp>option
config>service>vprn>if>dhcp>option>vendor
config>service>vprn>sub-if>grp-if>dhcp>option>vendor

Description This command enables the sending of the MAC address in the Alcatel-Lucent vendor specific suboption of the DHCP relay packet.

The **no** form of the command disables the sending of the MAC address in the Alcatel-Lucent vendor specific suboption of the DHCP relay packet.

pool-name

Syntax [**no**] **pool-name**

Context config>service>vprn>if>dhcp>option

Description This command enables the sending of the pool name in the Alcatel vendor-specific suboption of the DHCP relay packet.

The **no** form of the command disables the feature.

if-name

Syntax [**no**] **if-name**

Context config>service>vprn>nw-if>dhcp>option

Description This command enables the sending of the interface name in the Alcatel vendor specific suboption of the DHCP relay packet

The **no** form of the command disables the sending.

port-id

Syntax [**no**] **port-id**

Context config>service>vprn>nw-if>dhcp>option

Description This command enables sending of the port-id in the Alcatel vendor specific suboption of the DHCP relay packet

The **no** form of the command disables the sending.

sap-id

Syntax [**no**] **sap-id**

Context config>service>vprn>if>dhcp>option>vendor
config>service>vprn>sub-if>grp-if>dhcp>option>vendor

Description This command enables the sending of the SAP ID in the Alcatel-Lucent vendor specific suboption of the DHCP relay packet.

The **no** form of the command disables the sending of the SAP ID in the Alcatel-Lucent vendor specific suboption of the DHCP relay packet.

service-id

Syntax [**no**] **service-id**

Context config>service>vprn>if>dhcp>option>vendor
config>service>vprn>sub-if>grp-if>dhcp>option>vendor

Description This command enables the sending of the service ID in the Alcatel-Lucent vendor specific suboption of the DHCP relay packet.

The **no** form of the command disables the sending of the service ID in the Alcatel-Lucent vendor specific suboption of the DHCP relay packet.

string

Syntax [**no**] **string** *text*

Context config>service>vprn>if>dhcp>option>vendor
config>service>vprn>sub-if>grp-if>dhcp>option>vendor

Description This command specifies the vendor specific suboption string of the DHCP relay packet.

The **no** form of the command returns the default value.

Parameters *text* — The string can be any combination of ASCII characters up to 32 characters in length. If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

system-id

Syntax [**no**] **system-id**

Context config>service>vprn>if>dhcp>option>vendor
config>service>vprn>nw-if>dhcp>option>vendor
config>service>vprn>sub-if>grp-if>dhcp>option>vendor

Description This command specifies whether the system-id is encoded in the Alcatel-Lucent vendor specific sub-option of Option 82.

Default None

proxy-server

Syntax **proxy-server**

Context config>service>if>dhcp
config>service>vprn>sub-if>grp-if>dhcp

Description This command configures the DHCP proxy server.

emulated-server

Syntax **emulated-server** *ip-address*
no emulated-server

Context config>service>vprn>if>dhcp>proxy
config>service>vprn>sub-if>grp-if>dhcp>proxy-server

Description This command configures the IP address to be used as the DHCP server address in the context of this service. Typically, the configured address should be in the context of the subnet.

The **no** form of this command reverts to the default setting. The local proxy server will not become operational without a specified emulated server address.

Parameters *ip-address* — Specifies the emulated server address.

Default Note that for a retail interface, the default is the local interface.

lease-time

Syntax **lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**radius-override**]
no lease-time

Context config>service>vprn>if>dhcp>proxy
config>service>vprn>sub-if>grp-if>dhcp>proxy-server

Description This command defines the length of lease-time that will be provided to DHCP clients. By default the local-proxy-server will always make use of the lease-time information provide by either a RADIUS or DHCP server.

The no form of this command disables the use of the lease-time command. The local-proxy-server will use the lease-time offered by either a RADIUS or DHCP server.

Default 7 days 0 hours 0 seconds

Parameters **radius-override —** Specifies that the local-proxy-server will use the configured lease-time information to provide DHCP clients.

days — Specifies the number of days that the given IP address is valid.

Values 0 — 3650

hours — Specifies the number of hours that the given IP address is valid.

Values 0 — 23

minutes — Specifies the number of minutes that the given IP address is valid.

Values 0 — 59

seconds — Specifies the number of seconds that the given IP address is valid.

Values 0 — 59

server

Syntax **server** *server1* [*server2*...(up to 8 max)]

Context config>service>vprn>if>dhcp
config>service>vprn>nw-if>dhcp
config>service>vprn>sub-if>grp-if>dhcp

Description This command specifies a list of servers where requests will be forwarded. The list of servers can entered as either IP addresses or fully qualified domain names. There must be at least one server specified for DHCP relay to work. If there are multiple servers then the request is forwarded to all of the servers in the list. There can be a maximum of 8 DHCP servers configured.

The flood command is applicable only in the VPLS case. There is a scenario with VPLS where the VPLS node only wants to add Option 82 information to the DHCP request to provider per-subscriber information, but it does not do full DHCP relay. In this case, the server is set to "flood". This means the DHCP request is still a broadcast and is sent through the VPLS domain. A node running at L3 further upstream then can perform the full L3 DHCP relay function.

Default no server

Parameters *server* — Specifies the DHCP server IP address.

relay-plain-bootp

Syntax [**no**] **relay-plain-bootp**

Context config>service>vprn>if>dhcp

Description This command enables the relaying of plain BOOTP packets.

The **no** form of the command disables the relaying of plain BOOTP packets.

relay-unicast-msg

Syntax **relay-unicast-msg** [**release-update-src-ip**]
no relay-unicast-msg

Context config>service>vprn>sub-if>dhcp
config>service>vprn>sub-if>grp-if>dhcp

Description Relay unicast client DHCPv4 request (renew) messages. In the upstream direction: update the source-ip address and add the gateway IP address (gi-address) field before sending the message to the intended DHCP server (the message is not broadcasted to all configured DHCP servers). In the downstream direction: remove the gi-address and update the destination IP address to the value of the yiaddr (your IP addess) field.

By default, unicast DHCPv4 release messages are forwarded transparently.

Additionally when the optional flag “relay-unicast-msg” is enabled, then the gi address and source IP address of relayed DHCPv4 messages can be configured to any local configured IP address in the same routing instance.

Default no relay-unicast-msg

Parameters **release-update-src-ip —** Updates the source IP address with the value used for relayed DHCPv4 messages

snoop

Syntax [**no**] **snoop**

Context config>service>vprn>nw-if>dhcp

Description This command enables snooping of DHCP packets on this interface.

The **no** form of the command disables snooping.

trusted

Syntax [**no**] **trusted**

Context config>service>vprn>if>dhcp
config>service>vprn>nw-if>dhcp
config>service>vprn>sub-if>grp-if>dhcp

Description According to RFC 3046, *DHCP Relay Agent Information Option*, a DHCP request where the giaddr is 0.0.0.0 and which contains a Option 82 field in the packet, should be discarded, unless it arrives on a "trusted" circuit.

If trusted mode is enabled on an IP interface, the relay agent (the SR-Series) will modify the request's giaddr to be equal to the ingress interface and forward the request.

Note that this behavior only applies when the action in the Relay Agent Information Option is "keep". In the case where the Option 82 field is being replaced by the relay agent (action = "replace"), the original Option 82 information is lost anyway, and there is thus no reason for enabling the trusted option.

The **no** form of this command returns the system to the default.

Default not enabled

egress

Syntax **egress**

Context config>service>vprn>nw-if

Description This command enables the context to configure egress network filter policies for the interface.

use-arp

Syntax [**no**] **use-arp**

Context config>service>vprn>if>dhcp

Description This command enables the use of ARP to determine the destination heardware address.

The **no** form of the command disables the use of ARP to determine the destination heardware address

user-db

Syntax **user-db** *local-user-db-name*
no user-db

Context config>service>vprn>sub-if>grp-if>dhcp

Description This command configures the local user database to use for authentication.

The **no** form of the command removes the value from the configuration.

Default no user-db

Parameters *local-user-db-name* — Specifies the local user database to use for authentication.

dynamic-tunnel-redundant-next-hop

Syntax **dynamic-tunnel-redundant-next-hop** *ip-address*
no dynamic-tunnel-redundant-next-hop

Context config>service>vprn>if

Description This command specifies redundant next-hop address on public or private IPsec interface (with public or private tunnel-sap) for dynamic IPsec tunnel. The specified next-hop address will be used by standby node to shunt traffic to master in case of it receives them.

The next-hop address will be resolved in routing table of corresponding service.

Default none

Description *ip-address* — Specifies the dynamic ISA tunnel redundant next-hop address.

enable-ingress-stats

Syntax [**no**] **enable-ingress-stats**

Context config>router>interface
config>service>ies >interface
config>service>vprn>interface
config>service>ies>sub-if>grp-if
config>service>vprn>sub-if>grp-if

Description This command enables the collection of ingress interface IP stats. This command is only appliable to IP statistics, and not to uRPF statistics.

If enabled, then the following statistics are collected:

IPv4 offered packets

IPv4 offered octets

IPv6 offered packets

IPv6 offered octets

Note that octet statistics for IPv4 and IPv6 bytes at IP interfaces include the layer 2 frame overhead.

Default no enable-ingress-stats

enable-mac-accounting

Syntax [**no**] **enable-mac-accounting**

Context config>service>vprn>if

Description This command enables MAC accounting functionality on this interface.

The **no** form of the command disables MAC accounting functionality on this interface.

host-connectivity-verify

Syntax **host-connectivity-verify** [**interval** *interval*] [**action** {**remove** | **alarm**}]

Context config>service>vprn>if>sap
config>service>vprn>sub-if>grp-if
config>service>vprn>sub-if>grp-if>dhcp

Description This command enables enables subscriber host connectivity verification on a given SAP within a service.

This tool will periodically scan all known hosts (from dhcp-state) and perform a UC ARP request. The subscriber host connectivity verification will maintain state (connected vs. not-connected) for all hosts.

Default no host-connectivity-verify

Parameters **interval** ***interval*** **—** The interval, expressed in minutes, which specifies the time interval which all known sources should be verified. The actual rate is then dependent on number of known hosts and interval.

Values 1— 6000) Note that a zero value can be used by the SNMP agent to disable host-connectivity-verify.)

action {**remove** | **alarm**} **—** Defines the action taken on a subscriber host connectivity verification failure for a given host. The **remove** keyword raises an alarm and removes dhcp-state and releases all allocated resources (queues, table entries, etc.). DHCP-RELEASE will be signaled to corresponding DHCP server. Static hosts will never be removed. The **alarm** keyword raises an alarm indicating that the host is disconnected.

Interface ICMP Commands

icmp

Syntax **icmp**

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command configures Internet Control Message Protocol (ICMP) parameters on a VPRN service.

mask-reply

Syntax [**no**] **mask-reply**

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the **mask-reply** command configures the router interface to reply to the request.

By default, the router instance will reply to mask requests.

The **no** form of this command disables replies to ICMP mask requests on the router interface.

Default **mask-reply** — Reply to ICMP mask requests.

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This commad configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.

When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The **redirects** command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional *number* and *seconds* parameters

by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.

By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the generation of icmp redirects on the router interface.

Default **redirects 100 10** — Maximum of 100 redirect messages in 10 seconds.

Parameters *number* — The maximum number of ICMP redirect messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *seconds* of ICMP redirect messages that can be issued.

Values 1 — 60

ttl-expired

Syntax **ttl-expired** *number seconds*
no ttl-expired

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description Configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the limiting the rate of TTL expired messages on the router interface.

Default ttl-expired 100 10

Parameters *number* — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

Values 1 — 60

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This command enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachable messages is enabled at a maximum rate of 10 per 10 second time interval.

The **no** form of this command disables the generation of icmp destination unreachable messages on the router interface.

Default **unreachables 100 10**

Parameters *number* — The maximum number of ICMP unreachable messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP unreachable messages that can be issued.

Values 1 — 60

Interface ICMP Commands

icmp

Syntax **icmp**

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command configures Internet Control Message Protocol (ICMP) parameters on a VPRN service.

mask-reply

Syntax [**no**] **mask-reply**

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the **mask-reply** command configures the router interface to reply to the request.

By default, the router instance will reply to mask requests.

The **no** form of this command disables replies to ICMP mask requests on the router interface.

Default **mask-reply** — Reply to ICMP mask requests.

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This commad configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.

When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The **redirects** command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional *number* and *seconds* parameters

by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.

By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the generation of icmp redirects on the router interface.

Default **redirects 100 10** — Maximum of 100 redirect messages in 10 seconds.

Parameters *number* — The maximum number of ICMP redirect messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *seconds* of ICMP redirect messages that can be issued.

Values 1 — 60

ttl-expired

Syntax **ttl-expired** *number seconds*
no ttl-expired

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description Configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the limiting the rate of TTL expired messages on the router interface.

Default ttl-expired 100 10

Parameters *number* — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

Values 1 — 60

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This command enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachable messages is enabled at a maximum rate of 10 per 10 second time interval.

The **no** form of this command disables the generation of icmp destination unreachable messages on the router interface.

Default **unreachables 100 10**

Parameters *number* — The maximum number of ICMP unreachable messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP unreachable messages that can be issued.

Values 1 — 60

Router Advertisement Commands

router-advertisement

Syntax [**no**] **router-advertisement**

Context config>service>vprn

Description This command configures router advertisement properties. By default, it is disabled for all IPv6 enabled interfaces.

The **no** form of the command disables all IPv6 interface. However, the **no interface** *interface-name* command disables a specific interface.

Default disabled

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>service>vprn>router-advertisement

Description This command configures router advertisement properties on a specific interface. The interface must already exist in the **config>router>interface** context.

Default No interfaces are configured by default.

Parameters *ip-int-name* — Specify the interface name. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

current-hop-limit

Syntax **current-hop-limit** *number*
no current-hop-limit

Context config>service>vprn>router-advert>if

Description This command configures the current-hop-limit in the router advertisement messages. It informs the nodes on the subnet about the hop-limit when originating IPv6 packets.

Default 64

Parameters *number* — Specifies the hop limit.

Values 0 — 255. A value of zero means there is an unspecified number of hops.

managed-configuration

Syntax [**no**] **managed-configuration**

Context config>service>vprn>router-advert>if

Description This command sets the managed address configuration flag. This flag indicates that DHCPv6 is available for address configuration in addition to any address autoconfigured using stateless address autoconfiguration. See RFC 3315, *Dynamic Host Configuration Protocol (DHCP) for IPv6*.

Default no managed-configuration

max-advertisement-interval

Syntax [**no**] **max-advertisement-interval** *seconds*

Context config>service>vprn>router-advert>if

Description This command configures the maximum interval between sending router advertisement messages.

Default 600

Parameters *seconds* — Specifies the maximum interval in seconds between sending router advertisement messages.

Values 4 — 1800

min-advertisement-interval

Syntax [**no**] **min-advertisement-interval** *seconds*

Context config>service>vprn>router-advert>if

Description This command configures the minimum interval between sending ICMPv6 neighbor discovery router advertisement messages.

Default 200

Parameters *seconds* — Specify the minimum interval in seconds between sending ICMPv6 neighbor discovery router advertisement messages.

Values 3 — 1350

mtu

Syntax [**no**] **mtu** *mtu-bytes*

Context config>service>vprn>router-advert>if

Description This command configures the MTU for the nodes to use to send packets on the link.

Default no mtu — The MTU option is not sent in the router advertisement messages.

Parameters *mtu-bytes* — Specify the MTU for the nodes to use to send packets on the link.

Values 1280 — 9212

other-stateful-configuration

Syntax [**no**] **other-stateful-configuration**

Description This command sets the "Other configuration" flag. This flag indicates that DHCPv6lite is available for autoconfiguration of other (non-address) information such as DNS-related information or information on other servers in the network. See RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) for IPv6*.

Default no other-stateful-configuration

prefix

Syntax [**no**] **prefix** [*ipv6-prefix*/*prefix-length*]

Context config>service>vprn>router-advert>if

Description This command configures an IPv6 prefix in the router advertisement messages. To support multiple IPv6 prefixes, use multiple prefix statements. No prefix is advertised until explicitly configured using prefix statements.

Default none

Parameters *ip-prefix* — The IP prefix for prefix list entry in dotted decimal notation.

Values

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 — 32
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 — FFFF]H d: [0 — 255]D
ipv6-prefix-length	0 — 128

prefix-length — Specifies a route must match the most significant bits and have a prefix length.

Values 1 — 128

autonomous

Syntax [**no**] **autonomous**

Context config>service>vprn>router-advert>if>prefix

Description This command specifies whether the prefix can be used for stateless address autoconfiguration.

Default enabled

on-link

Syntax [**no**] **on-link**

Context config>service>vprn>router-advert>if>prefix

Description This command specifies whether the prefix can be used for onlink determination.

Default enabled

preferred-lifetime

Syntax [**no**] **preferred-lifetime** {*seconds* | **infinite**}

Context config>service>vprn>router-advert>if

Description This command configures the remaining length of time in seconds that this prefix will continue to be preferred, such as, time until deprecation. The address generated from a deprecated prefix should not be used as a source address in new communications, but packets received on such an interface are processed as expected.

Default 604800

Parameters *seconds* — Specifies the remaining length of time in seconds that this prefix will continue to be preferred.

infinite — Specifies that the prefix will always be preferred. A value of 4,294,967,295 represents infinity.

valid-lifetime

Syntax **valid-lifetime** {*seconds* | **infinite**}

Context config>service>vprn>router-advert>if

Description This command specifies the length of time in seconds that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity.

The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

Default 2592000

Parameters *seconds* — Specifies the remaining length of time in seconds that this prefix will continue to be valid.

infinite — Specifies that the prefix will always be valid. A value of 4,294,967,295 represents infinity.

reachable-time

Syntax **reachable-time** *milli-seconds*
no reachable-time

Context config>service>vprn>router-advert>if

Description This command configures how long this router should be considered reachable by other nodes on the link after receiving a reachability confirmation.

Default no reachable-time

Parameters *milli-seconds* — Specifies the length of time the router should be considered reachable.

Values 0 — 3600000

retransmit-time

Syntax **retransmit-timer** *milli-seconds*
no retransmit-timer

Context config>service>vprn>router-advert>if

Description This command configures the retransmission frequency of neighbor solicitation messages.

Default no retransmit-time

Parameters *milli-seconds* — Specifies how often the retransmission should occur.

Values 0 — 1800000

router-lifetime

Syntax **router-lifetime** *seconds*
no router-lifetime

Context config>service>vprn>router-advert>if

Description This command sets the router lifetime.

Default 1800

Parameters *seconds* — The length of time, in seconds, (relative to the time the packet is sent) that the prefix is valid for route determination.

Values 0, 4 — 9000 seconds. 0 means that the router is not a default router on this link.

use-virtual-mac

Syntax [**no**] **use-virtual-mac**

Context config>service>vprn>router-advert>if

Description This command enables sending router advertisement messages using the VRRP virtual MAC address, provided that the virtual router is currently the master.

If the virtual router is not the master, no router advertisement messages are sent.

The **no** form of the command disables sending router advertisement messages.

Default no use-virtual-mac

NAT Commands

nat

Syntax [**no**] **nat**

Context config>service>vprn
config>router

Description This command configures, creates or deletes a NAT instance.

inside

Syntax **inside**

Context config>service>vprn>nat
config>router>nat

Description This command enters the “inside” contex to configure the inside NAT instance.

destination-prefix

Syntax [**no**] **destination-prefix** *ip-prefix/length*

Context config>service>vprn>nat>inside
config>router>nat>inside

Description This command configures a destination prefix. An (internal) static route will be created for this prefix. All traffic that hits this route will be subject to NAT. The system will not allow a destination-prefix to be configured if the configured nat-policy refers to an IP pool that resides in the same service (as this would result in a routing loop).

Parameters *ip-prefix* — Specifies the IP prefix; host bits must be zero (0).

Values a.b.c.d

length — Specifies the prefix length.

Values 0 — 32

dual-stack-lite

Syntax **dual-stack-lite**

Context config>service>vprn>nat
config>router>nat>inside

Description This command enables the context to configure Dual-Stack-Lite NAT parameters.

address

Syntax [**no**] **address** *ipv6-address*

Context config>service>vprn>nat>inside>dslite

Description This command configures a dual-stack-lite IPv6 address

The **no** form of the command removes the value from the configuration.

Default none

Parameters *ipv6-address* — Specifies the IPv6 address on the interface.

Values ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0 — FFFF]H
d [0 — 255]D

tunnel-mtu

Syntax **tunnel-mtu** *mtu-bytes*
no tunnel-mtu

Context config>service>vprn>nat>inside>dslite>address

Description This command configures the DSLite tunnel MTU for this Dual Stack Lite address.

The **no** form of the command reverts the default.

Default 1500

Parameters *mtu-bytes* — Specifies the DSLite tunnel MTU.

Values 512 — 9212

subscriber-prefix-length

Syntax **subscriber-prefix-length** *prefix-length*
no subscriber-prefix-length

Context config>service>vprn>nat>inside>dslite

Description This command configures the IPv6 prefix length of the dual-stack-lite subscribers.

The **no** form of the command reverts the default.

Default 128

Parameters **prefix-length** *prefix-length* — Specifies the IPv6 prefix length of the dual-stack-lite subscriber.

Values 32 — 64, 128

Default 128

l2-aware

Syntax **l2-aware**

Context config>services>vprn>nat>inside

Description This command enables the context to configure parameters specific to Layer 2-aware NAT.

address

Syntax [**no**] **address** *ip-address/mask*

Context config>services>vprn>nat>inside>l2-aware

Description This command configures a Layer 2-aware NAT address. This address will act as a local address of the system. Hosts connected to the inside service will be able to ARP for this address. To verify connectivity, a host can also ping the address. This address is typically used as next hop of the default route of a Layer 2-aware host. The given mask defines a Layer 2-aware subnet. The (inside) IP address used by anLayer 2-aware host must match one of the subnets defined here or it will be rejected.

Parameters *ip-address* — Specifies the IP address in a.b.c.d format.

mask — Specifies the mask.

Values 16 — 32

nat-policy

Syntax **nat-policy** *nat-policy-name*
no nat-policy

Context config>services>vprn>nat>inside
config>router>nat>inside

Description This command configures the NAT policy that will be used for large-scale NAT in this service.

Parameters *nat-policy-name* — Specifies the NAT policy name.

Values 32 chars max

redundancy

Syntax **redundancy**

Context config>service>vprn>nat>inside
config>service>vprn>nat>outside>pool

Description This command enables the context to configure redundancy parameters.

peer

Syntax **peer** *ip-address*
no peer

Context config>service>vprn>nat>inside>redundancy

Description This command configures the IP address of the NAT redundancy peer in the realm of this virtual router instance.

steering-route

Syntax **steering-route** *ip-prefix/length*
no steering-route

Context config>service>vprn>nat>inside>redundancy

Description This command configures specifies the IP address and prefix length of the steering route. The steering route is used in the realm of this virtual router instance as an indirect next-hop for all the traffic that must be routed to the large scale NAT function.

outside

Syntax **outside**

Context config>service>vprn>nat
config>router>nat

Description This command enters the "outside" context to configure the outside NAT instance.

pool

Syntax **pool** *nat-pool-name* [**nat-group** *nat-group-id* **type** *pool-type* [**no-allocate**] [**create**]
no pool *nat-pool-name*

Context config>service>vprn>nat>outside
config>router>nat>outside

Description This command configures a NAT pool.

Parameters *nat-pool-name* — Specifies the NAT pool name.

Values 32 chars max

nat-group-id — Specifies the NAT group ID.

Values 1 — 4

create — This parameter must be specified to create the instance.

pool-type — Species the pool type, either large-scale or L2-aware.

address-range

Syntax **address-range** *start-ip-address end-ip-address* [**create**]
no address-range *start-ip-address end-ip-address*

Context config>service>vprn>nat>outside>pool
config>router>nat>outside>pool

Description This command configures a NAT address range.

Parameters *start-ip-address* — Specifies the beginning IP address in a.b.c.d form.

end-ip-address — Specifies the ending IP address in a.b.c.d. form.

create — This parameter must be specified to create the instance.

description

Syntax **description** *description-string*
no description

Context config>service>vprn>nat>outside>pool>address-range
config>service>vprn>nat>outside>pool
config>router>nat>outside>pool>address-range
config>router>nat>outside>pool

Description This command configures the description for the NAT address range.

Parameters *description-string* — Specifies the NAT address range description.

Values 80 chars max

drain

Syntax [**no**] **drain**

Context config>service>vprn>nat>outside>pool>address-range
config>router>nat>outside>pool>address-range

Description This command starts or stops draining this NAT address range. When an address-range is being drained, it will not be used to serve new hosts. Existing hosts, however, will still be able to use the

address that was assigned to them even if it is being drained.An address-range can only be deleted if the parent pool is shut down or if the range itself is effectively drained (no hosts are using the addresses anymore).

mode

Syntax **mode** {**auto** | **napt**}
no mode

Context config>service>vprn>nat>outside>pool

Description This command configures the mode of operation of this NAT address pool.

The mode value is only relevant while the value of pool type is equal to largeScale; while the value of pool type is equal to l2Aware, the mode of operation is always NAPT.

port-forwarding-range

Syntax **port-forwarding-range** *range-end*
no port-forwarding-range

Context config>service>vprn>nat>outside>pool

Description This command configures the end of the port range available for port forwarding. The start of the range is always equal to one.

The actual maximum value of the range end may be restricted to less than 65535 depending on the value of the objects port reservation type and port reservation value and on system specifications.

Default 1023

Parameters *range-end* — Specifies the mode of operation of this NAT pool

Values 1023 — 65535

port-reservation

Syntax **port-reservation blocks** *num-blocks*
port-reservation ports *num-ports*
no port-reservation

Context config>service>vprn>nat>outside>pool
config>router>nat>outside>pool

Description This command configures the size of the port-block that will be assigned to a host that is served by this pool. The number of ports configured here will be available to UDP, TCP and ICMP (as identifiers).

Parameters *num-blocks* — Specifies the number of port-blocks per IP address. Setting num-blocks to one (1) for large scale NAT will enable 1:1 NAT for IP addresses in this pool.

Values 1 — 64512

num-ports — Specifies the number of ports per block.

Values 1 — 32256

export

Syntax **export** *ip-prefix/length*
no export

Context config>service>vprn>nat>outside>pool>redundancy

Description This command configures the IP address of the prefix to be exported.

The form of the command removes the value from the configuration.

Syntax:	ip-prefix/length :	ip-prefix	a.b.c.d
		ip-prefix-length	0 — 32

Values 0, 4, 16

monitor

Syntax **monitor** *ip-prefix/length*
no monitor

Context config>service>vprn>nat>outside>pool>redundancy

Description This command configures the peer route to monitor.

subscriber-limit

Syntax **subscriber-limit** [1..65535]
no subscriber-limit

Context config>service>vprn>nat>outside>pool

Description This command configures the maximum number of subscribers per outside IP address.

If multiple port blocks per subscriber are used, the block size is typically small; all blocks assigned to a given subscriber belong to the same IP address; the subscriber limit guarantees that any subscriber can get a mimimum number of ports.

Parameters *limit* — Specifies the maximum number of subscribers per outside IP address.

Values 1 — 65535

watermarks

Syntax **watermarks high** *percentage-high* **low** *percentage-low*
no watermarks

Context config>service>vprn>nat>outside>pool
config>router>nat>outside>pool

Description This command configures the watermarks for this NAT pool.

Parameters *percentage-high* — Specifies the high percentage.

Values 2 — 100

percentage-low — Specifies the low percentage.

Values 1 — 99

Subscriber Interface Commands

subscriber-interface

Syntax **subscriber-interface** *ip-int-name* [**fwd-service** *service-id* **fwd-subscriber-interface** *ip-int-name*]
no subscriber-interface *ip-int-name*

Context config>service>vprn

Description This command allows the operator to create special subscriber-based interfaces. It is used to contain multiple group interfaces. Multiple subnets associated with the subscriber interface can be applied to any of the contained group interfaces in any combination. The subscriber interface allows subnet sharing between group interfaces.

Use the **no** form of the command to remove the subscriber interface.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

fwd-service *service-id* **—** Specifies the forwarding service ID for a subscriber interface in a retailer context.

fwd-subscriber-interface *ip-int-name* **—** Specifies the forwarding subscriber interface for a subscriber interface in a retailer context.

address

Syntax [**no**] **address** {ip-*address/mask*|*ip-address netmask*} [**gw-ip-address** *ip-address*] [**populate-host-routes**] [**track-srrp** *srrp-instance* [**holdup-time** *msecs*]]

Context config>service>vprn>subscriber-interface

Description This command configures the local subscriber subnets available on a subscriber IP interface. The configured ip-address and mask define the address space associated with the subscriber subnet. Up to 16 IP subnets can be created on a single subscriber IP interface. Each subnet supports a locally owned IP host address within the subnet that is not expected to appear on other routers that may be servicing the same subscriber subnet. For redundancy purposes, the keyword **gw-address** defines a separate IP address within the subnet for Subscriber Routed Redundancy Protocol (SRRP) routing. This IP address must be the same on the local and remote routers participating in a common SRRP instance.

In SRRP, a single SRRP instance is tied to a group IP interface. The group IP interface is contained directly within a subscriber IP interface context and thus directly associated with the subscriber subnets on the subscriber IP interface. The SRRP instance is also indirectly associated with any subscriber subnets tied to the subscriber interface through wholesale/retail VPRN configurations. With the directly-associated and the indirectly-associated subscriber interface subnets, a single SRRP instance can manage hundreds of SRRP gateway IP addresses. This automatic subnet association to the SRRP instance is different from VRRP where the redundant IP address is defined within the VRRP context.

Defining an SRRP gateway IP address on a subscriber subnet is not optional when the subnet is associated with a group IP interface with SRRP enabled. Enabling SRRP (**no shutdown**) will fail if one or more subscriber subnets do not have an SRRP gateway IP address defined. Creating a new subscriber subnet without an SRRP gateway IP address defined will fail when the subscriber subnet is associated with a group IP interface with an active SRRP instance. Once SRRP is enabled on a group interface, the SRRP instance will manage the ARP response and routing behavior for all subscriber hosts reachable through the group IP interface.

The no form of the command removes the address from a subscriber subnet. The address command for the specific subscriber subnet must be executed without the gw-address parameter. To succeed, all SRRP instances associated with the subscriber subnet must removed or shutdown.

Parameters *ip-address/mask* | *ip-address netmask* — Specifies the address space associated with the subscriber subnet

gw-ip-address *ip-address* — Specifies a separate IP address within the subnet for SRRP routing purposes. This parameter must be followed by a valid IP interface that exists within the subscriber subnet created by the address command. The defined gateway IP address cannot currently exist as a subscriber host (static or dynamic). If the defined ip-address already exists as a subscriber host address, the address command will fail. The specified ip-address must be unique within the system.

The gw-address parameter may be specified at anytime. If the subscriber subnet was created previously, executing the address command with a gw-address parameter will simply add the SRRP gateway IP address to the existing subnet.

If the address command is executed without the gw-address parameter when the subscriber subnet is associated with an active SRRP instance, the address will fail. If the SRRP instance is inactive or removed, executing the address command without the gw-address parameter will remove the SRRP gateway IP address from the specified subscriber subnet.

If the address command is executed with a new gw-address, all SRRP instances currently associated with the specified subscriber subnet will be updated with the new SRRP gateway IP address.

populate-host-routes — Specifies to populate subscriber-host routes in local FIB. Storing them in FIB benefits topologies only where the external router advertises more specific routes than the one corresponding to locally configured subscriber-interface subnets.

allow-unmatching-subnets

Syntax [**no**] **allow-unmatching-subnets**

Context config>service>vprn>subscriber-interface

Description This command specifies whether subscriber hosts with a subnet that does not match any of the subnets configured on this interface, are allowed.

group-interface

Syntax [**no**] **group-interface** *ip-int-name*

Context config>service>vprn>subscriber-interface

Description This command enables the context to configure a group interface. A group interface is an interface that may contain one or more SAPs. This interface is used in triple-play services where multiple SAPs are part of the same subnet.

Default none

Parameters *ip-int-name* — Configures the interface group name. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

arp-host

Syntax **arp-host**

Context config>service>vprn>sub-if>grp-if

Description This command enables the context to configure ARP host parameters.

host-limit

Syntax **host-limit** *max-num-hosts*
no host-limit

Context config>service>vprn>sub-if>grp-if>arp-host

Description This command configures the maximum number of ARP hosts.

Parameters *max-num-hosts* — Specifies the maximum number of ARP hosts.

Values 1 — 32767

min-auth-interval

Syntax **min-auth-interval** *min-auth-interval*
no min-auth-interval

Context onfig>service>vprn>sub-if>grp-if>arp-host

Description This command configures the minimum authentication interval.

Parameters *min-auth-interval* — Specifies the minimum authentication interval.

Values 1 — 6000

sap-host-limit

Syntax **sap-host-limit** *max-num-hosts-sap*

no sap-host-limit

Context config>service>vprn>sub-if>grp-if>arp-host

Description This command configures the maximum number of ARP hosts per SAP.

Parameters *max-num-hosts-sap* — Specifies the maximum number of ARP hosts per SAP allowed on this IES interface.

Values 1 — 32767

PPPoE Commands

pppoe

Syntax [**no**] **pppoe**

Context config>service>vprn>sub-if>grp-if

Description This command enables the context to configure PPPoE parameters.

dhcp-client

Syntax **dhcp-client**

Context config>service>vprn>sub-if>grp-if>pppoe

Description This command enables the context to configure the PPPoE-to-DHCP options.

ccag-use-origin-sap

Syntax [**no**] **ccag-use-origin-sap**

Context config>service>vprn>sub-if>grp-if>pppoe>dhcp-client

Description This command enables the original VPLS SAP to be included in the circuit-id option to send to the DHCP server (in case this interface is connected to a VPLS by a CCA MDA).

The **no** form of the command disables the feature.

Default no ccag-use-origin-sap

pap-chap-user-db

Syntax **pap-chap-user-db** *local-user-db-name*
no pap-chap-user-db

Context config>service>vprn>sub-if>grp-if>pppoe

Description This command configures the local user database to use for PPP Challenge-Handshake Authentication Protocol/Password Authentication Protocol (PAP/CHAP) authentication.

If an authentication policy is also configured, **pppoe-access-method** must be set to none in this authentication policy to use the local user database (in that case RADIUS authentication will not be used for PPPoE hosts).

Parameters *local-user-db-name* — Specifies the local user database to use for authentication.

pppoe-policy

Syntax **pppoe-policy** *pppoe-policy-name*
no pppoe-policy

Context config>service>vprn>sub-if>grp-if>pppoe

Description This command associates a PPPoE policy on this interface.

Default default

Parameters *pppoe-policy-name* — Specifies a a PPPoE policy up to 32 characters in length on this interface.

sap-session-limit

Syntax **sap-session-limit** *sap-session-limit*
no sap-session-limit

Context config>service>vprn>sub-if>grp-if>pppoe

Description This command specifies the number of PPPoE hosts per SAP allowed for this group-interface.

Default 1

Parameters *sap-session-limit* — Specifies the number of PPPoE hosts per SAP allowed.

Values 1 — 20000

session-limit

Syntax **session-limit** *session-limit*
no session-limit

Context config>service>vprn>sub-if>grp-if>pppoe

Description This command specifies the number of PPPoE hosts allowed for this group interface.

Default 1

Parameters *session-limit* — Specifies the number of PPPoE hosts allowed

Values 1 — 20000

Interface ICMP Commands

icmp

Syntax **icmp**

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command configures Internet Control Message Protocol (ICMP) parameters on a VPRN service.

mask-reply

Syntax [**no**] **mask-reply**

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the **mask-reply** command configures the router interface to reply to the request.

By default, the router instance will reply to mask requests.

The **no** form of this command disables replies to ICMP mask requests on the router interface.

Default **mask-reply** — Reply to ICMP mask requests.

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This commad configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.

When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The **redirects** command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.

By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the generation of icmp redirects on the router interface.

Default **redirects 100 10** — Maximum of 100 redirect messages in 10 seconds.

Parameters *number* — The maximum number of ICMP redirect messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *seconds* of ICMP redirect messages that can be issued.

Values 1 — 60

ttl-expired

Syntax **ttl-expired** *number seconds*
no ttl-expired

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description Configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the limiting the rate of TTL expired messages on the router interface.

Default ttl-expired 100 10

Parameters *number* — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

Values 1 — 60

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context config>service>vprn>if>icmp
config>service>vprn>sub-if>grp-if>icmp
config>service>vprn>nw-if>icmp

Description This command enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachable messages is enabled at a maximum rate of 10 per 10 second time interval.

The **no** form of this command disables the generation of icmp destination unreachable messages on the router interface.

Default **unreachables 100 10**

Parameters *number* — The maximum number of ICMP unreachable messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP unreachable messages that can be issued.

Values 1 — 60

lag

Syntax **lag** *lag-id*[:*encap-val*]
no lag

Context config>service>vprn>nw-if

Description This command binds the interface to a Link Aggregation Group (LAG)

The **no** form of the command removes the LAG id from the configuration.

Parameters *lag-ig*[:*encap-val*] — Specifies the LAG ID.

Values		
	lag-id	1 — 200
	encap-val	0 for null 0 — 4094 for dot1q

lsr-load-balancing

Syntax **lsr-load-balancing** *hashing-algorithm*
no lsr-load-balancing

Context config>service>vprn>nw-if

Description This command specifies whether the IP header is used in the LAG and ECMP LSR hashing algorithm. This is the per interface setting.

Default no lsr-load-balancing

Parameters **lbl-only —** Only the label is used in the hashing algorithm.

lbl-ip — The IP header is included in the hashing algorithm.

ip-only — the IP header is used exclusively in the hashing algorithm

Interface SAP Commands

sap

Syntax **sap** *sap-id* [**create**]
no sap *sap-id*

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if
config>service>vprn>ipsec-if>sap

Description This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.
Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.
A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the **config interface** *port-type port-id* **mode access** command. Channelized TDM ports are always access ports.
If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted.

Default No SAPs are defined.

Special Cases **VPRN —** A VPRN SAP must be defined on an Ethernet interface.

sap ipsec-*id*.**private** | **public**:*tag* — This parameter associates an IPSec group SAP with this interface. This is the public side for an IPSec tunnel. Tunnels referencing this IPSec group in the private side may be created if their local IP is in the subnet of the interface subnet and the routing context specified matches with the one of the interface.

This context will provide a SAP to the tunnel. The operator may associate an ingress and egress QoS policies as well as filters and virtual scheduling contexts. Internally this creates an Ethernet SAP that will be used to send and receive encrypted traffic to and from the MDA. Multiple tunnels can be associated with this SAP. The “tag” will be a dot1q value. The operator may see it as an identifier. The range is limited to 1 — 4094.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 2569 for command syntax.

port-id — Specifies the physical port ID in the *slot/mda/port* format.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 6/2/3 specifies port 3 on MDA 2

in slot 6.

The *port-id* must reference a valid port type. When the *port-id* parameter represents SONET/SDH and TDM channels the port ID must include the channel ID. A period "." separates the physical port from the *channel-id*. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

create — Keyword used to create a SAP instance.

split-horizon-group *group-name* **—** Specifies the name of the split horizon group to which the SAP belongs.

aarp

Syntax **aarp** *aarpId* **type** *type*
no aarp

Context config>service>vprn>if>sap
config>service>vprn>if>spoke-sdp

Description This command associates an aarp instance to a multi-homed SAP or spoke-sdp. This instance is paired with the same aarp-id in the same node or in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke-sdp.

The type specifies the role of this service point in the AARP: primary (dual-homed), secondary (dual-homed-secondary). The AA service attributes (app-profile, transit-policy) of the primary are inherited by the secondary endpoints. All endpoints within an aarp must be of the same type (sap or spoke), and all endpoints with an aarp must be within the same service.

The **no** form of the command removes the association.

Default no aarp

Parameters *aarpId* — Specifies the AARP instance associated with this SAP. If not configured, no AARP instance is associated with this SAP.

Values 1 —

type — Specifies the role of the SAP referenced by the AARP instance identified by AARP ID.

Values **dual-homed** — the primary dual homed aa-subscriber side service point of an aarp instance, only supported for IES and VPRN SAP and spoke-sdp
dual-homed-secondary — One of the secondary dual homed aa-subscriber side service points of an aarp instance, only supported for IES and VPRN SAP and spoke-sdp.

tod-suite

Syntax **tod-suite** *tod-suite-name*
no tod-suite

Context config>service>vprn>if>sap

Description This command applies a time-based policy (filter or QoS policy) to the SAP. The suite name must already exist in the **config>cron** context.

Default no tod-suite

Parameters *tod-suite-name* — Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP or a subscriber. The suite can be applied to more than one SAP.

transit-policy

Syntax **transit-policy** *ip-aasub-policy-id*
transit-policy prefix *prefix-aasub-policy-id*
no transit-ip-policy

Context config>service>vprn>if>sap>
config>service>vprn>if>spoke-sdp>

Description This command associates a transit aa subscriber IP policy to the service. The transit IP policy must be defined prior to associating the policy with a SAP in the **config>application assurance>group>policy>transit-ip-policy** context.

Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service.

The **no** form of the command removes the association of the policy to the service.

Default no transit-ip-policy

ip-aasub-policy-id — An integer that identifies a transit IP profile entry.

Values 1 — 65535

prefix-aasub-policy-id — An integer that identifies a prefix aasub-policy ID.

Values 1 — 65535

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context config>service>vprn>if>sap
config>service>vprn>if>spoke-sdp

Description This command creates the accounting policy context that can be applied to an interface SAP or interface SAP spoke SDP.

An accounting policy must be defined before it can be associated with a SAP.
If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SAP, and the acccounting policy reverts to the default.

Default Default accounting policy.

Parameters *acct-policy-id* — Enter the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 — 99

app-profile

Syntax **app-profile** *app-profile-name*
no app-profile

Context config>service>vprn>if>spoke-sdp

Description This command configures the application profile name.

Parameters *app-profile-name* — Specifies the application profile name.

Values 32 chars max

collect-stats

Syntax [**no**] **collect-stats**

Context config>service>vprn>if>sap
config>service>vprn>if>spoke-sdp

Description This command enables accounting and statistical data collection for either an interface SAP or interface SAP spoke SDP, or network port. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the IOM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default no collect-stats

cpu-protection

Syntax **cpu-protection** *policy-id* [**mac-monitoring**] | [**eth-cfm-monitoring** [**aggregate**][**car**]]
no cpu-protection

Context config>service>vprn>sub-if>grp-if>sap

Description This command assigns an existing CPU protection policy to the associated group interface. The CPU protection policies are configured in the **config>sys>security>cpu-protection>policy** *cpu-*

protection-policy-id context.

If no CPU-Protection policy is assigned to a group interface SAP, then the default policy is used to limit the overall-rate. The default policy is policy number 254 for access interfaces and 255 for network interfaces.

The **no** form of the command removes the association of the CPU protection policy from the associated interface and reverts to the default policy values.

Description cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of no cpu-protection returns the interface/SAP to the default policies as shown above.

Parameters *policy-id* — Specifies an existing CPU protection policy.

Values 1 — 255

mac-monitoring — This keyword enables MAC monitoring.

eth-cfm-monitoring — This keyword enables Ethernet Connectivity Fault Management monitoring.

aggregate — This keyword applies the rate limit to the sum of the per peer packet rates.

car — (Committed Access Rate) This keyword causes Eth-CFM packets to be ignored when enforcing the overall-rate.

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context config>service>vprn>sub-if>grp-if>sap
config>service>>vprn>if>sap

Description This command assigns a Distributed CPU Protection (DCP) policy to the SAP. Only a valid created DCP policy can be assigned to a SAP or a network interface (note that this rule does not apply to templates such as an msap-policy)

Default no dist-cpu-protection

default-host

Syntax **default-host** *ip-address*/*mask* **next-hop** *next-hop-ip*
no default-host *ip-address*/*mask*

Context config>service>vprn>sub-if>grp-if>sap

Description This command configures the default-host to be used. More than one default-host can be configured per SAP.

The **no** form of the command removes the values from the configuration.

Parameters *ip-address/mask* — Assigns an IP address/IP subnet format to the interface.

next-hop *next-hop-ip* **—** Assigns the next hop IP address.

Interface SAP ATM Commands

atm

Syntax **atm**

Context config>service>vprn>if>sap
config>service>vprn>sub-if>grp-if>sap

Description This command enables the context to configure ATM-related attributes. This command can only be used when a given context (for example, a channel or SAP) supporting ATM functionality such as:

- Configuring ATM port or ATM port-related functionality on MDAs supporting ATM functionality.
- Configuring ATM-related configuration for ATM-based SAPs that exist on MDAs supporting ATM functionality.

If ATM functionality is not supported for a given context, the command returns an error.

egress

Syntax **egress**

Context config>service>vprn>if>sap>atm
config>service>vprn>sub-if>grp-if>sap>atm

Description This command configures egress ATM attributes for the SAP.

encapsulation

Syntax **encapsulation** *atm-encap-type*

Context config>service>vprn>if>sap>atm
config>service>vprn>sub-if>grp-if>sap>atm

Description This command configures RFC 2684, *Multiprotocol Encapsulation over ATM AAL5,* encapsulation for an ATM PVCC delimited SAP. This command specifies the data encapsulation for an ATM PVCC delimited SAP. The definition also references the ATM Forum LAN Emulation specification. Ingress traffic that does not match the configured encapsulation will be dropped.

Default The encapsulation is driven by the services for which the SAP is configured.
For VPRN service SAPs, the default is **aal5snap-routed**.

Parameters *atm-encap-type* — Specify the encapsulation type.

Values **aal5snap-routed** — Routed encapsulation for LLC encapsulated circuit (LLC/SNAP precedes protocol datagram) as defined in RFC 2684.
aal5mux-ip — Routed IP encapsulation for VC multiplexed circuit as defined in RFC 2684.
aal5snap-bridged — Bridged encapsulation for LLC encapsulated circuit (LLC/SNAP precedes protocol datagram) as defined in RFC 2684.
aal5mux-bridged-eth-nofcs — Bridged IP encapsulation for VC multiplexed circuit as defined in RFC 2684.

ingress

Syntax **ingress**

Context config>service>vprn>if>sap>atm
config>service>vprn>sub-if>grp-if>sap>atm

Description This command configures ingress ATM attributes for the SAP.

traffic-desc

Syntax **traffic-desc** *traffic-desc-profile-id*
no traffic-desc

Context config>service>vprn>if>sap>atm>egress
config>service>vprn>if>sap>atm>ingress
config>service>vprn>sub-if>grp-if>sap>atm>egress
config>service>vprn>sub-if>grp-if>sap>atm>ingress

Description This command assigns an ATM traffic descriptor profile to a given context (for example, a SAP). When configured under the ingress context, the specified traffic descriptor profile defines the traffic contract in the forward direction. When configured under the egress context, the specified traffic descriptor profile defines the traffic contract in the backward direction.

The **no** form of the command reverts the traffic descriptor to the default traffic descriptor profile.

Default The default traffic descriptor (trafficDescProfileId. = 1) is associated with newly created PVCC-delimited SAPs.

Parameters *traffic-desc-profile-id* — Specify a defined traffic descriptor profile (see the QoS atm-td-profile command).

oam

Syntax **oam**

Context config>service>vprn>if >sap>atm
config>service>vprn>sub-if>grp-if>sap>atm

Description This command enables the context to configure OAM functionality for a PVCC delimiting a SAP.

The ATM-capable MDAs support F5 end-to-end OAM functionality (AIS, RDI, Loopback):

- ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance Principles and Functions version 11/95
- GR-1248-CORE - Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996
- GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994

alarm-cells

Syntax [**no**] **alarm-cells**

Context config>service>vprn>if>sap>atm>oam
config>service>vprn>sub-if>grp-if>sap>atm>oam

Description This command configures AIS/RDI fault management on a PVCC. Fault management allows PVCC termination to monitor and report the status of their connection by propagating fault information through the network and by driving PVCC's operational status.

When alarm-cells functionality is enabled, a PVCC's operational status is affected when a PVCC goes into an AIS or RDI state because of an AIS/RDI processing (assuming nothing else affects PVCC's operational status, for example, if the PVCC goes DOWN, or enters a fault state and comes back UP, or exits that fault state). RDI cells are generated when PVCC is operationally DOWN. No OAM-specific SNMP trap is raised whenever an endpoint enters/exits an AIS or RDI state, however, if as result of an OAM state change, the PVCC changes operational status, then a trap is expected from an entity the PVCC is associated with (for example a SAP).

The **no** command disables alarm-cells functionality for a PVCC. When alarm-cells functionality is disabled, a PVCC's operational status is no longer affected by a PVCC's OAM state changes due to AIS/RDI processing (note that when alarm-cells is disabled, a PVCC will change operational status to UP due to alarm-cell processing) and RDI cells are not generated as result of the PVCC going into AIS or RDI state. The PVCC's OAM status, however, will record OAM faults as described above.

Default Enabled for PVCCs delimiting VPRN SAPs

periodic-loopback

Syntax [**no**] **periodic-loopback**

Context config>service>vprn>if >sap>atm>oam
config>service>vprn>sub-if>grp-if>sap>atm

Description This command enables periodic OAM loopbacks on this SAP. This command is only configurable on VPRN SAPs. When enabled, an ATM OAM loopback cell is transmitted every period as configured in the `config>system>atm>oam>loopback-period` *`period`* context.

If a response is not received and consecutive retry-down retries also result in failure, the endpoint will transition to an alarm indication signal/loss of clock state. Then, an ATM OAM loopback cell will be transmitted every period as configured in the `loopback-period` *`period`*. If a response is

received for the periodic loopback and consecutive retry-up retries also each receive a response, the endpoint will transition back to the up state.

The **no** form of the command sets the value back to the default.

Default no periodic-loopback

Interface Anti-Spoofing Commands

anti-spoof

Syntax **anti-spoof** {**ip** | **mac** | **ip-mac** | **nh-mac**}
no anti-spoof-type

Context config>service>vprn>if>sap
config>service>vprn>sub-if>grp-if>sap

Description This command enables anti-spoof filtering and optionally changes the anti-spoof matching type for the interface.

The type of anti-spoof filtering defines what information in the incoming packet is used to generate the criteria to lookup an entry in the anti-spoof filter table. The type parameter (**ip**, **mac**, **ip-mac, nh-mac**) defines the anti-spoof filter type enforced by the SAP when anti-spoof filtering is enabled.

The **no** form of the command disables anti-spoof filtering on the SAP.

Default Filter type default types:

- Non-Ethernet encapsulation default anti-spoof filter type — When enabled on a non-Ethernet encapsulated SAP, the anti-spoof filter default type is **ip**.
- Ethernet encapsulated default anti-spoof filter type — When enabled on an Ethernet encapsulated SAP, the anti-spoof default type is **ip-mac**.
- Default anti-spoof filter state — Anti-spoof filtering is disabled by default on the SAP.

Parameters **ip —** Configures SAP anti-spoof filtering to use only the source IP address in its lookup. If a static host exists on the SAP without an IP address specified, the anti-spoof type **ip** command will fail.

mac — Configures SAP anti-spoof filtering to use only the source MAC address in its lookup. Setting the anti-spoof filter type to **mac** is not allowed on non-Ethernet encapsulated SAPs. If a static host exists on the SAP without a specified MAC address, the anti-spoof type **mac** command will fail. The anti-spoof type **mac** command will also fail if the SAP does not support Ethernet encapsulation.

ip-mac — Configures SAP anti-spoof filtering to use both the source IP address and the source MAC address in its lookup. If a static host exists on the SAP without both the IP address and MAC address specified, the anti-spoof type **ip-mac** command will fail. This is also true if the default anti-spoof filter type of the SAP is **ip-mac** and the default is not overridden. The anti-spoof type **ip-mac** command will also fail if the SAP does not support Ethernet encapsulation.

nh-mac — Indicates that the ingress anti-spoof is based on the source MAC address and the egress anti-spoof is based on the nh-ip-address.

app-profile

Syntax **app-profile** *app-profile-name*

no app-profile

Context config>service>vprn>if>sap
config>service>vprn>sub-if>grp-if>sap

Description This command configures the application profile name.

Parameters *app-profile-name* — Specifies an existing application profile name configured in the **config>app-assure>group>policy** context.

arp-populate

Syntax [**no**] **arp-populate**

Context config>service>vprn>if
config>service>vprn>sub-if>subscriber-interface
config>service>vprn>sub-if>grp-if

Description This command enables populating static and dynamic hosts into the system ARP cache. When enabled, the host's IP address and MAC address are placed in the system ARP cache as a managed entry. Static hosts must be defined on the interface using the **host** command. Dynamic hosts are enabled on the system through enabling lease-populate in the IP interface DHCP context. In the event that both a static host and a dynamic host share the same IP and MAC address, the system's ARP cache retains the host information until both the static and dynamic information are removed. Both static and dynamic hosts override static ARP entries. Static ARP entries are marked as inactive when they conflict with static or dynamic hosts and will be repopulated once all static and dynamic host information for the IP address are removed. Since static ARP entries are not possible when static subscriber hosts are defined or when DHCP lease state table population is enabled, conflict between static ARP entries and the arp-populate function is not an issue.

The **arp-populate** command will fail if an existing static subscriber host on the SAP does not have both MAC and IP addresses specified.

Once **arp-populate** is enabled, creating a static subscriber host on the SAP without both an IP address and MAC address will fail.

arp-populate can only be enabled on VPRN interfaces supporting Ethernet encapsulation.

Use the **no** form of the command to disable ARP cache population functions for static and dynamic hosts on the interface. All static and dynamic host information in the systems ARP cache will be removed. Any existing static ARP entries previously inactive due to static or dynamic hosts will be populated in the system ARP cache.

When **arp-populate** is enabled, the system will not send out ARP Requests for hosts that are not in the ARP cache. Only statically configured and DHCP learned hosts are reachable through an IP interface with arp-populate enabled.

Default not enabled

arp-timeout

Syntax **arp-timeout** *seconds*

no arp-timeout

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if

Description This command configures the minimum time in seconds an ARP entry learned on the IP interface will be stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host, otherwise, the ARP entry is aged from the ARP table. If **arp-timeout** is set to a value of zero seconds, ARP aging is disabled.

The **no** form of this command restores **arp-timeout** to the default value.

Default 14400 seconds

Parameters *seconds* — The minimum number of seconds a learned ARP entry will be stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries will not be aged.

Values 0 — 65535

authentication-policy

Syntax **authentication-policy** *name*
no authentication-policy

Context config>service>vprn>if
config>service>vprn>sub-if>grp-if

Description This command assigns an authentication policy to the interface.

The **no** form of this command removes the policy name from the group interface configuration.

Default no authentication-policy

Parameters *name* — Specifies the authentication policy name. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

delayed-enable

Syntax **delayed-enable** *seconds* [**init-only**]
no delayed-enable

Context config>service>vprn>sub-if>grp-if
config>service>vprn>nw-if

Description This command delays making interface operational by the specified number of seconds.

In environments with many subscribers, it can take time to synchronize the subscriber state between peers when the subscriber-interface is enabled (perhaps, after a reboot). To ensure that the state has time to be synchronized, the **delayed-enable** timer can be specified. The optional parameter **init-only** can be added to use this timer only after a reboot.

Default no delayed-enable

Parameters *seconds* — Specifies the number of seconds to delay before the interface is operational.

Values 1 — 1200

init-only — Delays the initialization of the subscriber-interface to give the rest of the system time to complete necessary tasks such as allowing routing protocols to converge and/or to allow MCS to sync the subscriber information. The delay only occurs immediately after a reboot.

calling-station-id

Syntax **calling-station-id** *calling-station-id*
no calling-station-id

Context config>service>vprn>sub-if>grp-if>sap
config>service>vprn>if>sap

Description This command enables the inclusion of the **calling-station-id** attribute in RADIUS authentication requests and RADIUS accounting messages. The value inserted is set at the SAP level. If no value is set at the SAP level, an empty string is included.

Default This attribute is not sent by default.

host

Syntax [**no**] **host** {[**ip** *ip-address* [**mac** *ieee-address*]} [**subscriber** *sub-ident-string*] [**sub-profile** *sub-profile-name*] [**sla-profile** *sla-profile-name*]
no host {[**ip** *ip-address*] [**mac** *ieee-address*]}

Context config>service>vprn>if>sap

Description This command creates a static host for the SAP. Applications within the system that make use of static host entries include anti-spoof, and source MAC population into the VPLS forwarding database.

Multiple static hosts can be defined on the SAP. Each host is identified by a source IP address, a source MAC address, or both a source IP and source MAC address. When anti-spoof in enabled on the SAP, the host information will be populated into the SAP's anti-spoof table, allowing ingress packets matching the entry access to the SAP. When the MAC address exists in the host definition, the MAC address is populated into the VPLS forwarding database and associates it with the SAP. The static host definition overrides any static MAC entries using the same MAC and prevents dynamic learning of the MAC on another interface.

Defining a static host identical to an existing static host has no effect and will not generate a log or error message.

Every static host definition must have at least one address defined, IP or MAC.

Static hosts may exist on the SAP even with anti-spoof and **arp-populate** (VPRN) features disabled. When enabled, each feature has different requirements for static hosts.

anti-spoof — When enabled, this feature uses static and dynamic host information to populate entries into an anti-spoof filter table. The anti-spoof filter entries generated will be of the same type as specified in the anti-spoof type parameter. If the SAP anti-spoof filter is defined as mac, each

static host definition must specify a MAC address. If the SAP anti-spoof filter is defined as ip, each static host definition must specify an IP address. If the SAP anti-spoof filter is defined as ip-mac, each static host definition must specify both an IP address and MAC address. If definition of a static host is attempted without the appropriate addresses specified for the enabled anti-spoof filter, the static host definition will fail.

arp-populate — When enabled, this feature uses static and dynamic host information to populate entries into the system's ARP cache. This is only available on the VPRN service SAPs. Both a MAC address and IP address are required to populate an ARP entry in the system. If definition of a static host is attempted without both a MAC and IP address specified when arp -populate is enabled, the static host definition will fail.

fdb-populate — This is an implicit feature that uses the static host definition as a static MAC in the VPLS forwarding database. It cannot be enabled or disabled and has no effect on the ability to create static hosts without a MAC address specified. When a MAC address is specified for a static host, it will automatically be populated into the VPLS forwarding database associated with the SAP on which the host is created. The static host MAC address will override any static MAC entries using the same MAC and prevent dynamic learning of the MAC on another interface. Existing static MAC entries with the same MAC address as a static host are marked as inactive but not deleted. If all static hosts are removed from the SAP, the static MAC may be populated. New static MAC definitions for the VPLS instance may be created while a static host exists associated with the static MAC address.

The **no** form of the command removes a static entry from the system. The specified **ip** *address* and **mac** *address* must match the host's exact IP and MAC addresses as defined when it was created. When a static host is removed from the SAP, the affect of its removal on the anti-spoof filter, ARP cache or the VPLS forwarding database is also evaluated.

Default There are no default static entries.

Parameters **ip** ***ip-address*** **—** Specify this optional parameter when defining a static host. The IP address must be specified for **anti-spoof** *ip* and **anti-spoof** *ip-mac* commands. Only one static host can be configured on the SAP with a given IP address.
The following rules apply to configure static hosts using an IP address:

- Only one static host can be defined using a specific IP address.
- Defining a static host with the same IP address as a previous static host overwrites the previous static host.
- If a static host has an IP address assigned, the MAC address for the host is optional (depending on the features enabled on the SAP).

mac mac-address **—** Specify this optional parameter when defining a static host. The MAC address must be specified for **anti-spoof** *mac*, and **anti-spoof** *ip-mac*. Multiple static hosts may be configured with the same MAC address given that each definition is distinguished by a unique IP address. The following rules apply to configuring static hosts using a MAC address:

- Multiple static hosts may share the same MAC address.
- Executing the host command with the same MAC address but a different IP address as an existing static host will create a new static host.
- If a static host has a MAC address assigned, the IP address for the host is optional (depending on the features enabled on the SAP).

Values 8k static and dynamic hosts per 10G forwarding complex. 64k8k per system.

subscriber *sub-ident-string* — Specify this optional parameter to specify an existing subscriber identification profile to be associated with the static subscriber host. The subscriber identification profile is configured in the **config>subscr-mgmt>sub-ident-policy** context. The subscriber information is used by the VPRN SAP arp-reply-agent to determine the proper handling of received ARP requests from subscribers.

- For VPRN SAPs with **arp-reply-agent** enabled with the optional *sub-ident* parameter, the static subscriber host's sub-ident-string is used to determine whether an ARP request received on the SAP is sourced from a host belonging to the same subscriber as the destination host. When both the destination and source hosts from the ARP request are known on the SAP and the subscriber identifications do not match, the ARP request may be forwarded to the rest of the VPRN destinations.

  If the static subscriber host's *sub-ident* string is not defined, the host is not considered to belong to the same subscriber as another host on the SAP.

  If source or destination host is unknown, the hosts are not considered to belong to the same subscriber. ARP messages from unknown hosts are subject to anti-spoof filtering rules applied at the SAP.

  If *sub-ident* is not enabled on the SAP arp-reply-agent, subscriber identification matching is not performed on ARP requests received on the SAP.

  ARP requests are never forwarded back to the same SAP or within the receiving SAP's split horizon group.

sub-profile *sub-profile-name* — Specify this optional parameter to specify an existing subscriber profile name to be associated with the static subscriber host. The subscriber profile is configured in the **config>subscr-mgmt>sub-profile** context.

sla-profile *sla-profile-name* — Specify this optional parameter to specify an existing SLA profile name to be associated with the static subscriber host. The SLA profile is configured in the **config>subscr-mgmt>sla-profile** context.

frame-relay

Syntax **frame-relay**

Context config>service>vprn>if>sap

Description This command enables the context to configure Frame Relay parameters on the SAP.

frf-12

Syntax [**no**] **frf-12**

Context config>service>vprn>if>sap

Description This command enables the use of FRF12 headers.

The **no** form of the command disables the use of FRF12 headers.

ete-fragment-threshold

Syntax **ete-fragment-threshold** *threshold*
no ete-fragment-threshold

Context config>service>vprn>if>sap>frf-12

Description This command specifies the maximum length of a fragment to be transmitted.

The **no** form of the command reverts to the default.

Parameters *threshold* — Specifies the maximum length of a fragment to be transmitted.

Values 128 — 512

Default 0

interleave

Syntax [**no**] **interleave**

Context config>service>vprn>if>sap>frame-relay>frf.12

Description This command enables interleaving of high priority frames and low-priority frame fragments within a FR SAP using FRF.12 end-to-end fragmentation.

When this option is enabled, only frames of the FR SAP non expedited forwarding class queues are subject to fragmentation. The frames of the FR SAP expedited queues are interleaved, with no fragmentation header, among the fragmented frames. In effect, this provides a behavior like in MLPPP Link Fragment Interleaving (LFI).

When this option is disabled, frames of all the FR SAP forwarding class queues are subject to fragmentation. The fragmentation header is however not included when the frame size is smaller than the user configured fragmentation size. In this mode, the SAP transmits all fragments of a frame before sending the next full or fragmented frame.

The receive direction of the FR SAP supports both modes of operation concurrently, with and without fragment interleaving.

The **no** form of this command restores the default mode of operation.

Default no interleave

scheduling-class

Syntax **scheduling-class** *class-id*

Context config>service>vprn>if>sap

Description This command specifies the scheduling class to use for this SAP.

Parameters *class-id* — Specifies the scheduling class to use for this SAP.

Values 0 — 3

Default 0

flowspec

Syntax **flowspec**
no flowspec

Context config>service>vprn>interface>sap>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>ies>interface>sap>ingress
config>service>ies>interface>spoke-sdp>ingress

Description This command enables IPv4 flowspec filtering on an access IP interface associated with a VPRN or IES service. Filtering is based on all of the IPv4 flowspec routes that have been received and accepted by the corresponding BGP instance. Ingress IPv4 traffic on an interface can be filtered by both a user-defined IPv4 filter and flowspec. Evaluation proceeds in this order:

1. user-defined IPv4 filter entries
2. flowspec-derived filter entries
3. user-defined IPv4 filter default-action

The **no** form of the command removes IPv4 flowspec filtering from an IP interface.

Default No access interfaces have IPv4 flowspec enabled.

flowspec-ipv6

Syntax **flowspec-ipv6**
no flowspec-ipv6

Context config>service>vprn>interface>sap>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>ies>interface>sap>ingress
config>service>ies>interface>spoke-sdp>ingress

Description This command enables IPv6 flowspec filtering on an access IP interface associated with a VPRN or IES service. Filtering is based on all of the IPv6 flowspec routes that have been received and accepted by the corresponding BGP instance. Ingress IPv6 traffic on an interface can be filtered by both a user-defined IPv6 filter and flowspec. Evaluation proceeds in this order:

1. user-defined IPv6 filter entries
2. flowspec-derived filter entries
3. user-defined IPv6 filter default-action

The **no** form of the command removes IPv6 flowspec filtering from an IP interface.

Default No access interfaces have IPv6 flowspec enabled.

host-lockout-policy

Syntax **host-lockout-policy** *policy-name*
no host-lockout-policy

Context config>service>vprn>if>sap

Description This command configures a host lockout policy.

The no form of the command removes the policy name from the configuration.

host-shutdown

Syntax [**no**] **host-shutdown**

Context config>service>vprn>if>sap

This command administratively enables host creation on this SAP.

ip-tunnel

Syntax **ip-tunnel** *name* [**create**]
no ip-tunnel *name*

Context config>service>vprn>if>sap

Description This command is used to configure an IP-GRE or IP-IP tunnel and associate it with a private tunnel SAP within an IES or VPRN service.

The no form of the command deletes the specified IP/GRE or IP-IP tunnel from the configuration. The tunnel must be administratively shutdown before issuing the no ip-tunnel command.

Default No IP tunnels are defined.

Parameters *ip-tunnel-name* — Specifies the name of the IP tunnel. Tunnel names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

backup-remote-ip

Syntax **backup-remote-ip** *ip-address*
no backup-remote-ip

Context config>service>interface>vprn>sap>ip-tunnel

Description This command sets the backup destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If the primary destination address is not reachable in the delivery service (there is no route) or not defined then this is the destination IPv4 address of GRE encapsulated

packets sent by the delivery service.

The **no** form of the command deletes the backup-destination address from the GRE tunnel configuration.

Parameters *ip-address* — Specifies the destination IPv4 address of the GRE tunnel.

Values 1.0.0.0 — 223.255.255.255

delivery-service

Syntax **delivery-service** {*service-id* | *svc-name*}
no delivery-service

Context config>service>interface>vprn>sap>ip-tunnel

Description This command sets the delivery service for GRE encapsulated packets associated with a particular GRE tunnel. This is the IES or VPRN service where the GRE encapsulated packets are injected and terminated. The delivery service may be the same service that owns the private tunnel SAP associated with the GRE tunnel. The GRE tunnel does not come up until a valid delivery service is configured.

The **no** form of the command deletes the delivery-service from the GRE tunnel configuration.

Parameters *service-id* — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel.

Values 1—2147483648

svc-name — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel.

Values 1—64 characters

dscp

Syntax **dscp** *dscp-name*
no dscp

Context config>service>interface>vprn>sap>ip-tunnel

Description This command sets the DSCP code-point in the outer IP header of GRE encapsulated packets associated with a particular GRE tunnel. The default, set using the no form of the command, is to copy the DSCP value from the inner IP header (after remarking by the private tunnel SAP egress qos policy) to the outer IP header.

Default no dscp

Parameters *dscp* — Specifies the DSCP code-point to be used.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43,

cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

source

Syntax **source** *ip-address*
no source

Context config>service>interface>vprn>sap>ip-tunnel

Description This command sets the source IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. It must be an address in the subnet of the associated public tunnel SAP interface. The GRE tunnel does not come up until a valid source address is configured.

The **no** form of the command deletes the source address from the GRE tunnel configuration. The tunnel must be administratively shutdown before issuing the **no source** command.

Parameters *ip-address* — Specifies the source IPv4 address of the GRE tunnel.

Values 1.0.0.0 — 223.255.255.255

remote-ip

Syntax **remote-ip** *ip-address*
no remote-ip

Context config>service>interface>vprn>sap>ip-tunnel

Description This command sets the primary destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If this address is reachable in the delivery service (there is a route) then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.

The **no** form of the command deletes the destination address from the GRE tunnel configuration.

Parameters *ip-address* — Specifies the destination IPv4 address of the GRE tunnel.

Values 1.0.0.0 — 223.255.255.255

Interface SAP Filter and QoS Policy Commands

egress

Syntax **egress**

Context config>service>vprn>if>sap
config>service>vprn>sub-if>grp-if>sap
config>service>vprn>ipsec-if>sap

Description This command enables the context to configure egress SAP Quality of Service (QoS) policies and filter policies.

If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing. If no egress filter is defined, no filtering is performed.

ingress

Syntax **ingress**

Context config>service>vprn>if>sap
config>service>vprn>sub-if>grp-if>sap
config>service>vprn>if>sap
config>service>vprn>ipsec-if>sap

Description This command enables the context to configure ingress SAP Quality of Service (QoS) policies and filter policies.

If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing. If no ingress filter is defined, no filtering is performed.

agg-rate-limit

Syntax **agg-rate-limit** *agg-rate* [**queue-frame-based-accounting**]
no agg-rate-limit

Context config>service>vprn>if>sap>egress
config>service>vprn>sub-if>grp-if>sap>egress
config>service>vprn>ipsec-if>sap>egress

Description This command defines a maximum total rate for all egress queues on a service SAP or multi-service site. The **agg-rate-limit** command is mutually exclusive with the egress scheduler policy. When an egress scheduler policy is defined, the **agg-rate-limit** command will fail. If the **agg-rate-limit** command is specified, an attempt to bind a **scheduler-policy** to the SAP or multi-service site will fail.

A multi-service site must have a port scope defined that ensures all queues associated with the site are on the same port or channel. If the scope is not set to a port, the agg-rate-limit command will fail.

Once an agg-rate-limit has been assigned to a multi-service site, the scope cannot be changed to card level.

A port scheduler policy must be applied on the egress port or channel the SAP or multi-service site is bound to in order for the defined agg-rate-limit to take effect. The egress port scheduler enforces the aggregate queue rate as it distributes its bandwidth at the various port priority levels. The port scheduler stops offering bandwidth to member queues once it has detected that the aggregate rate limit has been reached.

If a port scheduler is not defined on the egress port, the queues are allowed to operate based on their own bandwidth parameters.

The **no** form of the command removes the aggregate rate limit from the SAP or multi-service site.

Parameters *agg-rate* — Defines the rate, in kilobits-per-second, that the maximum aggregate rate that the queues on the SAP or multi-service site can operate.

Values 1 — 40000000, max

queue-frame-based-accounting — This keyword enables frame based accounting on all queues associated with the SAP or Multi-Service Site. If frame based accounting is required when an aggregate limit is not necessary, the max keyword should precede the queue-frame-based-accounting keyword. If frame based accounting must be disabled, execute agg-rate-limit without the queue-frame-based-accounting keyword present.

Default Frame based accounting is disabled by default

filter

Syntax **filter ip** *ip-filter-id*
no filter

Context config>service>vprn>if>sap>egress
config>service>vprn>if>sap>ingress
config>service>vprn>sub-if>grp-if>sap>egress
config>service>vprn>ipsec-if>sap>egress
config>service>vprn>ipsec-if>sap>ingress

Description This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface. Filter policies control the forwarding and dropping of packets based on IP matching criteria.

The **filter** command is used to associate a filter policy with a specified *ip-filter-id* with an ingress or egress SAP. The *ip-filter-id* must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

Parameters **ip** *ip-filter-id* — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 — 65535

flowspec

[**no**] **flowspec**

Context config>service>vprn>interface>sap>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>vprn>network-interface>ingress

Description This command enables flowspec filtering on an IP interface of a VPRN. Filtering is based on all of the flowspec routes that have been received and accepted by the VPRN. Ingress traffic on an IP interface can be filtered by both a user-defined ip filter and flowspec. Evaluation proceeds in this order:

1. user-defined ip filter entries with entry numbers less than the configured insert-point
2. flowspec-derived filter entries
3. user-defined ip filter entries with entry numbers greater than or equal to the configured insert-point
4. ip-filter default-action

The **no** form of the command removes flowspec filtering from an IP interface.

Default No interfaces have flowspec enabled.

flowspec-ipv6

Syntax [**no**] **flowspec-ipv6**

Context config>service>vprn>interface>sap>ingress
config>service>vprn>interface>spoke-sdp>ingress

Description This command enables flowspec filtering on an IP interface of the base router. Filtering is based on all of the flowspec routes that have been received and accepted by the base router. Ingress traffic on an IP interface can be filtered by both a user-defined ip filter and flowspec. In this case, the user-defined ip filter entries are evaluated before the flowspec routes and the default action of the user-defined ip filter applies as the very last rule.

The **no** form of the command removes flowspec filtering from an IP interface.

Default No interfaces have flowspec enabled.

hsmda-queue-override

Syntax [**no**] **hsmda-queue-override**

Context config>service>vprn>if>sap>egress

Description This command enables the context to configure HSMDA queue overrides.

queue

Syntax **queue** *queue-id* [**create**]
no queue *queue-id*

Context config>service>vprn>if>sap>egress>hsmda-queue-overider

Description This command configures overrides for a HSMDA queue. The actual valid values are those defined in the given SAP QoS policy.

Parameters *queue-id* — Specifies the queue ID to override.

Values 1 — 8

create — This keyword is mandatory while creating a new queue override.

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context config>service>vprn>if>sap>egress>hsmda-queue-overider

Description This command adds or subtracts the specified number of bytes to the accounting function for each packet handled by the HSMDA queue. Normally, the accounting and leaky bucket functions are based on the Ethernet DLC header, payload and the 4 byte CRC (everything except the preamble and inter-frame gap). As an example, the packet-byte-offset command can be used to add the frame encapsulation overhead (20 bytes) to the queues accounting functions.

The accounting functions affected include:

- Offered High Priority / In-Profile Octet Counter
- Offered Low Priority / Out-of-Profile Octet Counter
- Discarded High Priority / In-Profile Octet Counter
- Discarded Low Priority / Out-of-Profile Octet Counter
- Forwarded In-Profile Octet Counter
- Forwarded Out-of-Profile Octet Counter
- Peak Information Rate (PIR) Leaky Bucket Updates
- Committed Information Rate (CIR) Leaky Bucket Updates
- Queue Group Aggregate Rate Limit Leaky Bucket Updates

The secondary shaper leaky bucket, scheduler priority level leaky bucket and the port maximum rate updates are not affected by the configured packet-byte-offset. Each of these accounting functions are

frame based and always include the preamble, DLC header, payload and the CRC regardless of the configured byte offset.

The packet-byte-offset command accepts either add or subtract as valid keywords which define whether bytes are being added or removed from each packet traversing the queue. Up to 31 bytes may be added to the packet and up to 32 bytes may be removed from the packet. An example use case for subtracting bytes from each packet is an IP based accounting function. Given a Dot1Q encapsulation, the command packet-byte-offset subtract 14 would remove the DLC header and the Dot1Q header from the size of each packet for accounting functions only. The 14 bytes are not actually removed from the packet, only the accounting size of the packet is affected.

As inferred above, the variable accounting size offered by the packet-byte-offset command is targeted at the queue and queue group level. The packet-byte-offset, when set, applies to all queues in the quee group. The accounting size of the packet is ignored by the secondary shapers, the scheduling priority level shapers and the scheduler maximum rate. The actual on-the-wire frame size is used for these functions to allow an accurate representation of the behavior of the subscriberís packets on an Ethernet aggregation network.

The packet-byte-offset value may be overridden at the queue-group level.

Parameters **add** *add-bytes* **—** Indicates that the byte value should be added to the packet for queue and queue group level accounting functions. Either the **add** or **subtract** keyword must be specified. The corresponding byte value must be specified when executing the packet-byte-offset command. The **add** keyword is mutually exclusive with the **subtract** keyword.

Values 0 — 31

subtract *sub-bytes* **—** Indicates that the byte value should be subtracted from the packet for queue and queue group level accounting functions. The **subtract** keyword is mutually exclusive with the **add** keyword. Either the **add** or **subtract** keyword must be specified. The corresponding byte value must be specified when executing the packet-byte-offset command.

Values 1 — 32

slope-policy

Syntax **slope-policy** *hsmda-slope-policy-name*
no slope-policy

Context config>service>vprn>if>sap>egress>hsmda-queue-overider

Description This command specifies an existing slope policy name.

wrr-weight

Syntax **wrr-weight** *value*
no wrr-weight

Context config>service>vprn>if>sap>egress>hsmda-queue-overider>queue

Description This command assigns the weight value to the HSMDA queue.

The **no** form of the command returns the weight value for the queue to the default value.

Parameters *percentage* — Specifies the weight for the HSMDA queue.

Values 1— 32

wrr-policy

Syntax **wrr-policy** *hsmda-wrr-policy-name*
no wrr-policy

Context config>service>vprn>if>sap>egress>hsmda-queue-overider

Description This command associates an existing HSMDA weighted-round-robin (WRR) scheduling loop policy to the HSMDA queue.

Parameters *hsmda-wrr-policy-name* — Specifies the existing HSMDA WRR policy name to associate to the queue.

secondary-shaper

secondary-shaper *secondary-shaper-name*
no secondary-shaper

Context config>service>vprn>if>sap>egress>hsmda-queue-overider

Description This command configures an HSMDA secondary shaper. Note that an shaper override can only be configured on an HSMDA SAP.

Parameters *secondary-shaper-name* — Specifies a secondary shaper name up to 32 characters in length.

match-qinq-dot1p

Syntax **match-qinq-dot1p** {**top** | **bottom**}
no match-qinq-dot1p

Context config>service>vprn>if>sap>ingress
config>service>vprn>sub-if>grp-if>sap>ingress
config>service>vprn>ipsec-if>sap>ingress

Description This command specifies which Dot1Q tag position Dot1P bits in a QinQ encapsulated packet should be used to evaluate Dot1P QoS classification.

The **match-qinq-dot1p** command allows the top or bottom PBits to be used when evaluating the applied sap-ingress QoS policy's Dot1P entries. The **top** and **bottom** keywords specify which position should be evaluated for QinQ encapsulated packets.

The **no** form of the command restores the default dot1p evaluation behavior for the SAP.

By default, the bottom most service delineating Dot1Q tags Dot1P bits are used. The following table defines the default behavior for Dot1P evaluation when the **match-qinq-dot1p** command is not executed.

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN-ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	TopQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None
Dot1Q	Dot1P (Default SAP VLAN-ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	TopQ PBits
QinQ / QinQ	TopQ BottomQ	BottomQ PBits

Default no match-qinq-dot1p - No filtering based on p-bits.
top or bottom must be specified to override the default QinQ dot1p behavior.

Parameters **top —** The top parameter is mutually exclusive to the bottom parameter. When the top parameter is specified, the top most PBits are used (if existing) to match any dot1p dot1p-value entries. The following table defines the dot1p evaluation behavior when the top parameter is specified.

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN-ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	TopQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None
Dot1Q	Dot1P (Default SAP VLAN-ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	TopQ PBits

bottom — The bottom parameter is mutually exclusive to the top parameter. When the bottom parameter is specified, the bottom most PBits are used (if existing) to match any dot1p dot1p-value entries. The following tables define the bottom position QinQ and TopQ SAP dot1p evaluation and the default dot1p explicit marking actions.

Table 30: Bottom Position QinQ and TopQ SAP Dot1P Evaluation

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN-ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	BottomQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None
Dot1Q	Dot1P (Default SAP VLAN-ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	BottomQ PBits
QinQ / QinQ	TopQ BottomQ	BottomQ PBits

Egress SAP Type	Ingress Packet Preserved Dot1P State	Marked (or Remarked) PBits
Null	No preserved Dot1P bits	None
Null	Preserved Dot1P bits	Preserved tag PBits remarked using dot1p-value
Dot1Q	No preserved Dot1P bits	New PBits marked using dot1p-value
Dot1Q	Preserved Dot1P bits	Preserved tag PBits remarked using dot1p-value
TopQ	No preserved Dot1P bits	TopQ PBits marked using dot1p-value
TopQ	Preserved Dot1P bits (used as TopQ and BottomQ PBits)	TopQ PBits marked using dot1p-value, BottomQ PBits preserved
QinQ	No preserved Dot1P bits	TopQ PBits and BottomQ PBits marked using dot1p-value

Egress SAP Type	Ingress Packet Preserved Dot1P State	Marked (or Remarked) PBits
QinQ	Preserved Dot1P bits (used as TopQ and BottomQ PBits)	TopQ PBits and BottomQ PBits marked using dot1p-value

The dot1p dot1p-value command must be configured without the qinq-mark-top-only parameter to remove the TopQ PBits only marking restriction.

qinq-mark-top-only

Syntax [**no**] **qinq-mark-top-only**

Context config>service>vprn>if>sap>egress
config>service>vprn>sub-if>grp-if>sap>engress
config>service>vprn>ipsec-if>sap>egress

Description When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the **qinq-mark-top-only** command specifies which P-bits/DEI bitto mark during packet egress. When disabled, both set of P-bits/DEI bit are marked. When the enabled, only the P-bits/DEI bit in the top Q-tag are marked.

Default no qinq-mark-top-only

qos

Syntax **qos** *policy-id* [**port-redirect-group** *queue-group-name* **instance** *instance-id*]
no qos

Context config>service>vprn>if>sap>egress
config>service>vprn>sub-if>grp-if>sap>engress
config>service>vprn>ipsec-if>sap>egress

Description

This command associates a Quality of Service (QoS) policy with an ingress or egress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP or IP interface. If the policy- id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, no specific QoS policy is associated with the SAP for ingress or egress, so the

default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Default none

Parameters *policy-id* — The ingress/egress policy ID to associate with SAP or IP interface on ingress/egress. The policy ID must already exist.

1 — 65535

port-redirect-group — This keyword associates a SAP egress with an instance of a named queue group template on the egress port of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command.

queue-group-name — Specifies the name of the egress port queue group of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid egress queue group, created under config>port>ethernet>access>egress.

instance *instance-id* **—** Specifies the instance of the named egress port queue group on the IOM/IMM/XMA.

Values 1 — 40960

Default 1

qos

Syntax **qos** *policy-id* [**shared-queuing** | **multipoint-shared**] **fp-redirect-group** *queue-group-name* **instance** *instance-id*
no qos

Context config>service>vprn>if>sap>ingress
config>service>vprn>sub-if>grp-if>sap>ingress
config>service>vprn>ipsec-if>sap>ingress

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy- id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Default none

Parameters *policy-id* — The ingress/egress policy ID to associate with SAP or IP interface on ingress/egress. The policy ID must already exist.

Values 1 — 65535

shared-queuing — Specifies the ingress shared queue policy used by this SAP. When the value of this object is null it means that the SAP will use individual ingress QoS queues instead of the shared ones.

multipoint-shared — This keyword specifies that this *queue-id* is for multipoint forwarded traffic only. This *queue-id* can only be explicitly mapped to the forwarding class multicast, broadcast, or unknown unicast ingress traffic. Attempting to map forwarding class unicast traffic to a multipoint queue generates an error; no changes are made to the current unicast traffic queue mapping.

A queue must be created as **multipoint**. The **multipoint** designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the **multipoint** keyword, an error is generated and the command will not execute.

The **multipoint** keyword can be entered in the command line on a pre-existing multipoint queue to edit *queue-id* parameters.

Default Present (the queue is created as non-multipoint).

Values **Multipoint** or not present.

fp-redirect-group — This keyword creates an instance of a named queue group template on the ingress forwarding plane of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command. The named queue group template can contain only policers. If it contains queues, then the command will fail.

queue-group-name — Specifies the name of the queue group template to be instantiated on the forwarding plane of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid ingress queue group template name, configured under *config>qos>queue-group-templates*.

instance-id — Specifies the instance of the named queue group to be created on the IOM/IMM/XMA ingress forwarding plane.

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context config>service>vprn>if>sap>ingress

config>service>vprn>if>sap>egress
config>service>vprn>sub-if>grp-if>sap>engress
config>service>vprn>sub-if>grp-if>sap>ingress
config>service>vprn>ipsec-if>sap>egress
config>service>vprn>ipsec-if>sap>ingress

Description This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the **config>qos>scheduler-policy** *scheduler-policy-name* context.

The **no** form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the ingress SAP queues associated with the customer site. Queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler. The SAPs that have ingress queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more queues. When the **no scheduler-policy** command is executed, the customer site ingress or egress node will not contain an applied scheduler policy.

scheduler-policy-name: — The *scheduler-policy-name* parameter applies an existing scheduler policy that was created in the **config>qos>scheduler-policy** *scheduler-policy-name* context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues created on associated SAPs.

Values Any existing valid scheduler policy name.

ipsec-gw

Syntax **ipsec-gw** *name*
no ipsec-gw

Context config>service>vprn>if>sap

Description This command configures the IPSec gateway.

Parameters *name* — Specifies the IPSec gateway name up to 32 characters in length.

cert

Syntax **cert**

Context config>service>vprn>if>sap>ipsec-gw

Description This command enables the context to configure certificate parameters.

cert

Syntax **cert** *filename*
no cert

Context config>service>vprn>if>sap>ipsec-gw>cert

Description This command configures the cert with local file URL.

Default none

Parameters *filename* — Specifies the local file URL of the certifiate to be used with this SAP IPSec tunnel.

key

Syntax **key** *filename*
no key

Context config>service>vprn>if>sap>ipsec-gw>cert

Description This command configures the key-pair file to be used for X.509 certificate authentication with this SAP IPSec tunnel.

Default none

Parameters *filename* — Specifies a key with the CA profile.

trust-anchor

Syntax **trust-anchor** *ca-profile-name*
no trust-anchor

Context config>service>vprn>if>sap>ipsec-gw>cert

Description This command configures the Certificate-Authority Profile name associated with this SAP IPSec tunnel certificate.

Default none

Parameters *ca-profile-name* — Specify a CA profile name up to 32 characters in length.

default-secure-service

Syntax **default-secure-service** *service-id* **ipsec-interface** *ip-int-name*
no default-secure-service

Context config>service>vprn>if>sap>ipsec-gw

Description This command specifies a service ID or service name of the default security service used by this SAP IPSec gateway.

Parameters *service-id* — Specifies a default secure service.

Values *service-id*: 1 — 2147483648
svc-name: Specifies an existing service name up to 64 characters in length.

default-tunnel-template

Syntax **default-tunnel-template** *ipsec template identifier*
no default-tunnel-template

Context config>service>vprn>if>sap>ipsec-gw

Description This command configures the default tunnel policy template for the gateway.

Parameters *ipsec template id** — [1..2048]

ike-policy

Syntax **ike-policy** *ike-policy-id*
no ike-policy

Context config>service>vprn>if>sap>ipsec-gw
config>service>vprn>ipsec-if>sap>tunnel>dynamic-keying

Description This command configures the IKE policy for the gateway.

Parameters *ike-policy-id* — Specifies the IKE policy ID.

Values 1 — 2048

local-gateway-address

Syntax **local-gateway-address** *ip-address*
no local-gateway-address

Context config>service>vprn>if>sap>ipsec-gw

Description This command configures the ipsec-gateway local address.

Parameters *ip-address* — Specifies the IP unicast address.

local-id

Syntax **local-id type** {**ipv4**|**fqdn**} [**value** [*value*]]
no local-id

Context config>service>vprn>if>sap>ipsec-gw

Description This command specifies the local ID of the router used for IDi or IDr for IKEv2 tunnels. The local-id can only be changed or removed when tunnel or gateway is shutdown.

Default: Depends on local-auth-method such as:

- Psk:local tunnel ip address
- Cert-auth: subject of the local certificate

Parameters **type** — Specifies the type of local ID payload, it could be ipv4 address/FQDN domain name/ distinguish name of subject in X.509 certificate.

Values ipv4 — Use ipv4 as the local ID type, the default value is the local tunnel end-point address.
fqdn — Use FQDN as the local ID type, the value must be configured.
dn — Use the subject of the certificate configured for the tunnel or gateway.

pre-shared-key

Syntax **pre-shared-key** *key*
no pre-shared-key

Context config>service>vprn>if>sap>ipsec-gw
config>service>vprn>ipsec-if>sap>tunnel>dynamic-keying

Description This command specifies the shared secret between the two peers forming the tunnel.

Parameters *key* — Specifies a pre-shared-key for dynamic-keying.

radius-accounting-policy

Syntax **radius-accounting-policy** *policy-name*
no radius-accounting-policy

Context

Description

radius-authentication-policy

Syntax **radius-authentication-policy** *name*
no radius-authentication-policy

Context

Description

lag-link-map-profile

Syntax **lag-link-map-profile** *lnk-map-profile-id*

no lag-link-map-profile

Context config>service>vprn>if>sap
config>service>vprn> sub-if>grp-if >sap

Description This command assigns a pre-configured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/de-assigned, the SAP/network interface egress traffic will be re-hashed over LAG as required by the new configuration.

The **no** form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

Default **no lag-link-map-profile**

Parameters *link-map-profile-id* — An integer from 1 to 32 that defines a unique lag link map profile on which the LAG the SAP/network interface exist.

multi-service-site

Syntax **multi-service-site** *customer-site-name*
no multi-service-site *customer-site-name*

Context config>service>vprn>if>sap
config>service>vprn>sub-if>grp-if>sap

Description This command creates a new customer site or edits an existing customer site with the *customer-site-name* parameter. A customer site is an anchor point to create an ingress and egress virtual scheduler hierarchy. When a site is created, it must be assigned to a chassis slot or port with the exception of the 7750 SR-1 in which the slot is set to 1. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs).

The scheduler policy association with the customer site normally prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site. The multi-service-site object will generate a log message indicating that the association was deleted due to scheduler policy removal.

When the multi-service customer site is created, an ingress and egress scheduler policy association does not exist. This does not prevent the site from being assigned to a chassis slot or prevent service SAP assignment. After the site has been created, the ingress and egress scheduler policy associations can be assigned or removed at any time.

Default None — Each customer site must be explicitly created.

Parameters *customer-site-name:* — Each customer site must have a unique name within the context of the customer. If *customer-site-name* already exists for the customer ID, the CLI context changes to that site name for the purpose of editing the site scheduler policies or assignment. Any modifications made to an existing site will affect all SAPs associated with the site. Changing a scheduler policy association may cause new schedulers to be created and existing queues on the SAPs to no longer be orphaned. Existing schedulers on the site may cease to exist, causing queues relying on that scheduler to be orphaned.

If the *customer-site-name* does not exist, it is assumed that an attempt is being made to create a site of that name in the customer ID context. The success of the command execution depends on the following:

- The maximum number of customer sites defined for the chassis slot has not been met.
- The *customer-site-name* is valid.
- The **create** keyword is included in the command line syntax (if the system requires it).

When the maximum number of customer sites has been exceeded a configuration error occurs; the command will not execute and the CLI context will not change.

If the *customer-site-name* is invalid, a syntax error occurs; the command will not execute and the CLI context will not change.

Values Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

static-host

Syntax **static-host ip** *ip/did-address* [**mac** *ieee-address*] [**create**]
static-host mac *ieee-address* [**create**]
no static-host [**ip** *ip-address*>] **mac** *ieee-address*>
no static-host all [**force**]
no static-host ip *ip-address*

Context config>service>vprn>if>sap
config>service>vprn>sub-if>grp-if>sap

Description This command configures a static host on this SAP.

Syntax **ip** *ip-address* **—** Specifies the IPv4 unicast address.

mac *ieee-address* — Specify this optional parameter when defining a static host. Every static host definition must have at least one address defined, IP or MAC.

force — Specifies the forced removal of the static host addresses.

sla-profile *sla-profile-name*

This optional parameter is used to specify an existing SLA profile name to be associated with the static subscriber host. The SLA profile is configured in the **config>subscr-mgmt>sla-profile** context.

ancp-string

Syntax **ancp-string** *ancp-string*
no ancp-string

Context config>service>vprn>if>sap>static-host
config>service>vprn>sub-if>grp-if>sap>static-host

Description This command specifies the ANCP string associated to this SAP host.

Parameters *ancp-string* — Specifies the ANCP string up to 63 characters in length.

app-profile

Syntax **app-profile** *app-profile-name*
no app-profile

Context config>service>vprn>if>sap>static-host
config>service>vprn>sub-if>grp-if>sap>static-host

Description This command specifies an application profile name.

Parameters *app-profile-name* — Specifies the application profile name up to 32 characters in length.

inter-dest-id

Syntax **inter-dest-id** *intermediate-destination-id*
no inter-dest-id

Context config>service>vprn>if>sap>static-host
config>service>vprn>sub-if>grp-if>sap>static-host

Description This command specifies to which intermediate destination (for example a DSLAM) this host belongs.

Parameters *intermediate-destination-id* — Specifies the intermediate destination ID.

managed-routes

Syntax **managed-routes**

Context config>service>vprn>sub-if>grp-if>sap>static-host>managed-routes

Description This command configures managed routes.

route

Syntax **route** {*ip-prefix/length* | *ip-prefix netmask*} [**create**]
no route {*ip-prefix/length* | *ip-prefix netmask*}

Context config>service>vprn>sub-if>grp-if>sap>static-host>managed-routes

Description This command assigns managed-route to a given subscriber-host. As a consequence, a static-route pointing subscriber-host ip address as a next hop will be installed in FIB. Up to 16 managed routes per subscriber-host can be configured.

The **no** form of the command removes the respective route. Per default, there are no managed-routes configured.

sla-profile

Syntax **sla-profile** *sla-profile-name*
no sla-profile

Context config>service>vprn>if>sap>static-host

Description This command specifies an existing SLA profile name to be associated with the static subscriber host. The SLA profile is configured in the **config>subscr-mgmt>sla-profile** context.

Parameters *sla-profile-name* — Specifies the SLA profile name.

sub-profile

Syntax **sub-profile** *sub-profile-name*
no sub-profile

Context config>service>vprn>if>sap>static-host

Description This command specifies an existing subscriber profile name to be associated with the static subscriber host.

Parameters *sub-profile-name* — Specifies the sub-profile name.

subscriber

Syntax **subscriber** *sub-ident*
no subscriber

Context config>service>vprn>if>sap>static-host

Description This command specifies an existing subscriber identification profile to be associated with the static subscriber host.

Parameters *sub-ident* — Specifies the subscriber identification/

subscriber-sap-id

Syntax [**no**] **subscriber-sap-id**

Context config>service>vprn>if>sap>static-host

Description This command enables using the SAP ID as subscriber id.

Parameters **subscriber-sap-id —** Specifies to use the sap-id as the subscriber-id.

queue-override

Syntax [**no**] **queue-override**

Context config>service>vprn>if>sap>egress
config>service>vprn>if>sap>ingress
config>service>vprn>ipsec-if>sap>egress
config>service>vprn>ipsec-if>sap>ingress

Description This command enables the context to configure override values for the specified SAP egress or ingress QoS queue. These values override the corresponding ones specified in the associated SAP egress or ingress QoS policy.

queue

Syntax [**no**] **queue** *queue-id*

Context config>service>vprn>if>sap>egress>queue-override
config>service>vprn>if>sap>ingress>queue-override
config>service>vprn>ipsec-if>sap>egress>queue-override
config>service>vprn>ipsec-if>sap>ingress>queue-override

Description This command specifies the ID of the queue whose parameters are to be overridden.

Parameters *queue-id* — The queue ID whose parameters are to be overridden.

Values 1 — 32

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]
no adaptation-rule

Context config>service>vprn>if>sap>egress>queue-override>queue
config>service>vprn>if>sap>ingress>queue-override>queue
config>service>vprn>ipsec-if>sap>egress>queue-override>queue
config>service>vprn>ipsec-if>sap>ingress>queue-override>queue

Description This command can be used to override specific attributes of the specified queue's adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The **no** form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default no adaptation-rule

Parameters **pir —** The **pir** parameter defines the constraints enforced when adapting the PIR rate defined within the **queue** *queue-id* **rate** command. The **pir** parameter requires a qualifier that defines the

constraint used when deriving the operational PIR for the queue. When the **rate** command is not specified, the default applies.

cir — The **cir** parameter defines the constraints enforced when adapting the CIR rate defined within the **queue** *queue-id* **rate** command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule — Specifies the criteria to use to compute the operational CIR and PIR values for this queue, while maintaining a minimum offset.

Values **max** — The **max** (maximum) keyword is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

min — The **min** (minimum) keyword is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

closest — The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR for the queue will be the rate closest to the rate specified using the **rate** command.

avg-frame-overhead

Syntax **avg-frame-overhead** *percent*
no avg-frame-overhead

Context config>service>vprn>if>sap>egress>queue-override>queue
config>service>vprn>ipsec-if>sap>egress>queue-override>queue

Description This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- Offered-load — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.
- Frame encapsulation overhead — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue's current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

  For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- Frame based offered-load — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.
- Packet to frame factor — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue's offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.
- Frame based CIR — The frame based CIR is calculated by multiplying the packet to frame factor with the queue's configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.
- Frame based within-cir offered-load — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

  As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue's frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler's within-cir pass.
- Frame based PIR — The frame based PIR is calculated by multiplying the packet to frame factor with the queue's configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.
- Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to determine the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

SAP and subscriber SLA-profile average frame overhead override — The average frame overhead parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress defined overhead.

The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet based queue statistics for

calculating port scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

Default 0

Parameters *percent* — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0 — 100

cbs

Syntax **cbs** *size-in-kbytes*
no cbs

Context config>service>vprn>if>sap>egress>queue-override>queue
config>service>vprn>if>sap>ingress>queue-override>queue
config>service>vprn>ipsec-if>sap>egress>queue-override>queue
config>service>vprn>ipsec-if>sap>ingress>queue-override>queue

Description This command can be used to override specific attributes of the specified queue's CBS parameters.

It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queue's CBS setting into the defined reserved total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly drop packets.

If the CBS value is larger than the MBS value, an error will occur, preventing the CBS change.

The **no** form of this command returns the CBS size to the default value.

Default no cbs

Parameters *size-in-kbytes* — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

Values 0 — 131072 or default

high-prio-only

Syntax **high-prio-only** *percent*
no high-prio-only

Context config>service>vprn>if>sap>egress>queue-override>queue
config>service>vprn>if>sap>ingress>queue-override>queue
config>service>vprn>ipsec-if>sap>egress>queue-override>queue
config>service>vprn>ipsec-if>sap>ingress>queue-override>queue

Description This command can be used to override specific attributes of the specified queue's high-prio-only parameters. The **high-prio-only** command configures the percentage of buffer space for the queue, used exclusively by high priority packets.

The priority of a packet can only be set in the SAP ingress QoS policy and is only applicable on the ingress queues for a SAP. The **high-prio-only** parameter is used to override the default value derived from the **network-queue** command.

The defined **high-prio-only** value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the **high-prio-only** value larger than the current MBS size will also result in an error and fail execution.

The **no** form of this command restores the default high priority reserved size.

Parameters *percent* — The *percent* parameter is the percentage reserved for high priority traffic on the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that none of the MBS of the queue will be reserved for high priority traffic. This does not affect RED slope operation for packets attempting to be queued.

Values 0 — 100 | default

mbs

Syntax **mbs** {*size-in-kbytes* | **default**}
no mbs

Context config>service>vprn>if>sap>egress>queue-override>queue
config>service>vprn>if>sap>egress>hsmda-queue-override>queue
config>service>vprn>ipsec-if>sap>egress>queue-override>queue

Description This command can be used to override specific attributes of the specified queue's MBS parameters. The MBS is a mechanism to override the default maximum size for the queue.

The sum of the MBS for all queues on an egress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet's RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The **no** form of this command returns the MBS size assigned to the queue.

Default default

Parameters *size-in-kbytes* — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

Values 0 — 131072 or default

mbs

Syntax **mbs** {*size-in-kbytes* | **default**}
no mbs

Context config>service>vprn>if>sap>ingress>queue-override>queue
config>service>vprn>ipsec-if>sap>ingress>queue-override>queue

Description This command can be used to override specific attributes of the specified queue's MBS parameters. The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet's RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the high-prio-only value larger than the current MBS size will also result in an error and fail execution.

The **no** form of this command returns the MBS size assigned to the queue to the value.

Default default

Parameters *size-in-kbytes* — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

Values 0 — 131072 or default

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context config>service>vprn>if>sap>egress>queue-override>queue
config>service>vprn>if>sap>ingress>queue-override>queue
config>service>vprn>ipsec-if>sap>egress>queue-override>queue

config>service>vprn>ipsec-if>sap>ingress>queue-override>queue

Description This command can be used to override specific attributes of the specified queue's Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters. The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

The **no** form of the command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

Default **rate max cir 0 —** The **max** default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The **max** value is mutually exclusive to the **pir-rate** value.

Parameters *pir-rate* — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.
Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 — 100000000

Default max

cir-rate — The **cir** parameter overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be given as a positive integer. The **sum** keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues.

Values 0 — 100000000, **max**, **sum**

Default 0

rate

Syntax **rate** *pir-rate*
no rate

Context config>service>vprn>if>sap>egress>hsmda-queue-overide>queue

Description This command can be used to override specific attributes of the specified queue's Peak Information Rate (PIR). The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The **rate** command can be executed at any time, altering the PIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

The **no** form of the command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR parameters (**max**, 0).

Default *pir-rate* — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.
Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 — 100000000

Default max

scheduler-override

Syntax [**no**] **scheduler-override**

Context config>service>vprn>if>sap>egress
config>service>vprn>if>sap>ingress
config>service>vprn>ipsec-if>sap>egress
config>service>vprn>ipsec-if>sap>ingress

Description This command specifies the set of attributes whose values have been overridden via management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP's ingress scheduler policy.

scheduler

Syntax **scheduler** *scheduler-name*
no scheduler *scheduler-name*

Context config>service>vprn>if>sap>egress>sched-override
config>service>vprn>if>sap>ingress>sched-override
config>service>vprn>ipsec-if>sap>egress>sched-override
config>service>vprn>ipsec-if>sap>ingress>sched-override

Description This command can be used to override specific attributes of the specified scheduler name.

A scheduler defines a bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child

associations. The scheduler can be a child (take bandwidth from a scheduler in a higher tier, except for schedulers created in tier 1). A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If *scheduler-name* already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the *scheduler-name* exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the *scheduler-name* does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

1. The maximum number of schedulers has not been configured.
2. The provided *scheduler-name* is valid.
3. The **create** keyword is entered with the command if the system is configured to require it (enabled in the **environment create** command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.
If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

Parameters *scheduler-name* — The name of the scheduler.

Values Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Default None. Each scheduler must be explicitly created.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given *scheduler-name*. If the **create** keyword is omitted, **scheduler-name** is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context config>service>vprn>if>sap>egress>sched-override>scheduler
config>service>vprn>ipsec-if>sap>egress>sched-override
config>service>vprn>ipsec-if>sap>ingress>sched-override

Description This command can be used to override specific attributes of the specified scheduler rate. The **rate** command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler's 'within CIR' distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other then its maximum rate. The scheduler's parent scheduler may not have the available bandwidth to meet the scheduler's needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is **max**. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The **no** form of this command returns all queues created with this *queue-id* by association with the QoS policy to the default PIR and CIR parameters.

Parameters *pir-rate* — The **pir** parameter accepts a step multiplier value that specifies the multiplier used to determine the PIR rate at which the queue will operate. A value of 0 to 100000000 or the keyword **max** or **sum** is accepted. Any other value will result in an error without modifying the current PIR rate.

To calculate the actual PIR rate, the rate described by the queue's **rate** is multiplied by the *pir-rate*.

The SAP ingress context for PIR is independent of the defined forwarding class (fc) for the queue. The default **pir** and definable range is identical for each class. The PIR in effect for a queue defines the maximum rate ate which the queue will be allowed to forward packets in a given second, thus shaping the queue's output.

The PIR parameter for SAP ingress queues do not have a negate (**no**) function. To return the queue's PIR rate to the default value, that value must be specified as the PIR value.

Values 1 — 100000000, **max**

Default max

cir cir-rate — The **cir** parameter accepts a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue will operate. A value of 0 to 250 or the keyword max is accepted. Any other value will result in an error without modifying the current CIR rate.

To calculate the actual CIR rate, the rate described by the **rate pir** *pir-rate* is multiplied by the cir *cir-rate*. If the **cir** is set to max, then the CIR rate is set to infinity.

The SAP ingress context for CIR is dependent on the defined forwarding class (fc) for the queue. The default CIR and definable range is different for each class. The CIR in effect for a queue defines both its profile (in or out) marking level as well as the relative importance compared to other queues for scheduling purposes during congestion periods.

Values 0 — 10000000, **max**, **sum**

Default sum

Routed VPLS Commands

vpls

Syntax **vpls** *service-name*

Context config>service
config>service>vprn>if

Description The **vpls** command, within the IP interface context, is used to bind the IP interface to the specified service name.

The system does not attempt to resolve the service name provided until the IP interface is placed into the administratively up state (**no shutdown**). Once the IP interface is administratively up, the system will scan the available VPLS services that have the allow-ip-int-binding flag set for a VPLS service associated with the name. If the service name is bound to the service name when the IP interface is already in the administratively up state, the system will immediately attempt to resolve the given name.

If a VPLS service is found associated with the name and with the allow-ip-int-binding flag set, the IP interface will be attached to the VPLS service allowing routing to and from the service virtual ports once the IP interface is operational.

A VPLS service associated with the specified name that does not have the allow-ip-int-binding flag set or a non-VPLS service associated with the name will be ignored and will not be attached to the IP interface.

If the service name is applied to a VPLS service after the service name is bound to an IP interface and the VPLS service allow-ip-int-binding flag is set at the time the name is applied, the VPLS service will be automatically resolved to the IP interface if the interface is administratively up or when the interface is placed in the administratively up state.

If the service name is applied to a VPLS service without the allow-ip-int-binding flag set, the system will not attempt to resolve the applied service name to an existing IP interface bound to the name. To rectify this condition, the flag must first be set and then the IP interface must enter or reenter the administratively up state.

While the specified service name may be assigned to only one service context in the system, it is possible to bind the same service name to more than one IP interface. If two or more IP interfaces are bound to the same service name, the first IP interface to enter the administratively up state (if currently administratively down) or to reenter the administratively up state (if currently administratively up) when a VPLS service is configured with the name and has the allow-ip-int-binding flag set will be attached to the VPLS service. Only one IP interface is allowed to attach to a VPLS service context. No error is generated for the remaining non-attached IP interfaces using the service name.

Once an IP interface is attached to a VPLS service, the name associated with the service cannot be removed or changed until the IP interface name binding is removed. Also, the allow-ip-int-binding flag cannot be removed until the attached IP interface is unbound from the service name.

Unbinding the service name from the IP interface causes the IP interface to detach from the VPLS service context. The IP interface may then be bound to another service name or a SAP or SDP binding may be created for the interface using the **sap** or **spoke-sdp** commands on the interface.

IES Chassis Mode Dependency

An IES IP interface cannot be bound to a service name unless the system is configured in chassis mode D Once an IES interface is bound to a service name, the chassis mode of the system cannot be changed to B or C.

VPRN Hardware Dependency

When a service name is bound to a VPRN IP interface, all SAPs associated with the VPRN service must be on hardware based on the FlexPath forwarding plane. Currently, these include the IOM3-XP, the various IMM modules and the SR7710c12. If any SAPs are associated with the wrong hardware type, the service name binding to the VPRN IP interface will fail. Once an IP interface within the VPRN service is bound to a service name, attempting to create a SAP on excluded hardware will fail.

Route Export and Import between Routing Contexts

The IES chassis mode dependency and the VPRN hardware dependency each are designed to prevent a condition where an ingress routing decision on hardware that does not support the mixed Layer 2 and Layer 3 behavior of routed VPLS is asked to route to a VPLS based next-hop.

Even with these restrictions, it is still possible using route leaking or import/export routing policies to create a condition where a FlexPath forwarding plane resolves a route to a VPLS next-hop. In this case, the forwarding plane handles the resolved next-hop as if it points to a null IP interface. Packets associated with a null next-hop egress IP interface will be discarded and an ICPM unreachable message will be generated when enabled.

IP Interface MTU and Fragmentation

A VPLS service is affected by two MTU values; port MTUs and the VPLS service MTU. The MTU on each physical port defines the largest Layer 2 packet (including all DLC headers and CRC) that may be transmitted out a port. The VPLS itself has a service level MTU that defines the largest packet supported by the service. This MTU does not include the local encapsulation overhead for each port (QinQ, Dot1Q, TopQ or SDP service delineation fields and headers) but does include the remainder of the packet. As virtual ports are created in the system, the virtual port cannot become operational unless the configured port MTU minus the virtual port service delineation overhead is greater than or equal to the configured VPLS service MTU. Thus, an operational virtual port is ensured to support the largest packet traversing the VPLS service. The service delineation overhead on each Layer 2 packet is removed before forwarding into a VPLS service. VPLS services do not support fragmentation and must discard any Layer 2 packet larger than the service MTU after the service delineation overhead is removed.

IP interfaces have a configurable up MTU that defines the largest packet that may egress the IP interface without being fragmented. This MTU encompasses the IP portion of the packet and does not include any of the egress DLC header or CRC. This MTU does not affect the size of the largest ingress packet on the IP interface. If the egress IP portion of the packet is larger than the IP interface MTU and the IP header do not fragment flag is not set, the packet is fragmented into smaller packets that will not exceed the configured MTU size. If the do not fragment bit is set, the packet is silently discarded at egress when it exceeds the IP MTU.

When the IP interface is bound to a VPLS service, the IP MTU must be at least 18 bytes less than the VPLS service MTU. This allows for the addition of the minimal Ethernet encapsulation overhead; 6 bytes for the DA, 6 bytes for the SA, 2 bytes for the Etype and 4 bytes for the trailing CRC. Any remaining egress virtual port overhead (Dot1P, Dot1Q, QinQ, TopQ or SDP) required above the minimum is known to be less than the egress ports MTU since the virtual port would not be operational otherwise.

If the IP interface IP MTU value is too large based on the VPLS service MTU, the IP interface will enter the operationally down state until either the IP MTU is adequately lowered or the VPLS service MTU is sufficiently increased.

The **no** form of the command on the IP interface is used to remove the service name binding from the IP interface. If the service name has been resolved to a VPLS service context and the IP interface has been attached to the VPLS service, the IP interface will also be detached from the VPLS service.

Default none

Parameters service-name

The service-name parameter is required when using the IP interface vpls command and specifies the service name that the system will attempt to resolve to an allow-ip-int-binding enabled VPLS service associated with the name. The specified name is expressed as an ASCII string comprised of up to 32 characters. It does not need to already be associated with a service and the system does not check to ensure that multiple IP interfaces are not bound to the same name.

ingress

Syntax **ingress**

Context config>service>vprn>if>vpls

Description The ingress node in this context under the vpls binding is used to define the routed IPv4 and IPv6 optional filter overrides.

v4-routed-override-filter

Syntax **v4-routed-override-filter** *ipv4-filter-id*
no v4-routed-override-filter

Context config>service>vprn>if>vpls>ingress

Description The v4-routed-override-filter command is used to specify an IPv4 filter ID that will be applied to all ingress packets entering the VPLS service. The filter overrides any existing ingress IPv4 filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed, the IPv4 routed packets will use the any existing ingress IPv4 filter on the VPLS virtual port.

The **no** form of the command is used to remove the IPv4 routed override filter from the ingress IP interface. When removed, the IPv4 ingress routed packets within a VPLS service attached to the IP interface will use the IPv4 ingress filter applied to the packets virtual port when defined.

Default none

Parameters *ipv4-filter-id* — The ipv4-filter-id parameter is required when executing the v4-routed-override-filter command. The specified filter ID must exist as an IPv4 filter within the system or the override command will fail.

v6-routed-override-filter

Syntax **v6-routed-override-filter** *ipv6-filter-id*
no v6-routed-override-filter

Context config>service>vprn>if>vpls>ingress

Description The v6-routed-override-filter command is used to specify an IPv6 filter ID that will be applied to all ingress packets entering the VPLS service. The filter overrides any existing ingress IPv6 filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed, the IPv6 routed packets will use the any existing ingress IPv6 filter on the VPLS virtual port.

The no v6-routed-override-filter command is used to remove the IPv6 routed override filter from the ingress IP interface. When removed, the IPv6 ingress routed packets within a VPLS service attached to the IP interface will use the IPv6 ingress filter applied to the packets virtual port when defined.

Default none

Parameters *ipv6-filter-id* — The ipv6-filter-id parameter is required when executing the v6-routed-override-filter command. The specified filter ID must exist as an IPv6 filter within the system or the override command will fail.

egress

Syntax **egress**

Context config>service>vprn>if>vpls

Description The egress node under the vpls binding is used to define the optional sap-egress QoS policy that will be used for reclassifying the egress forwarding class or profile for routed packets associated with the IP interface on the attached VPLS service context.

reclassify-using-qos

Syntax **reclassify-using-qos** *sap-egress-qos-id*
no reclassify-using-qos

Context config>service>vprn>if>vpls>egress

Description The reclassify-using-qos command is used to specify a sap-egress QoS policy that will be used to reclassify the forwarding class and profile of egress routed packets on the VPLS service. When routed packets associated with the IP interface egress a VPLS SAP, the reclassification rules within the sap-egress QoS policy applied to the SAP are always ignored (even when reclassify-using-qos is not defined).

Any queues or policers defined within the specified QoS policy are ignored and are not created on the VPLS egress SAPs. Instead, the routed packets continue to use the forwarding class mappings, queues and policers from the sap-egress QoS policy applied to the egress VPLS SAP.

While the specified sap-egress policy ID is applied to an IP interface it cannot be deleted from the system.

The **no** form of the command removes the sap-egress QoS policy used for reclassification from the egress IP interface. When removed, IP routed packets will not be reclassified on the egress SAPs of the VPLS service attached to the IP interface.

Parameters *sap-egress-qos-id* — The sap-egress-qos-id parameter is required when executing the reclassify-using-qos command. The specified SAP egress QoS ID must exist within the system or the command will fail.

allow-ip-int-binding

Syntax [**no**] **allow-ip-int-binding**

Context config>service>vpls

Description This command sets a flag on the VPLS service that enables the ability to attach an IES or VPRN IP interface to the VPLS service in order to make the VPLS service routable. When the allow-ip-int-binding command is not enabled, the VPLS service cannot be attached to an IP interface.

VPLS Configuration Constraints for Enabling allow-ip-int-binding

When attempting to set the allow-ip-int-binding VPLS flag, the system first checks to see if the correct configuration constraints exist for the VPLS service and the network ports. In Release 8.0 the following VPLS features must be disabled or not configured for the allow-ip-int-binding flag to set:

- SAP ingress QoS policies applied to the VPLS SAPs cannot have MAC match criteria defined
- SDPs used in spoke or mesh SDP bindings cannot be configured as GRE
- The VPLS service type cannot be B-VPLS or M-VPLS and it cannot be an I-VPLS service bound to a B-VPLS context
- MVR from Routed VPLS and to another SAP is not supported
- Enhanced and Basic Subscriber Management features
- Network Domain on SDP bindings [Not sure how we enforce this.]

Once the VPLS allow-ip-int-binding flag is set on a VPLS service, the above features cannot be enabled on the VPLS service.

NETWORK PORT HARDWARE CONSTRAINTS

The system also checks to ensure that all ports configured in network mode are associated with FlexPath forwarding planes. If a port is currently in network mode and the port is associated with a FlexPath forwarding plane, the allow-ip-int-binding command will fail. Once the allow-ip-int-binding flag is set on any VPLS service, attempting to enable network mode on a port associated with a FlexPath forwarding plane will fail.

VPLS SAP HARDWARE CONSTRAINTS

Besides VPLS configuration and network port hardware association, the system also checks to that all SAPs within the VPLS are created on Ethernet ports and the ports are associated with FlexPath forwarding planes. Certain Ethernet ports and virtual Ethernet ports are not supported which include HSMDA ports and CCAG virtual ports (VSM based). If a SAP in the VPLS exists on an unsupported port type or is associated with a FlexPath forwarding plane, the allow-ip-int-binding command will

fail. Once the allow-ip-int-binding flag is set on the VPLS service, attempting to create a VPLS SAP on the wrong port type or associated with a FlexPath forwarding plane will fail.

VPLS SERVICE NAME BOUND TO IP INTERFACE WITHOUT ALLOW-IP-INT-BINDING FLAG SET

In the event that a service name is applied to a VPLS service and that service name is also bound to an IP interface but the allow-ip-int-binding flag has not been set on the VPLS service context, the system attempt to resolve the service name between the VPLS service and the IP interface will fail. After the allow-ip-int-binding flag is successfully set on the VPLS service, either the service name on the VPLS service must be removed and reapplied or the IP interface must be re-initialized using the shutdown / no shutdown commands. This will cause the system to reattempt the name resolution process between the IP interface and the VPLS service.

The **no** form of the command resets the allow-ip-int-binding flag on the VPLS service. If the VPLS service currently has an IP interface from an IES or VPRN service attached, the no allow-ip-int-binding command will fail. Once the allow-ip-int-binding flag is reset on the VPLS service, the configuration and hardware restrictions associated with setting the flag are removed. The port network mode hardware restrictions are also removed.

ETH-CFM Service Commands

eth-cfm

Syntax **eth-cfm**

Context config>service>vprn
config>service>vprn>if>sap
config>service>vprn>if>spoke-sdp
config>service>vprn>sub-if>grp-if>sap

Description This command enables the context to configure ETH-CFM parameters.

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {**up** | **down**}]
no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context config>service>vprn>if>sap>eth-cfm
config>service>vprn>if>spoke-sdp>eth-cfm
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description This command configures the ETH-CFM maintenance endpoint (MEP).

Parameters *mep-id* — Specifies the maintenance association end point identifier.

Values 1 — 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 — 4294967295

ma-index — Specifies the MA index value.

Values 1 — 4294967295

direction up|down — Indicates the direction in which the maintenance association (MEP) faces on the bridge port. Direction UP is not supported on VPRN MEPs.

down — Sends continuity check messages away from the MAC relay entity.

up — Sends continuity check messages towards the MAC relay entity.

ais-enable

Syntax [**no**] **ais-enable**

Context config>service>vprn>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm

Description This command configures the reception of Alarm Indication Signal (AIS) message.

ccm-enable

Syntax [**no**] **ccm-enable**

Context config>service>vprn>if>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm>mep
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description This command enables the generation of CCM messages.

The **no** form of the command disables the generation of CCM messages.

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context config>service>vprn>if>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm>mep
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of the command removes the priority value from the configuration.

Default The highest priority on the bridge-port.

Parameters *priority* — Specifies the priority of CCM and LTM messages.

Values 0 — 7

ccm-padding-size

Syntax [**no**] **ccm-padding-size** *ccm-padding*

Context config>service>epipe>sap>eth-cfm>mep
config>service>epipe>sdp>eth-cfm>mep
config>service>vpls>sap>eth-cfm>mep
config>service>vpls>spoke-sdp>eth-cfm>mep
config>service>vpls>mesh-sdp>eth-cfm>mep
config>service>vpls>sap>eth-cfm>mep
config>service>vpls>spoke-sdp>eth-cfm>mep
config>service>vpls>mesh-sdp>eth-cfm>mep
config>service>ies>if>sap>eth-cfm>mep
config>service>ies>if>spoke-sdp>eth-cfm>mep
config>service>vprn>sub-if>grp-if>sap>eth-cfm
config>service>vprn>if>sap>eth-cfm>mep

config>service>vprn>if>spoke-sdp>eth-cfm>mep
config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep
config>service>ipipe>sap>eth-cfm>mep
config>port>ethernet>eth-cfm>mep
config>lag>eth-cfm>eth-cfm>mep
config>router>if>eth-cfm>mep

Description Set the byte size of the optional Data TLV to be included in the ETH-CC PDU. This will increase the size of the ETH-CC PDU by the configured value. The base size of the ETH-CC PDU, including the Interface Status TLV and Port Status TLV, is 83 bytes not including the Layer Two encapsulation. CCM padding is not supported when the CCM-Interval is less than one second.

Default ccm-padding-size

Parameters *ccm-padding* — specifies the byte size of the Optional Data TLV

Values 3 — 1500

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context config>service>vprn>if>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm>mep
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description This command enables eth-test functionality on MEP. For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test then can be done using the following OAM commands:

`oam eth-cfm eth-test` *`mac-address`* `mep` *`mep-id`* `domain` *`md-index`* `association` *`ma-index`* `[priority` *`priority`*`] [data-length` *`data-length`*`]`

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context config>service>vprn>if>sap>eth-cfm>mep>eth-test-enable
config>service>vprn>if>spoke-sdp>eth-cfm>mep>eth-test-enable
config>service>vprn>sub-if>grp-if>sap>eth-cfm>eth-test-enable

Description This command configures the test pattern for eth-test frames.

The **no** form of the command removes the values from the configuration.

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

Default all-zeros

bit-error-threshold

Syntax **bit-error-threshold** *bit-errors*

Context config>service>vprn>if>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm>mep
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default 1

Parameters *bit-errors* — Specifies the lowest priority defect.

Values 0 — 11840

one-way-delay-threshold

Syntax **one-way-delay-threshold** *time*

Context config>service>vprn>if>sap>eth-cfm
config>service>vprn>if>spoke-sdp>eth-cfm
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description This command enables one way delay threshold time limit.

Default 3 seconds

Parameters *priority* — Specifies the value for the threshold.

Values 0 — 600

tunnel-fault

Syntax **tunnel-fault** {**accept | ignore**}

Context config>service>vprn>eth-cfm
config>service>vprn>if>sap>eth-cfm
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description Allows the individual service SAPs to react to changes in the tunnel MEP state. When tunnel-fault accept is configured at the service level, the SAP will react according to the service type, Epipe will set the operational flag and VPLS, IES and VPRN SAP operational state will become down on failure or up on clear. This command triggers the OAM mapping functions to mate SAPs and bindings in an

Epipe service as well as setting the operational flag. If AIS generation is the requirement for the Epipe services this command is not required. See the command ais-enable under epipe>sap>eth-cfm>ais-enable for more details. This works in conjunction with the tunnel-fault accept on the individual SAPs. Both must be set to accept to react to the tunnel MEP state. By default the service level command is "ignore" and the sap level command is "accept". This means simply changing the service level command to "accept" will enable the feature for all SAPs. This is not required for Epipe services that only wish to generate AIS on failure.

Parameters **accept —** Share fate with the facility tunnel MEP

ignore — Do not share fate with the facility tunnel MEP

Default **ignore** (Service Level)

accept (SAP Level for Epipe and VPLS)

fault-propagation-enable

Syntax **fault-propagation-enable** {**use-if-tlv** | **suspend-ccm**}
no fault-propagation-enable

Context config>service>vprn>if>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm>mep
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description This command configures the fault propagation for the MEP.

Parameters **use-if-tlv —** Specifies to use the interface TLV.

suspend-ccm — Specifies to suspend the continuity check messages.

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context config>service>vprn>if>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm>mep
config>service>vprn>sub-if>grp-if>sap>eth-cfm

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default macRemErrXcon

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM; or
noXcon	No defects DefXcon or lower are to be reported

SAP Subscriber Management Commands

sub-sla-mgmt

Syntax [**no**] **sub-sla-mgmt**

Context config>service>vprn>sub-if>grp-if>sap

Description This command enables the context to configure subscriber management parameters for this SAP.

Default no sub-sla-mgmt

def-sla-profile

Syntax **def-sla-profile** *default-sla-profile-name*
no def-sla-profile

Context config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt

Description This command specifies a default SLA profile for this SAP. The SLA profile must be defined prior to associating the profile with a SAP in the **config>subscriber-mgmt>sla-profile** context.

An SLA profile is a named group of QoS parameters used to define per service QoS for all subscriber hosts common to the same subscriber within a provider service offering. A single SLA profile may define the QoS parameters for multiple subscriber hosts. SLA profiles are maintained in two locations, the subscriber identification policy and the subscriber profile templates. After a subscriber host is associated with an SLA profile name, either the subscriber identification policy used to identify the subscriber or the subscriber profile associated with the subscriber host must contain an SLA profile with that name. If both the subscriber identification policy and the subscriber profile contain the SLA profile name, the SLA profile in the subscriber profile is used.

The **no** form of the command removes the default SLA profile from the SAP configuration.

Default no def-sla-profile

Parameters *default-sla-profile-name* — Specifies a default SLA profile for this SAP. The SLA profile must be defined prior to associating the profile with a SAP in the **config>subscriber-mgmt>sla-profile** context.

def-sub-profile

Syntax **def-sub-profile** *default-subscriber-profile-name*

Context config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt

Description This command specifies a default subscriber profile for this SAP. The subscriber profile must be defined prior to associating the profile with a SAP in the **config>subscriber-mgmt>sub-profile** context.

A subscriber profile defines the aggregate QoS for all hosts within a subscriber context. This is done through the definition of the egress and ingress scheduler policies that govern the aggregate SLA for subscriber using the subscriber profile. Subscriber profiles also allow for specific SLA profile definitions when the default definitions from the subscriber identification policy must be overridden.

The **no** form of the command removes the default SLA profile from the SAP configuration.

Parameters *default-sub-profile* — Specifies a default subscriber profile for this SAP. The subscriber profile must be defined prior to associating the profile with a SAP in the **config>subscriber-mgmt>sub-profile** context.

multi-sub-sap

Syntax **multi-sub-sap** [*number-of-sub*]
no multi-sub-sap

Context config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt

Description This command configures the maximum number of subscribers for this SAP. It is used in conjunction with the **profiled-traffic-only** command on single subscriber SAPs and creates a subscriber host which is used to forward non-IP traffic through the single subscriber SAP without the need for SAP queues.

The **no** form of this command returns the default value.

Default 1

Parameters *number-of-sub* — Specifies the maximum number of subscribers for this SAP.

Values 2 — 8000

single-sub-parameters

Syntax **single-sub-parameters**

Context config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt

Description This command enables the context to configure single subscriber parameters for this SAP.

non-sub-traffic

Syntax **non-sub-traffic sub-profile** *sub-profile-name* **sla-profile** *sla-profile-name* [**subscriber** *sub-ident-string*]
no non-sub-traffic

Context config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt>single-sub

Description This command configures non-subscriber traffic profiles. It is used in conjunction with the **profiled-traffic-only** command on single subscriber SAPs and creates a subscriber host which is used to forward non-IP traffic through the single subscriber SAP without the need for SAP queues.

The **no** form of the command removes removes the profiles and disables the feature.

Parameters **sub-profile** *sub-profile-name* **—** Specifies an existing subscriber profile name to be associated with the static subscriber host. The subscriber profile is configured in the **config>subscr-mgmt>sub-profile** context.

sla-profile *sla-profile-name* **—** Specifies an existing SLA profile name to be associated with the static subscriber host. The SLA profile is configured in the **config>subscr-mgmt>sla-profile** context.

subscriber *sub-ident-string* — Specifies an existing subscriber identification profile to be associated with the static subscriber host. The subscriber identification profile is configured in the **config>subscr-mgmt>sub-ident-policy** context. The subscriber information is used by the VPRN SAP arp-reply-agent to determine the proper handling of received ARP requests from subscribers.

- For VPRN SAPs with **arp-reply-agent** enabled with the optional *sub-ident* parameter, the static subscriber host's sub-ident-string is used to determine whether an ARP request received on the SAP is sourced from a host belonging to the same subscriber as the destination host. When both the destination and source hosts from the ARP request are known on the SAP and the subscriber identifications do not match, the ARP request may be forwarded to the rest of the VPRN destinations.

  If the static subscriber host's *sub-ident* string is not defined, the host is not considered to belong to the same subscriber as another host on the SAP.

  If source or destination host is unknown, the hosts are not considered to belong to the same subscriber. ARP messages from unknown hosts are subject to anti-spoof filtering rules applied at the SAP.

  If *sub-ident* is not enabled on the SAP arp-reply-agent, subscriber identification matching is not performed on ARP requests received on the SAP.

  ARP requests are never forwarded back to the same SAP or within the receiving SAP's split horizon group.

profiled-traffic-only

Syntax [**no**] **profiled-traffic-only**

Context config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt>single-sub

Description This command enables profiled traffic only for this SAP. The profiled traffic refers to single subscriber traffic on a dedicated SAP (in the VLAN-per-subscriber model). When enabled, subscriber queues are instantiated through the QOS policy defined in the sla-profile and the associated SAP queues are deleted. This can increase subscriber scaling by reducing the number of queues instantiated per subscriber (in the VLAN-per-subscriber model). In order for this to be achieved, any configured multi-sub-sap limit must be removed (leaving the default of 1).

The **no** form of the command disables the command.

sub-ident-policy

Syntax **sub-ident-policy** *sub-ident-policy-name*

Context config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt

Description This command associates a subscriber identification policy to this SAP. The subscriber identification policy must be defined prior to associating the profile with a SAP in the **config>subscriber-mgmt>sub-ident-policy** context.

Subscribers are managed by the system through the use of subscriber identification strings. A subscriber identification string uniquely identifies a subscriber. For static hosts, the subscriber identification string is explicitly defined with each static subscriber host.

For dynamic hosts, the subscriber identification string must be derived from the DHCP ACK message sent to the subscriber host. The default value for the string is the content of Option 82 CIRCUIT-ID and REMOTE-ID fields interpreted as an octet string. As an option, the DHCP ACK message may be processed by a subscriber identification policy which has the capability to parse the message into an alternative ASCII or octet string value.

When multiple hosts on the same port are associated with the same subscriber identification string they are considered to be host members of the same subscriber.

The **no** form of the command removes the default subscriber identifcation policy from the SAP configuration.

Default no sub-ident-policy

Parameters *sub-ident-policy-name* — Specifies a subscriber identification policy for this SAP. The subscriber profile must be defined prior to associating the profile with a SAP in the **config>subscriber-mgmt>sub-ident-policy** context.

srrp

Syntax [**no**] **srrp** *srrp-id*

Context config>service>vprn>sub-if>grp-if

Description This command creates an SRRP instance on a group IP interface. An SRRP instance manages all subscriber subnets within the group interfaces subscriber IP interface or other subscriber IP interfaces that are associated through a wholesale/retail relationship. Only one unique SRRP instance can be configured per group interface.

The **no** form of the command removes an SRRP instance from a group IP interface. Once removed, the group interface ignores ARP requests for the SRRP gateway IP addresses that may exist on subscriber subnets associated with the group IP interface. Then the group interface stops routing using the redundant IP interface associated with the group IP interface and will stop routing with the SRRP gateway MAC address. Ingress packets destined to the SRRP gateway MAC will also be silently discarded. This is the same behavior as a group IP interface that is disabled (shutdown).

Default no srrp

Parameters *srrp-id* — Specifies a 32 bit instance ID that must be unique to the system. The instance ID must also match the instance ID used by the remote router that is participating in the same SRRP context. SRRP is intended to perform a function similar to VRRP where adjacent IP hosts within local subnets use a default gateway to access IP hosts on other subnets.

Values 1 — 4294967295

gw-mac

Syntax **gw-mac** *mac-address*
no gw-mac

Context config>service>vprn>sub-if>grp-if>srrp

Description This command overrides the default SRRP gateway MAC address used by the SRRP instance. Unless specified, the system uses the same base MAC address for all SRRP instances with the last octet overridden by the lower 8 bits of the SRRP instance ID. The same SRRP gateway MAC address should be in-use by both the local and remote routers participating in the same SRRP context.

One reason to change the default SRRP gateway MAC address is if two SRRP instances sharing the same broadcast domain are using the same SRRP gateway MAC. The system will use the SRRP instance ID to separate the SRRP messages (by ignoring the messages that does not match the local instance ID), but a unique SRRP gateway MAC is essential to separate the routed packets for each gateway IP address.

The **no** form of the command removes the explicit SRRP gateway MAC address from the SRRP instance. The SRRP gateway MAC address can only be changed or removed when the SRRP instance is shutdown.

Parameters *mac-address* — Specifies a MAC address that is used to override the default SRRP base MAC address

Values Any MAC address except all zeros, broadcast or multicast addresses. The offset is expressed in normal Ethernet MAC address notation. The defined gw-mac cannot be 00:00:00:00:00:00, ff:ff:ff:ff:ff:ff or any multicast address.

If not specified, the system uses the default SRRP gateway MAC address with the last octet set to the 8 least significant bits of the SRRP instance ID.

keep-alive-interval

Syntax **keep-alive-interval** *interval*
no keep-alive-interval

Context config>service>vprn>sub-if>grp-if>srrp

Description This command defines the interval between SRRP advertisement messages sent when operating in the master state. The interval is also the basis for setting the master-down timer used to determine when the master is no longer sending. The system uses three times the keep-alive interval to set the timer. Every time an SRRP advertisement is seen that is better then the local priority, the timer is reset. If the timer expires, the SRRP instance assumes that a master does not exist and initiates the attempt to become master.

When in backup state, the SRRP instance takes the keep-alive interval of the master as represented in the masters SRRP advertisement message. Once in master state, the SRRP instance uses its own configured keep-alive interval.

The keep-alive-interval may be changed at anytime, but will have no effect until the SRRP instance is in the master state.

The **no** form of the command restores the default interval.

Parameters *interval* — Specifies the interval, in milliseconds, between SRRP advertisement messages sent when operating in the master state.

Values 1 — 100

Default 10 milliseconds

message-path

Syntax **message-path** *sap-id*
no message-path

Context config>service>vprn>sub-if>grp-if>srrp

Description This command defines a specific SAP for SRRP in-band messaging. A message-path SAP must be defined prior to activating the SRRP instance. The defined SAP must exist on the SRRP instances group IP interface for the command to succeed and cannot currently be associated with any dynamic or static subscriber hosts. Once a group IP interface SAP has been defined as the transmission path for SRRP Advertisement messages, it cannot be administratively shutdown, will not support static or dynamic subscriber hosts and cannot be removed from the group IP interface.

The SRRP instance message-path command may be executed at anytime on the SRRP instance. Changing the message SAP will fail if a dynamic or static subscriber host is associated with the new SAP. Once successfully changed, the SRRP instance will immediately disable anti-spoof on the SAP and start sending SRRP Advertisement messages if the SRRP instance is activated.

Changing the current SRRP message SAP on an active pair of routers should be done in the following manner:

1. Shutdown the backup SRRP instance.
2. Change the message SAP on the shutdown node.
3. Change the message SAP on the active master node.
4. Re-activate the shutdown SRRP instance.

Shutting down the backup SRRP instance prevents the SRRP instances from becoming master due to temporarily using differing message path SAPs.

If an MCS peering is operational between the redundant nodes and the SRRP instance has been associated with the peering, the designated message path SAP will be sent from each member.

The **no** form of the command can only be executed when the SRRP instance is shutdown. Executing no message-path allows the existing SAP to be used for subscriber management functions. A new message-path SAP must be defined prior to activating the SRRP instance.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 2569 for command syntax.

policy

Syntax [**no**] **policy** *vrrp-policy-id*

Context config>service>vprn>sub-if>grp-if>srrp

Description This command associates one or more VRRP policies with the SRRP instance. A VRRP policy is a collection of connectivity and verification tests used to manipulate the in-use priorities of VRRP and SRRP instances. A VRRP policy can test the link state of ports, ping IP hosts, discover the existence of routes in the routing table or the ability to reach Layer 2 hosts. When one or more of these tests fail, the VRRP policy has the option of decrementing or setting an explicit value for the in-use priority of an SRRP instance.

More than one VRRP policy may be associated with an SRRP instance. When more than one VRRP policy is associated with an SRRP instance the delta decrement of the in-use priority is cumulative unless one or more test fail that have explicit priority values. When one or more explicit tests fail, the lowest priority value event takes effect for the SRRP instance. When the highest delta-in-use-limit is used to manage the lowest delta derived in-use priority for the SRRP instance.

VRRP policy associations may be added and removed at anytime. A maximum of two VRRP policies can be associated with a single SRRP instance.

The **no** form of the command removes the association with vrrp-policy-id from the SRRP instance.

Parameters *vrrp-policy-id* — Specifies one or more VRRP policies with the SRRP instance.

Values 1 — 9999

priority

Syntax **priority** *priority*
no priority

Context config>service>vprn>sub-if>grp-if>srrp

Description This command overrides the default base priority for the SRRP instance. The SRRP instance priority is advertised by the SRRP instance to its neighbor router and is compared to the priority received from the neighbor router. The router with the best (highest) priority enters the master state while the other router enters the backup state. If the priority of each router is the same, the router with the lowest source IP address in the SRRP advertisement message assumes the master state.

The base priority of an SRRP instance can be managed by VRRP policies. A VRRP policy defines a set of connectivity or verification tests which, when they fail, may lower an SRRP instances base priority (creating an in-use priority for the instance). Every time an SRRP instances in-use priority changes when in master state, it sends an SRRP advertisement message with the new priority. If the dynamic priority drops to zero or receives an SRRP Advertisement message with a better priority, the SRRP instance transitions to the *becoming backup* state.

When the priority command is not specified, or the no priority command is executed, the system uses a default base priority of 100. The priority command may be executed at anytime.

The **no** form of the command restores the default base priority to the SRRP instance. If a VRRP policy is associated with the SRRP instance, it will use the default base priority as the basis for any modifications to the SRRP instances in-use priority.

Parameters *priority* — Specifies a base priority for the SRRP instance to override the default.

Values 1 — 254

Default 100

send-fib-population-packets

Syntax **send-fib-population-packets** (**all** | **outer-tag-only**)
no send-fib-population-packets

Context config>service>vprn>sub-if>grp-if>srrp

Description This command sends FIB population packets.

The **no** form of the command disables sending FIB population packets.

Default all

Parameters **all —** Sends FIB population packets to all VLANs.

outer-tag-only — Sends FIB population packets to only outer VLAN tags.

generate-garp-on-outer-vlan

Syntax **send-fib-population-packets** (**all** | **outer-tag-only**)
no send-fib-population-packets

Context config>service>vprn>sub-if>grp-if>srrp

Description This command sends GARP packets to outer VLANs only.

The **no** form of the command disables sending GARP packets to outer VLANs only.

Default no send-fib-population-packets

Interface VRRP Commands

vrrp

Syntax **vrrp** *virtual-router-id* [**owner**]
no vrrp *virtual-router-id*

Context config>service>vprn>if

Description This command creates or edits a Virtual Router ID (VRID) on the service IP interface. A VRID is internally represented in conjunction with the IP interface name. This allows the VRID to be used on multiple IP interfaces while representing different virtual router instances.

Two VRRP nodes can be defined on an IP interface. One, both, or none may be defined as owner. The nodal context of vrrp virtual-router-id is used to define the configuration parameters for the VRID.

The **no** form of this command removes the specified VRID from the IP interface. This terminates VRRP participation for the virtual router and deletes all references to the VRID. The VRID does not need to be shutdown in order to remove the virtual router instance.

Default No default

Parameters *virtual-router-id* — The virtual-router-id parameter specifies a new virtual router ID or one that can be modified on the IP interface.

Values 1 — 255

authentication-key

Syntax **authentication-key** [*authentication-key* **|** *hash-key*] [**hash** | **hash2**]
no authentication-key

Context config>service>vprn>if>vrrp

Description The **authentication-key** command, within the vrrp *virtual-router-id* context, is used to assign a simple text password authentication key to generate master VRRP advertisement messages and validate received VRRP advertisement messages.

The **authentication-key** command is one of the few commands not affected by the presence of the **owner** keyword. If simple text password authentication is not required, this command is not required. If the command is re-executed with a different password key defined, the new key will be used immediately. If a no **authentication-key** command is executed, the password authentication key is restored to the default value. The **authentication-key** command may be executed at any time, altering the simple text password used when **authentication-type** password authentication method is used by the virtual router instance. The **authentication-type password** command does not need to be executed prior to defining the **authentication-key** command.

To change the current in-use password key on multiple virtual router instances:

- Identify the current master

- Shutdown the virtual router instance on all backups
- Execute the authentication-key command on the master to change the password key
- Execute the authentication-key command and no shutdown command on each backup key

The **no** form of this command restores the default null string to the value of key.

Default No default. The authentication data field contains the value 0 in all 16 octets.

Parameters *authentication-key* — The *key* parameter identifies the simple text password used when VRRP Authentication Type 1 is enabled on the virtual router instance. Type 1 uses a string eight octets long that is inserted into all transmitted VRRP advertisement messages and compared against all received VRRP advertisement messages. The authentication data fields are used to transmit the key.

The *key* parameter is expressed as a string consisting of up to eight alpha-numeric characters. Spaces must be contained in quotation marks (“ ”). The quotation marks are not considered part of the string.

The string is case sensitive and is left-justified in the VRRP advertisement message authentication data fields. The first field contains the first four characters with the first octet (starting with IETF RFC bit position 0) containing the first character. The second field holds the fifth through eighth characters. Any unspecified portion of the authentication data field is padded with the value 0 in the corresponding octet.

Values Any 7-bit printable ASCII character.

Exceptions:	Double quote (")	ASCII 34
	Carriage Return	ASCII 13
	Line Feed	ASCII 10
	Tab	ASCII 9
	Backspace	ASCII 8

hash-key — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

authentication-type

Syntax **authentication-type {password | message-digest}**
no authentication-type

Context config>service>vprn>if>vrrp

Description

The **authentication-type** command, within the **vrrp** *virtual-router-id* context, is used to assign the authentication method to generate master VRRP advertisement messages and validate received VRRP advertisement messages.

NOTE: The authentication management for VRRP closely follows the authentication management format used for IS-IS.

The **authentication-type** command is one of the commands not affected by the presence of the owner keyword. If authentication is not required, the authenticaton-type command must not be executed. If the command is re-executed with a different authentication type defined, the new type will be used. If the no authentication-type command is executed, authentication is removed and no authentication is performed. The authentication-type command may be executed at any time, altering the authentication method used by the virtual router instance.

The **no** form of this command removes authentication from the virtual router instance. All VRRP Advertisement messages sent will have the Authentication Type field set to 0 and the Authentication Data fields will contain 0 in all octets. VRRP Advertisement messages received with Authentication Type fields containing a value other than 0 will be discarded.

password — The password keyword identifies VRRP Authentication Type 1. Type 1 requires the definition of a string of eight octets long using the authentication-key command. All transmitted VRRP Advertisement messages must have the Authentication Type field set to 1 and the Authentication Data fields must contain the authentication-key password.

All received VRRP advertisement messages must contain a value of 1 in the Authentication Type field and the Authentication Data fields must match the defined authentication-key. All other received messages will be silently discarded.

message-digest — The message-digest keyword identifies VRRP Authentication Type 2. Type 2 defines a lower IP layer MD5 authentication mechanism using HMAC and IP authentication header standards. An MD5 key must be defined using the message-digest-key command. All transmitted VRRP advertisement messages must have the Authentication Type field set to 2 and the Authentication Data fields must contain 0 in all octets. The message-digest key is used in the hashing process when populating the IP Authentication Header fields. A sequential incrementing counter (set to zero when the message-digest-key is set) is incremented and then used in the IP Authentication Header to prevent replay attacks on authorized participating virtual router instances.

All received VRRP advertisement messages must contain a value of 2 in the Authentication Type field and the Authentication Data fields are ignored. The message must have been authorized by the lower layer IP Authentication Header process with the sequential counter field and the source IP address presented to the virtual router instance. To track the validity of the received counter, the virtual router instance maintains a master counter table containing up to 32 source IP addresses and the last received counter value. Populate the table as follows:

1. Check to see if source IP address exists in table.
   - If non-existent, create an entry if available.
   - If no entry is available, delete the oldest and create an entry.
     The new entry should have a counter value of zero.
2. Compare the message counter value to the entry value (0 if new entry or equal to the previous message counter from the source IP address).
   - If the message counter is not greater than the entry counter value, silently discard the packet.

– If the message counter is greater than the entry counter value, accept the message for further checking and replace the entry counter value with the message counter value and time stamp the entry.

backup

Syntax [**no**] **backup** *ip-address*

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command configures virtual router IP addresses for the interface.

bfd-enable

Syntax **bfd-enable interface** *interface-name* **dst-ip** *ip-address*
bfd-enable *service-id* **interface** *interface-name* **dst-ip** *ip-address*
no bfd-enable interface *interface-name* **dst-ip** *ip-address*
no bfd-enable *service-id* **interface** *interface-name* **dst-ip** *ip-address*

Context config>service>vprn>if>vrrp
config>service>vprn>sub-if>grp-if>srrp
config>service>vprn>if>ipv6>vrrp

Description This commands assigns a bi-directional forwarding (BFD) session providing heart-beat mechanism for the given VRRP/SRRP instance. There can be only one BFD session assigned to any given VRRP/SRRP instance, but there can be multiple SRRP/VRRP sessions using the same BFD session. If the interface used is configured with centralized BFD, the BFD transmit and receive intervals need to be set to at least 300ms.

BFD control the state of the associated interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface. The specified interface may not be configured with BFD; when it is, the virtual router will then initiate the BFD session.

The **no** form of this command removes BFD from the configuration.

Default none

Parameters *service-id* — Specifies the service ID of the interface running BFD.

Values *service-id*: 1 — 2147483648
svc-name: Specifies an existing service name up to 64 characters in length.
No service ID indicates a network interface.

interface *interface-name* **—** Specifies the name of the interface running BFD.

dst-ip *ip-address* **—** Specifies the destination address to be used for the BFD session.

init-delay

Syntax **init-delay** *seconds*
no init-delay

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command configures a VRRP initialization delay timer.

Default no init-delay

Parameters *seconds* — Specifies the initialization delay timer for VRRP, in seconds.

Values 1 — 65535

mac

Syntax [**no**] **mac** *ieee-mac-address*

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command assigns a specific MAC address to an IP interface.

The **no** form of this command returns the MAC address of the IP interface to the default value.

Default The physical MAC address associated with the Ethernet interface that the SAP is configured on.

Parameters *ieee-mac-address* — Specifies the 48-bit MAC address for the static ARP in the form *aa***:***bb***:***cc***:***dd***:***ee***:***ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

master-int-inherit

Syntax [**no**] **master-int-inherit**

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command allows the master instance to dictate the master down timer (non-owner context only).

Default no master-int-inherit

message-interval

Syntax **message-interval** {[*seconds*] [**milliseconds** *milliseconds*]}
no message-interval

Context config>service>vprn>if

config>service>vprn>if>ipv6>vrrp

Description This command sets the advertisement timer and indirectly sets the master down timer on the virtual router instance. The message-interval setting must be the same for all virtual routers participating as a virtual router. Any VRRP advertisement message received with an Advertisement Interval field different than the virtual router instance configured message-interval value will be silently discarded.

The message-interval command is available in both non-owner and owner **vrrp** *virtual-router-id* nodal contexts. If the message-interval command is not executed, the default message interval of 1 second will be used.

The **no** form of this command restores the default message interval value of 1 second to the virtual router instance.

Parameters *seconds* — The number of seconds that will transpire before the advertisement timer expires.

Values 1 — 255

Default 1

milliseconds *milliseconds* — Specifies the milliseconds time interval between sending advertisement messages. This parameter is not supported on single-slot chassis.

Values 100 — 900

ping-reply

Syntax [**no**] **ping-reply**

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command enables the non-owner master to reply to ICMP Echo Requests directed at the virtual router instances IP addresses. The ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parental IP interface or based on the Ping source host address). When ping-reply is not enabled, ICMP Echo Requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP Echo Requests regardless of the setting of ping-reply configuration.

The ping-reply command is only available in non-owner **vrrp** *virtual-router-id* nodal context. If the ping-reply command is not executed, ICMP Echo Requests to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all ICMP Echo Request messages destined to the non-owner virtual router instance IP addresses.

Default no ping-reply

policy

Syntax **policy** *vrrp-policy-id*

no policy

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command associates a VRRP priority control policy with the virtual router instance (non-owner context only).

Parameters *vrrp-policy-id* — Specifies a VRRP priority control policy.

Values 1 — 9999

preempt

Syntax **preempt**
no preempt

Context config>service>vprn>if
config>service>vprn>if>ipv6>vrrp

Description This command provides the ability of overriding an existing non-owner master to the virtual router instance. Enabling preempt mode is recommended for proper operation of the base-priority and vrrp-policy-id definitions on the virtual router instance. If the virtual router cannot preempt an existing non-owner master, the affect of the dynamic changing of the in-use priority is greatly diminished.

The preempt command is only available in the non-owner **vrrp** *virtual-router-id* nodal context. The owner may not be preempted due to the fact that the priority of non-owners can never be higher than the owner. The owner will always preempt all other virtual routers when it is available.

Non-owner virtual router instances will only preempt when preempt is set and the current master has an in-use message priority value less than the virtual router instances in-use priority.

A master non-owner virtual router will only allow itself to be preempted when the incoming VRRP Advertisement message Priority field value is one of the following:

- Greater than the virtual router in-use priority value
- Equal to the in-use priority value and the source IP address (primary IP address) is greater than the virtual router instance primary IP address

The **no** form of this command prevents a non-owner virtual router instance from preempting another, less desirable virtual router. Use the preempt command to restore the default mode.

Default preempt

priority

Syntax **priority** *priority*
no priority

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description The priority command provides the ability to configure a specific priority value to the virtual router instance. In conjunction with an optional policy command, the base-priority is used to derive the in-use priority of the virtual router instance.

The priority command is only available in the non-owner **vrrp** *virtual-router-id* nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed. For non-owner virtual router instances, if the priority command is not executed, the base-priority will be set to 100.

The **no** form of this command restores the default value of 100 to base-priority.

Parameters *base-priority* — The base-priority parameter configures the base priority used by the virtual router instance. If a VRRP priority control policy is not also defined, the base-priority will be the in-use priority for the virtual router instance.

Values 1 — 254

Default 100

ssh-reply

Syntax [**no**] **ssh-reply**

Context config>service>vprn>if>vrrp

Description This command enables the non-owner master to reply to SSH Requests directed at the virtual router instance's IP addresses. The SSH request can be received on any routed interface. SSH must not have been disabled at the management security level (either on the parental IP interface or based on the SSH source host address). Proper login and CLI command authentication is still enforced.

When ssh-reply is not enabled, SSH packets to non-owner master virtual IP addresses are silently discarded. Non-owner backup virtual routers never respond to SSH regardless of the ssh-reply configuration.

The ssh-reply command is only available in non-owner **vrrp** *virtual-router-id* nodal context. If the ssh-reply command is not executed, SSH packets to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all SSH packets destined to the non-owner virtual router instance IP addresses.

Default no ssh-reply

standby-forwarding

Syntax [**no**] **standby-forwarding**

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command allows the forwarding of packets by a standby router.

The **no** form of the command specifies that a standby router should not forward traffic sent to virtual router's MAC address. However, the standby router should forward traffic sent to the standby router's real MAC address.

Default no standby-forwarding

telnet-reply

Syntax [**no**] **telnet-reply**

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command enables the non-owner master to reply to TCP port 23 Telnet Requests directed at the virtual router instance's IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Proper login and CLI command authentication is still enforced.

When telnet-reply is not enabled, TCP port 23 Telnet packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet Requests regardless of the telnet-reply configuration.

The telnet-reply command is only available in non-owner **VRRP** nodal context. If the telnet-reply command is not executed, Telnet packets to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all Telnet packets destined to the non-owner virtual router instance IP addresses.

Default no telnet-reply

traceroute-reply

Syntax [**no**] **traceroute-reply**

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the **traceroute-reply** status.

Default no traceroute-reply

PIM Commands

pim

Syntax [**no**] **pim**

Context config>service>vprn

Description This command configures a Protocol Independent Multicast (PIM) instance in the VPRN service. When an PIM instance is created, the protocol is enabled. PIM is used for multicast routing within the network. Devices in the network can receive the multicast feed requested and non-participating routers can be pruned. The router supports PIM sparse mode (PIM-SM).

The **no** form of the command deletes the PIM protocol instance removing all associated configuration parameters.

Default none

apply-to

Syntax **apply-to** {**all** | **none**}

Context config>service>vprn>pim

Description This command creates a PIM interface with default parameters.

If a manually created interface or modified interface is deleted, the interface will be recreated when the **apply-to** command is executed. If PIM is not required on a specific interface, then execute a **shutdown** command.

The **apply-to** command is saved first in the PIM configuration structure, all subsequent commands either create new structures or modify the defaults as created by the **apply-to** command.

Default none (keyword)

Parameters **all** — Specifies that all VPRN and non-VPRN interfaces are automatically applied in PIM.

none — No interfaces are automatically applied in PIM. PIM interfaces must be manually configured.

import

Syntax **import** {**join-policy** | **register-policy**} [*policy-name* [.. *policy-name*] *policy-name*]
no import {**join-policy** | **register-policy**}

Context config>service>vprn>pim

Description This command specifies the import route policy to be used for determining which routes are accepted from peers. Route policies are configured in the **config>router>policy-options** context. When an import policy is not specified, BGP routes are accepted by default.

The **no** form of the command removes the policy association from the IGMP instance.

Default no import join-policy
no import register-policy

Parameters **join-policy —** Use this command to filter PIM join messages which prevents unwanted multicast streams from traversing the network.

register-policy — This keyword filters register messages. PIM register filters prevent register messages from being processed by the RP. This filter can only be defined on an RP. When a match is found, the RP immediately sends back a register-stop message.

policy-name — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>service>vprn>pim

Description This command enables PIM on an interface and enables the context to configure interface-specific parameters. By default interfaces are activated in PIM based on the **apply-to** command, and do not have to be configured on an individual basis unless the default values must be changed.

The **no** form of the command deletes the PIM interface configuration for this interface. If the **apply-to** command parameter is configured, then the **no interface** form must be saved in the configuration to avoid automatic (re)creation after the next **apply-to** is executed as part of a reboot.

The **shutdown** command can be used to disable an interface without removing the configuration for the interface.

Default Interfaces are activated in PIM based on the apply-to command.

Parameters *ip-int-name* — Specify the interface name. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

assert-period

Syntax **assert-period** *assert-period*
no assert-period

Context config>service>vprn>pim>if

Description This command configures the period in seconds for periodic refreshes of PIM Assert messages on an interface.

The **no** form of the command reverts to the default.

Default 60

assert-period — Specifies the period, in seconds, for periodic refreshes of PIM Assert messages on an interface.

Values 1 — 300

bfd-enable

Syntax [**no**] **bfd-enable [ipv4|ipv6]**

Context config>service>vprn>pim>if

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

Default no bfd-enable

bsm-check-rtr-alert

Syntax [**no**] **bsm-check-rtr-alert**

Context config>service>vprn>pim>if

Description This command enables the checking of router alert option in the bootstrap messages received on this interface.

Default no bsm-check-rtr-alert

hello-interval

Syntax **hello-interval** *hello-interval*
no hello-interval

Context config>service>vprn>pim>if

Description This command configures the frequency at which PIM Hello messages are transmitted on this interface.

The **no** form of this command reverts to the default value.

Default **30**

Parameters *hello-interval* — Specifies the hello interval in seconds. A 0 (zero) value disables the sending of hello messages.

Values 0 — 255 seconds

hello-multiplier

Syntax **hello-multiplier** *deci-units*
no hello-multiplier

Context config>service>vprn>pim>if

Description This command configures the multiplier to determine the holdtime for a PIM neighbor.

The **hello-multiplier** in conjunction with the **hello-interval** determines the holdtime for a PIM neighbor.

Parameters *deci-units* — Specify the value, specified in multiples of 0.1, for the formula used to calculate the hello-holdtime based on the hello-multiplier:

(hello-interval * hello-multiplier) / 10

This allows the PIMv2 default timeout of 3.5 seconds to be supported.

Values 20 — 100

Default 35

improved-assert

Syntax [**no**] **improved-assert**

Context config>service>vprn>pim>if

Description This command enables improved assert processing on this interface. The PIM assert process establishes a forwarder for a LAN and requires interaction between the control and forwarding planes.

The assert process is started when data is received on an outgoing interface. This could impact performance if data is continuously received on an outgoing interface.

When enabled, the PIM assert process is done entirely on the control-plane with no interaction between the control and forwarding plane.

Default enabled

instant-prune-echo

[**no**] **instant-prune-echo**

max-groups

Syntax **max-groups** *value*
no max-groups

Context config>service>vprn>pim>if

Description This command configures the maximum number of groups for which PIM can have downstream state based on received PIM Joins on this interface. This does not include IGMP local receivers on the interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed. When this object has a value of 0, there is no limit to the number of groups.

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 — 16000

multicast-senders

Syntax **multicast-senders** {**auto** | **always** | **never**}
no multicast-senders

Context config>service>vprn>pim>if

Description This command configures the way subnet matching is done for incoming data packets on this interface. An IP multicast sender is an user entity to be authenticated in a receiving host.

Parameters **auto —** Subnet matching is automatically performed for incoming data packets on this interface.

always — Subnet matching is always performed for incoming data packets on this interface.

never — Subnet matching is never performed for incoming data packets on this interface.

priority

Syntax **priority** *dr-priority*
no priority

Context config>service>vprn>pim>if

Description This command sets the priority value to become the rendezvous point (RP) that is included in bootstrap messages sent by the router. The RP is sometimes called the bootstrap router.
The **priority** command indicates whether the router is eligible to be a bootstrap router.

The **no** form of the command disqualifies the router to participate in the bootstrap election.

Default **1** (The router is the least likely to become the designated router.)

Parameters *dr-priority* — Specifies the priority to become the designated router. The higher the value, the higher the priority.

Values 1 — 4294967295

sticky-dr

Syntax **sticky-dr** [**priority** *dr-priority*]
no sticky-dr

Context config>service>vprn>pim>if

Description This command enables sticky-dr operation on this interface. When enabled, the priority in PIM hellos sent on this interface when elected as the designateed router (DR) will be modified to the value configured in *dr-priority*. This is done to avoid the delays in forwarding caused by DR recovery, when switching back to the old DR on a LAN when it comes back up.

By enabling **sticky-dr** on this interface, it will continue to act as the DR for the LAN even after the old DR comes back up.

The **no** form of the command disables sticky-dr operation on this interface.

Default disabled

Parameters **priority** *dr-priority* — Sets the DR priority to be sent in PIM Hello messages following the election of that interface as the DR, when sticky-dr operation is enabled.

Values 1 — 4294967295

three-way-hello

Syntax **three-way-hello** [**compatibility-mode**]
no three-way-hello

Context config>service>vprn>pim>if

Description This command configures the compatibility mode for enabling the three way hello.

Parameters **compatibility-mode** — Specifies to enable the three way hello.

tracking-support

Syntax [**no**] **tracking-support**

Context config>service>vprn>pim>if

Description This command sets the the T bit in the LAN Prune Delay option of the Hello Message. This indicates the router's capability to disable Join message suppression.

Default no tracking-support

ipv4-multicast-disable

Syntax [**no**] **ipv4-multicast-disable**

Context config>service>vprn>pim
config>service>vprn>pim>interface

Description This command administratively disables/enables PIM operation for IPv4.

Default no ipv4-multicast-disable

ipv6-multicast-disable

Syntax **ipv6-multicast-disable**

Context config>service>vprn>pim
config>service>vprn>pim>interface

Description This command administratively disables/enables PIM operation for IPv6.

Default ipv6-multicast-disable

mc-ecmp-balance

Syntax [**no**] **mc-ecmp-balance**

Context config>service>vprn>pim

Description This command enables multicast balancing of traffic over ECMP links. When enabled, each multicast stream that needs to be forwarded over an ECMP link will be re-evaluated for the total multicast bandwidth utilization. Re-evaluation occurs on the ECMP interface in question.

The **no** form of the command disables the multicast balancing.

mc-ecmp-balance-hold

Syntax **mc-ecmp-balance-hold** *minutes*
no mc-ecmp-balance-hold

Context config>service>vprn>pim

Description This command configures the hold time for multicast balancing over ECMP links.

Parameters *minutes* — Specifies the hold time, in minutes, that applies after an interface has been added to the ECMP link.

mc-ecmp-hashing-enabled

Syntax [**no**] **mc-ecmp-hashing-enabled**

Context config>service>vprn>pim

Description This command distributes PIM joins over the multiple ECMP paths based on a hash of S and G. When a link in the ECMP set is removed, the multicast streams that were using that link are re-distributed over the remaining ECMP links using the same hash algorithm. When a link is added to the ECMP set, new joins may be allocated to the new link based on the hash algorithm, but existing multicast streams using the other ECMP links stay on those links until they are pruned.

The **no mc-ecmp-hashing-enabled** form of the command means that the use of multiple ECMP paths if enabled at the **config>router** or **config>service>vprn** context is controlled by the existing implementation and CLI commands **mc-ecmp-balance**.

Default no mc-ecmp-hashing-enabled

non-dr-attract-traffic

Syntax [**no**] **non-dr-attract-traffic**

Context config>service>vprn>pim

Description This command specifies whether the router should ignore the designated router state and attract traffic even when it is not the designater router.

An operator can configure an interface (router or IES or VPRN interfaces) to IGMP and PIM. The interface IGMP state will be synchronized to the backup node if it is associated with the redundant peer port. The interface can be configured to use PIM which will cause multicast streams to be sent to the elected DR only. The DR will also be the router sending traffic to the DSLAM. Since it may be required to attract traffic to both routers a flag non-dr-attract-trafffic can be used in the PIM context to have the router ignore the DR state and attract traffic when not DR. Note that while using this flag the router may not send the stream down to the DSLAM while not DR.

When enabled, the designated router state is ignored. When disabled, **no non-dr-attract-traffic**, the designated router value is honored.

Default no non-dr-attract-traffic

rp

Syntax **rp**

Context config>service>vprn>pim

Description This command enables access to the context to configure the rendezvous point (RP)) of a PIM protocol instance.

An Alcatel-Lucent PIM router acting as an RP must respond to a PIM register message specifying an SSM multicast group address by sending to the first hop router stop register message(s). It does not build an (S, G) shortest path tree toward the first hop router. An SSM multicast group address can be either from the SSM default range of 232/8 or from a multicast group address range that was explicitly configured for SSM.

Default rp enabled when PIM is enabled.

anycast

Syntax [**no**] **anycast** *rp-ip-address*

Context config>service>vprn>pim>rp

Description This command configures a PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The **no** form of the command removes the anycast instance from the configuration.

Default none

Parameters *rp-ip-address* — Configure the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address will be replaced with the new address. If no ip-address is entered then the command is simply used to enter the anycast CLI level.

Values Any valid loopback address configured on the node.

rp-set-peer

Syntax [**no**] **rp-set-peer** *ip-address*

Context config>service>vprn>pim>rp>anycast

Description This command configures a peer in the anycast rp-set. The address identifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this rp-set.

Although there is no set maximum of addresses that can be configured in an rp-set, up to 15 multicast addresses is recommended.

The **no** form of the command removes an entry from the list.

Default None

Parameters *ip-address* — Specifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

auto-rp-discovery

Syntax [**no**] **auto-rp-discovery**

Context config>service>vprn>pim>rp

Description This command enables Auto-RP protocol in discovery mode. In discovery mode, RP-mapping and RP-candidate messages are received and forwarded to downstream nodes. RP-mapping messages are received locally to learn about availability of RP nodes present in the network.

The **no** form of the command disables auto RP.

Default disabled

bootstrap-export

Syntax **bootstrap-export** *policy-name* [*policy-name*... up to five]
no bootstrap-export

Context config>service>vprn>pim>rp

Description This command exports policies to control the flow of bootstrap messages from the RP. Up to five policies can be defined.

The **no** form of this command removes the specified policy names from the configuration.

Default none

Parameters *policy-name* — Specify the policy name. The policy statement must already be configured in the config>router>policy-options context.

bootstrap-import

Syntax **bootstrap-import** *policy-name* [*policy-name*... up to five]
no bootstrap-import *policy-name* [*policy-name*... up to five]

Context config>service>vprn>pim>rp

Description This command imports policies to control the flow of bootstrap messages into the RP. Up to five policies can be defined.

The **no** form of this command removes the specified policy names from the configuration.

Default none

Parameters *policy-name* — Specify the policy name. The policy statement must already be configured in the config>router>policy-options context.

bsr-candidate

Syntax **bsr-candidate**

Context config>service>vprn>pim>rp
config>service>vprn>pim>rp>ipv6

Description This command enables the context to configure a local rendezvous point (RP) of a PIM protocol instance.

Default Enabled when PIM is enabled.

address

Syntax **[no] address** *ip-address*

Context config>service>vprn>pim>rp>bsr-candidate
config>service>vprn>pim>rp>rp-candidate

Description This command configures a static bootstrap or rendezvous point (RP) as long as the source is not directly attached to this router.

Use the **no** form of this command to remove the static RP from the configuration.

Default No IP address is specified.

Parameters *ip-address* — The static IP address of the RP. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 – 223.255.255.255

address

Syntax **[no] address** *ipv6-address*

Context config>service>vprn>pim>rp>ipv6>bsr-candidate
config>service>vprn>pim>rp>ipv6>rp-candidate

Description This command configures a static bootstrap or rendezvous point (RP) as long as the source is not directly attached to this router.

Use the **no** form of this command to remove the static RP from the configuration.

Default No IP address is specified.

Parameters *ipv6-address* — The static IP address of the RP. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values

ipv6-address	: x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0..FFFF]H
	d [0..255]D

hash-mask-len

Syntax **hash-mask-len** *hash-mask-length*
no hash-mask-len

Context config>service>vprn>pim>rp>bsr-candidate

Description This command is used to configure the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

Default 30

Parameters *hash-mask-length* — The hash mask length.

Values 0 — 32

hash-mask-length

Syntax **hash-mask-length** *hash-mask-length*
no hash-mask-length

Context config>service>vprn>pim>rp>ipv6>bsr-candidate

Description This command is used to configure the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

Default 126

Parameters *hash-mask-length* — The hash mask length.

Values 0 — 128

priority

Syntax **priority** *bootstrap-priority*

Context config>service>vprn>pim>rp>bsr-candidate
config>service>vprn>pim>rp>ipv6>bsr-candidate

Description This command defines the priority used to become the rendezvous point (RP) . The higher the priority value the more likely that this router becomes the RP. If there is a tie, the router with the highest IP address is elected.

Parameters *bootstrap-priority* — The priority to become the bootstrap router.

Values 0 — 255

Default 0 (the router is not eligible to be the bootstrap router)

ipv6

Syntax **ipv6**

Context config>service>vprn>pim>rp

Description This command enables access to the context to configure the rendezvous point (RP) of a PIM IPv6 protocol instance.

An Alcatel-Lucent IPv6 PIM router acting as an RP must respond to an IPv6 PIM register message specifying an SSM multicast group address by sending to the first hop router stop register message(s). It does not build an (S, G) shortest path tree toward the first hop router. An SSM multicast group address can be either from the SSM default range or from a multicast group address range that was explicitly configured for SSM.

Default ipv6 RP enabled when IPv6 PIM is enabled.

anycast

Syntax **anycast** *ipv6-address*
no anycast *ipv6-address*

Context config>service>vprn>pim>rp>ipv6

Description This command configures an IPv6 PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The **no** form of the command removes the anycast instance from the configuration.

Default none

Parameters *ipv6-address* — Configures the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address will be replaced with the new address. If no address is entered then the command is simply used to enter the anycast CLI level. –thi highlighted text is invalid, don't add here and please remove from IPv4 command

Values *ipv6-address* : x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0..FFFF]H
d [0..255]D

rp-set-peer

Syntax **[no] rp-set-peer** *ipv6-address*

Context config>service>vprn>pim>rp>ipv6>anycast

Description This command configures an IPv6 peer in the anycast rp-set. The address identifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this rp-set.

Although there is no set maximum of addresses that can be configured in an rp-set, up to 15 multicast addresses is recommended.

The **no** form of the command removes an entry from the list.

Default None

Parameters *ipv6-address* — Specifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

Values ipv6-address : x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0..FFFF]H
d [0..255]D

embedded-rp

Syntax **embedded-rp**

Context config>service>vprn>pim>rp>ipv6

Description This command enables context to configure IPv6 embedded RP parameteres.

group-range

Syntax **[no] group-range** *{ipv6-address/prefix-length}*

Context config>service>vprn>pim>rp>ipv6>embedded-rp
config>service>vprn>pim>rp>ipv6>rp-candidate

Description This command configures the group address or range of group addresses for which this router can be the rendezvous point (RP).

Use the no form of this command to remove the group address or range of group addresses for which this router can be the RP from the configuration.

Default none

Parameters *ipv6-address* — Specify the addresses or address ranges that this router can be an RP.

prefix-length — Specify the address prefix length.

Values ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d

x [0..FFFF] H
d [0..255] D
prefix-length [8..128] // for embedded-rp
prefix-length [16..128] // for rp-candidate

group-prefix

Syntax **[no] group-prefix grp-ipv6-address/prefix-length**

Context config>service>vprn>pim>rp>ipv6>static

Description The group-prefix for a static-rp defines a range of multicast-ip-addresses for which this static RP is applicable.

The no form of the command removes the criterion.

Default none

Parameters *grp-ipv6-address* — Specifies the multicast IPv6 address.

prefix-length — Specifies the address prefix length.

Values

grp-ipv6-address	x:x:x:x:x:x:x:x	(eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d	
	x [0..FFFF] H	
	d [0..255] D	
prefix-length	*[8..128]*	

rp-candidate

Syntax **rp-candidate**

Context config>service>vprn>pim>rp
config>service>vprn>pim>rp>ipv6

Description This command enables the context to configure the candidate rendezvous point (RP) parameters.

Default Enabled when PIM is enabled.

group-range

Syntax [**no**] **group-range** {*ip-prefix*/*mask* | *ip-prefix netmask*}

Context config>service>vprn>pim>rp>rp-candidate
config>service>vprn>pim>ssm

Description This command configures the group address or range of group addresses for which this router can be the rendezvous point (RP).

Use the **no** form of this command to remove the group address or range of group addresses for which this router can be the RP from the configuration.

Default none

Parameters *ip-prefix* — Specify the addresses or address ranges that this router can be an RP.

Values
ipv4-prefix - a.b.c.d
ipv4-prefix-le - [0..32]
ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bitpieces)
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D
ipv6-prefix-le - [0..128]

mask — Specify the address mask with the address to define a range of addresses.

netmask — Specify the subnet mask in dotted decimal notation.

Values :a.b.c.d (network bits all 1 and host bits all 0)

holdtime

Syntax **holdtime** *holdtime*
no holdtime *holdtime*

Context config>service>vprn>pim>rp>rp-candidate
config>service>vprn>pim>rp>ipv6>rp-candidate

Description Use this command to define the length of time neighboring router consider this router to be up.

Use the **no** form of this command to revert to the default value.

Default 150

Parameters *holdtime* — Specify the length of time, in seconds, that neighbor should consider the sending router to be operational.

Values 0 — 255

priority

Syntax **priority** *priority*
no priority *priority*

Context config>router>pim>rp>local
config>service>vprn>pim>rp>rp-candidate

Description This command defines the priority used to become the rendezvous point (RP). The higher the priority value, the more likely that this router will become the RP.

Use the **no** form of this command to revert to the default value.

Default 1

Parameters *priority* — Specify the priority to become the designated router. The higher the value the more likely the router will become the RP.

Values 0 — 255

static

Syntax **static**

Context config>service>vprn>pim>rp

Description This command enables access to the context to configure a static rendezvous point (RP) of a PIM-SM protocol instance.

Default none

address

Syntax [**no**] **address** *ip-address*

Context config>service>vprn>pim>rp>static

Description This command configures the static rendezvous point (RP) address.

The **no** form of this command removes the static RP entry from the configuration.

Default none

group-prefix

Syntax [**no**] **group-prefix** {*grp-ip-address*/*mask* | *grp-ip-address netmask*}

Context config>service>vprn>pim>rp>static

Context The **group-prefix** for a static-rp defines a range of multicast-ip-addresses for which a certain RP is applicable.

The **no** form of the command removes the criterion.

Default none

Parameters *grp-ip-address* — Specify the multicast IP address.

mask — Defines the mask of the multicast-ip-address.

Values 4 — 32

netmask — Enter the subnet mask in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

override

Syntax [**no**] **override**

Context config>service>vprn>pim>rp>static

Description This command changes the precedence of static RP over dyanamically learned Rendezvous Point (RP).

When enabled, the static group-to-RP mappings take precedence over the dynamically learned mappings.

Default no override

rpf-table

Syntax [**no**] **rpf-table** {**rtable-m** | **rtable-u** | **both**}

Context config>service>vprn>pim

Description This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a particular multicast route.

By default, only the unicast route table is looked up to calculate RPF interface towards the source/ rendezvous point. However, the operator can specify the following:

a) Use unicast route table only

b) Use multicast route table only or

c) Use both the route tables.

Default rpf-table rtable-u

Parameters **rtable-m —** pecified that only the multicast route table is to be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table contains routes submitted by static routes and OSPF.

rtable-u — Specifies that only the unicast route table is to be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table contains routes submitted by all the unicast routing protocols.

both — Specifies that PIM always lookup first in the multicast route table, and if there is a route, PIM use it. If PIM does not find a route in the first lookup, it will try to find it in the unicast route table. rtable-m is checked before rtable-u.

spt-switchover-threshold

Syntax **spt-switchover-threshold** {*grp-ip-address/mask* | *grp-ip-address netmask*} *spt-threshold*
no spt-switchover-threshold {*grp-ip-address/mask* | *grp-ip-address netmask*}

Context config>service>vprn>pim

Description This command configures a shortest path tree (SPT tree) switchover threshold for a group prefix.

Parameters *grp-ip-address* — Specify the multicast group address.

mask — Defines the mask of the multicast-ip-address.

Values 4 — 32

netmask — Enter the subnet mask in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

spt-threshold — Specifies the configured threshold in kilo-bits per second(kbps) for the group to which this (S,G) belongs. For a group G configured with a threshold, switchover to SPT for an (S,G) is attempted only if the (S,G)'s rate exceeds this configured threshold.

ssm-assert-compatible-mode

Syntax **ssm-assert-compatible-mode [enable|disable]**

Context config>service>vprn>pim

Description This command specifies whether SSM assert is enabled in compatibility mode for this PIM protocol instance. When enabled, for SSM groups, PIM will consider the SPT bit to be implicitly set to compute the value of CouldAssert (S,G,I) as defined in RFC 4601, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*. When disabled, for SSM groups, PIM will not assume the SPT bit to be set. The SPT bit will be set by Update_SPTbit(S,G,iif) macro defined in RFC 4601.

Default disable

Parameters **enable —** Enables SSM assert in compatibility mode for this PIM protocol instance.

disable — Disabled SSM assert in compatibility mode for this PIM protocol instance.

ssm-default-range-disable

Syntax **ssm-default-range-disable ipv4**

Context config>service>vprn>pim

Description This command specifies whether to disable the use of default range (232/8) for SSM so that it can be used by ASM to process (*,G). When enabled, the use of default range is disabled for SSM and it can be used by ASM. When disabled, the SSM default range is enabled.

Default disable

ssm-groups

Syntax [**no**] **ssm-groups**

Context config>service>vprn

Description This command enables access to the context to enable a source-specific multicast (SSM) configuration instance.

Default none

C-MLDP Commands

mld

Syntax [**no**] **mld**

Context config>service>vprn

Description This command enables the context to configure Multicast Listener Discovery (MLD) parameters.

The **no** form of the command disables MLD.

Default no mld

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>service>vprn>mld

Description This command enables the context to configure an Multicast Listener Discovery (MLD) interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled.

The **no** form of the command deletes the MLD interface. The **shutdown** command in the **config>router>mld>interface** context can be used to disable an interface without removing the configuration for the interface.

Default **no interface** — No interfaces are defined.

Parameters *ip-int-name* — The IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context config>service>vprn>mld>interface

Description This command enables router alert checking for MLD messages received on this interface.

The no form of the command disables the router alert checking.

Default none

import

Syntax **import** *policy-name*
no import

Context config>service>vprn>mld>interface

Description This command specifies the import route policy to be used for determining which membership reports are accepted by the router. Route policies are configured in the **config>router>policy-options** context.

When an import policy is not specified, all the MLD reports are accepted.

The **no** form of the command removes the policy association from the MLD instance.

Default **no import** — No import policy specified.

Parameters *policy-name* — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

max-groups

Syntax **max-groups** *value*
no max-groups

Context config>service>vprn>mld>interface

Description This command specifies the maximum number of groups for which MLD can have local receiver information based on received MLD reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

Default 0, no limit to the number of groups.

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 — 16000

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context config>service>vprn>mld>interface

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default 125

Parameters *seconds* — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 — 1024

query-last-member-interval

Syntax **query-last-member-interval** *seconds*

Context config>service>vprn>mld>interface

Description This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default 1

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 — 1024

query-response-interval

Syntax **query-response-interval** *seconds*

Context config>service>vprn>mld>interface

Description This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default 10

Parameters *seconds* — Specifies the the length of time to wait to receive a response to the host-query message from the host.

Values 1 — 1023

static

Syntax **static**

Context config>service>vprn>mld>interface

Description This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Default none

group

Syntax [**no**] **group** *ipv6-address*

Context config>service>vprn>mld>interface>static

Description This command enables the context to add a static multicast group either as a (*,G) or one or more (S,G) records. Use MLD static group memberships to test multicast forwarding without a receiver host. When MLD static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static MLD group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static MLD group entries do not generate join messages toward the RP.

The **no** form of the command removes the IPv6 address from the configuration.

Default none

Parameters *ipv6-address* — Specifies an MLD multicast group address that receives data on an interface. The IP address must be unique for each static group.

source

Syntax [**no**] **source** *ipv6-address*

Context config>service>vprn>mld>interface>static>group

Description This command specifies an IPv6 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the source(s) that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The source command, in combination with the group, is used to create a specific (S,G) static group entry.

The **no** form of the command removes the source from the configuration.

Default none

Parameters *ip-address* — Specifies the IPv6 unicast address.

starg

Syntax [**no**] **starg**

Context config>service>vprn>mld>interface>static>group

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the **no** form of the command to remove the starg entry from the configuration.

Default none

version

Syntax **version** *version*
no version

Context config>service>vprn>mld>interface

Description This command specifies the MLD version. If routers run different versions, they will negotiate the lowest common version of MLD that is supported by hosts on their subnet and operate in that version. For MLD to function correctly, all routers on a LAN should be configured to run the same version of MLD on that LAN.

Default 1

Parameters *version* — Specifies the MLD version number.

Values 1, 2

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context config>service>vprn>mld

Description This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default 2

Parameters *robust-count* — Specify the robust count value.

Values 2 — 10

ssm-translate

Syntax **ssm-translate**

Context config>service>vprn>mld

Description This command enables the context to configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the **source** command with **starg** command enabled.

grp-range

Syntax [**no**] **grp-range** *start end*

Context config>service>vprn>mld>ssm-translate

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters *start* — An IP address that specifies the start of the group range.

end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the *start* value.

source

Syntax [**no**] **source** *ip-address*

Context config>service>vprn>mld>ssm-translate>grp-range

Description This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters *ip-address* — Specifies the IP address that will be sending data.

Network Interface Commands

network-interface

Syntax **network-interface** *interface-name* [**create**]
no network-interface *interface-name*

Context config>service>vprn

Description This command configures a network interface in a VPRN that acts as a CSC interface to a CSC-CE in a Carrier Supporting Carrier IP VPN deployment model.

BGP Commands

bgp

Syntax [**no**] **bgp**

Context service>vprn

Description This command enables the BGP protocol with the VPRN service.

The **no** form of the command disables the BGP protocol from the given VPRN service.

Default no bgp

bgp-shared-queue

Syntax **bgp-shared-queue** [**cir** *rate*] [**pir** *rate*]
no bgp-shared-queue

Context config>service>vprn

Description This command enables all BGP peers within a VPRN instance to share a single CPM queue. This command takes affect on new BGP connections established; already established BGP peers continue to use their own CPM queue. Any changes to PIR/CIR of the shared queue takes effect only after BGP connections are re-established.

Parameters **cir** *rate* — Specifies the CIR rate for the shared queue.

pir *rate* — Specifies the PIR rate for the shared queue.

advertise-inactive

Syntax [**no**] **advertise-inactive**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables or disables the advertising of inactive BGP routers to other BGP peers.

By default, BGP only advertises BGP routes to other BGP peers if a given BGP route is chosen by the route table manager as the most preferred route within the system and is active in the forwarding plane. This command allows system administrators to advertise a BGP route even though it is not the most preferred route within the system for a given destination.

Default no advertise-inactive

aggregator-id-zero

Syntax [**no**] **aggregator-id-zero**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command is used to set the router ID in the BGP aggregator path attribute to zero when BGP aggregates routes. This prevents different routers within an AS from creating aggregate routes that contain different AS paths.

When BGP is aggregating routes, it adds the aggregator path attribute to the BGP update messages. By default, BGP adds the AS number and router ID to the aggregator path attribute.

When this command is enabled, BGP adds the router ID to the aggregator path attribute. This command is used at the group level to revert to the value defined under the global level, while this command is used at the neighbor level to revert to the value defined under the group level.

The **no** form of the command used at the global level reverts to default where BGP adds the AS number and router ID to the aggregator path attribute.

The **no** form of the command used at the group level reverts to the value defined at the group level.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default no aggregator-id-zero — BGP adds the AS number and router ID to the aggregator path attribute.

always-compare-med

Syntax **always-compare-med** {**zero** | **infinity**}
no always-compare-med strict-as {zero | infinity}
no always-compare-med

Context config>router>bgp>best-path-selection

Description This command configures the comparison of BGP routes based on the MED attribute. The default behavior of SR-OS (equivalent to the **no** form of the command) is to only compare two routes on the basis of MED if they have the same neighbor AS (the first non-confed AS in the received AS_PATH attribute). Also by default, a route without a MED attribute is handled the same as though it had a MED attribute with the value 0. The **always-compare-med** command without the **strict-as** keyword allows MED to be compared even if the paths have a different neighbor AS; in this case, if neither **zero** or **infinity** is specified, the **zero** option is inferred, meaning a route without a MED is handled the same as though it had a MED attribute with the value 0. When the **strict-as** keyword is present, MED is only compared between paths from the same neighbor AS, and in this case, **zero** or **infinity** is mandatory and tells BGP how to interpret paths without a MED attribute.

Default **no always-compare-med**

Parameters **zero —** Specifies that for routes learned without a MED attribute that a zero (0) value is used in the MED comparison. The routes with the lowest metric are the most preferred.

infinity — Specifies for routes learned without a MED attribute that a value of infinity (2^32-1) is used in the MED comparison. This in effect makes these routes the least desirable.

strike-as — Specifies BGP paths to be compared even with different neighbor AS.

as-path-ignore

Syntax [**no**] **as-path-ignore**

Context config>service>vprn>bgp

Description This command determines whether the AS path is used to determine the best BGP route.

If this option is present, the AS paths of incoming routes are not used in the route selection process.

The **no** form of the command removes the parameter from the configuration.

Default no as-path-ignore

deterministic-med

Syntax [**no**] **deterministic-med**

Context config>service>vprn>bgp>best-path-selection

Description This command controls how the BGP decision process compares routes on the basis of MED. When **deterministic-med** is configured, BGP groups paths that are equal up to the MED comparison step based on neighbor AS, and then compares the best path from each group to arrive at the overall best path. This change to the BGP decision process makes best path selection completely deterministic in all cases. Without **deterministic-med**, the overall best path selection is sometimes dependent on the order of the route arrival because of the rule that MED cannot be compared in routes from different neighbor AS.

Default no deterministic-med

as-override

Syntax [**no**] **as-override**

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command replaces all instances of the peer's AS number with the local AS number in a BGP route's AS_PATH.

This command breaks BGP's loop detection mechanism. It should be used carefully.

Default as-override is not enabled by default.

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
no authentication-key

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the BGP authentication key.

Authentication is performed between neighboring routers before setting up the BGP session by verifying the password. Authentication is performed using the MD-5 message-based digest. The authentication key can be any combination of letters or numbers from 1 to 16.

The no form of the command removes the authentication password from the configuration and effectively disables authentication.

Default Authentication is disabled and the authentication password is empty.

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 255 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

auth-keychain

Syntax **auth-keychain** *name*

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the BGP authentication key for all peers.

The keychain allows the rollover of authentication keys during the lifetime of a session.

Default **no auth-keychain**

Parameters *name* — Specifies the name of an existing keychain, up to 32 characters, to use for the specified TCP session or sessions.

backup-path

Syntax [**no**] **backup-path** [**ipv4**] [**ipv6**]

Context config>router
config>router>bgp
config>service>vprn>bgp

Description This command enables the computation and use of a backup path for IPv4 and/or IPv6 BGP-learned prefixes belonging to the base router or a particular VPRN. Multiple paths must be received for a prefix in order to take advantage of this feature. When a prefix has a backup path and its primary path(s) fail the affected traffic is rapidly diverted to the backup path without waiting for control plane re-convergence to occur. When many prefixes share the same primary path(s), and in some cases also the same backup path, the time to failover traffic to the backup path is independent of the number of prefixes. In some cases prefix independent convergence may require use of FP2 or later IOMs/IMMs/XMAs.

By default, IPv4 and IPv6 prefixes do not have a backup path installed in the IOM.

Default **no backup-path**

Parameters **ipv4 —** enable the use of a backup path for BGP-learned IPv4 prefixes.

ipv6 — enable the use of a backup path for BGP-learned IPv6 prefixes.

best-path-selection

Syntax **best-path-selection**

Context config>service>vprn>bgp

Description This command enables path selection configuration.

ignore-nh-metric

Syntax **ignore-nh-metric**
no ignore-nh-metric

Context config>router>bgp>best-path-selection
config>service>vprn
config>service>vprn>bgp>best-path-selection

Description This command instructs BGP to disregard the resolved distance to the BGP next-hop in its decision process for selecting the best route to a destination. When configured in the config>router>bgp>best-path-selection context, this command applies to the comparison of two BGP routes with the same NLRI learned from base router BGP peers. When configured in the config>service>vprn context, this command applies to the comparison of two BGP-VPN routes for the same IP prefix imported into the VPRN from the base router BGP instance. When configured in the config>service>vprn>bgp>best-path-selection context, this command applies to the comparison of two BGP routes for the same IP prefix learned from VPRN BGP peers.

The no form of the command (no ignore-nh-metric) restores the default behavior whereby BGP factors distance to the next-hop into its decision process.

Default **no ignore-nh-metric**

ignore-router-id

Syntax **ignore-router-id**
no ignore-router-id

Context config>router>bgp>best-path-selection
config>service>vprn>bgp>best-path-selection

Description When the ignore-router-id command is present and the current best path to a destination was learned from EBGP peer X with BGP identifier x and a new path is received from EBGP peer Y with BGP identifier y the best path remains unchanged if the new path is equivalent to the current best path up to the BGP identifier comparison – even if y is less than x. The no form of the command restores the default behavior of selecting the route with the lowest BGP identifier (y) as best.

Default **no ignore-router-id**

bfd-enable

Syntax [**no**] **bfd-enable**

Context config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated BGP protocol peering.

Default **no bfd-enable**

cluster

Syntax **cluster** *cluster-id*
no cluster

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the cluster ID for a route reflector server.

Route reflectors are used to reduce the number of IBGP sessions required within an AS. Normally, all BGP speakers within an AS must have a BGP peering with every other BGP speaker in an AS. A route reflector and its clients form a cluster. Peers that are not part of the cluster are considered to be non-clients.

When a route reflector receives a route, first it must select the best path from all the paths received. If the route was received from a non-client peer, then the route reflector sends the route to all clients in the cluster. If the route came from a client peer, the route reflector sends the route to all non-client peers and to all client peers except the originator.

For redundancy, a cluster can have multiple route reflectors.

Confederations can also be used to remove the full IBGP mesh requirement within an AS.

The **no** form of the command deletes the cluster ID and effectively disables the Route Reflection for the given group.

Default no cluster — No cluster ID is defined.

Parameters *cluster-id* — The route reflector cluster ID is expressed in dot decimal notation.

Values Any 32 bit number in dot decimal notation. (0.0.0.1 — 255.255.255.255)

connect-retry

Syntax **connect-retry** *seconds*
no connect-retry

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the BGP connect retry timer value in seconds.

When this timer expires, BGP tries to reconnect to the configured peer. This configuration parameter can be set at three levels: global level (applies to all peers), peer-group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of the command used at the global level reverts to the default value.
The **no** form of the command used at the group level reverts to the value defined at the global level.
The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default 120 seconds

Parameters *seconds* — The BGP Connect Retry timer value in seconds, expressed as a decimal integer.

Values 1 — 65535

damp-peer-oscillations

Syntax **damp-peer-oscillations** [**idle-hold-time** *initial-wait second-wait max-wait*] [**error-interval** *minutes*]

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command controls how long a BGP peer session remains in the idle-state after some type of error causes the session to reset. In the idle state, BGP does not initiate or respond to attempts to establish a new session. Repeated errors that occur a short while after each session reset cause longer and longer hold times in the idle state. This command supports the DampPeerOscillations FSM behavior described in section 8.1 of RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*.

The default behavior, which applies when no damp-peer-oscillations is configured, is to immediately transition out of the idle-state after every reset.

Default *no damp-peer-oscillations*

Parameters *initial-wait* — The amount of time, in minutes, that a session remains in the idle-state after it has been stable for a while.

Values 0 — 2048

Default 0

second-wait — A period of time, in minutes, that is doubled after each repeated session failure that occurs within a relatively short span of time.

Values 0 — 2048

Default 5

max-wait — The maximum amount of time, in minutes, that a session remains in the idle-state after it has experienced repeated instability.

Values 0 — 2048

Default 60

minutes — The interval of time, in minutes after a session reset, during which the session must be error-free in order to reset the penalty counter and return to idle-hold-time to initial-wait.

Values 0 — 2048

Default 30

damping

Syntax [**no**] **damping**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables BGP route damping for learned routes which are defined within the route policy. Use damping to reduce the number of update messages sent between BGP peers and reduce the load on peers without affecting the route convergence time for stable routes. Damping parameters are set via route policy definition.

The **no** form of the command used at the global level disables route damping.
The **no** form of the command used at the group level reverts to the value defined at the global level.
The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

When damping is enabled and the route policy does not specify a damping profile, the default damping profile is used. This profile is always present and consists of the following parameters:

Half-life: 15 minutes
Max-suppress: 60 minutes
Suppress-threshold:3000
Reuse-threshold 750

Default no damping — Learned route damping is disabled.

disable-4byte-asn

Syntax [**no**] **disable-4byte-asn**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command disables the use of 4-byte ASNs. It can be configured at all 3 level of the hierarchy so it can be specified down to the per peer basis.

If this command is enabled 4-byte ASN support should not be negotiated with the associated remote peer(s).

The **no** form of the command resets the behavior to the default which is to enable the use of 4-byte ASN.

disable-capability-negotiation

Syntax [**no**] **disable-capability-negotiation**

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command disables the exchange of capbilities. When command is enabled and after the peering is flapped, any new capabilities are not negotiated and will strictly support IPv4 routing exchanges with that peer.

The **no** form of the command removes this command from the configuration and restores the normal behavior.

Default no disable-capability-negotiation

disable-client-reflect

Syntax [**no**] **disable-client-reflect**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command disables the reflection of routes by the route reflector to the group or neighbor. This only disables the reflection of routes from other client peers. Routes learned from non-client peers are still reflected to all clients.

The **no** form re-enables client reflection of routes.

Default no disable-client-reflect — Client routes are reflected to all client peers.

disable-communities

Syntax **disable-communities** [**standard**] [**extended**]
no disable-communities

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures BGP to disable sending communities.

Parameters **standard —** Specifies standard communities that existed before VPRNs or 2547.

extended — Specifies BGP communities used were expanded after the concept of 2547 was introduced, to include handling the VRF target.

disable-fast-external-failover

Syntax [**no**] **disable-fast-external-failover**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures BGP fast external failover.

eibgp-loadbalance

Syntax [**no**] **eibgp-loadbalance**

Context config>service>vprn>bgp

Description This command enables eiBGP load sharing so routes with both MP-BGP and IPv4 next-hops can be used simultaneously.

In order for this command to be effective, the **ecmp** and **multipath** commands for the associated VPRN instance must also be configured to allow for multiple routes to the same destination.

The **no** form of the command used at the global level reverts to default values.

Default no eibgp-loadbalance — Multipath disabled.

enable-bgp-vpn-backup

Syntax **enable-bgp-vpn-backup [ipv4] [ipv6]**
no enable-bgp-vpn-backup

Context config>service>vprn

Description This command enables BGP-VPN routes imported into the VPRN to have backup paths calculated for them (when they are the best path) and to be considered as backup path candidates (for other VPN-IP routes and VPRN BGP routes learned from CEs).

Default no enable-bgp-vpn-backup

enable-peer-tracking

Syntax [**no**] **enable-peer-tracking**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables BGP peer tracking.

Default no enable-peer-tracking

graceful-restart

Syntax [**no**] **graceful-restart**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables or disables graceful-restart for all VPRN BGP peers.

enable-notification

Syntax **enable-notification**
no enable-notification

Context config>service>vprn>bgp>graceful-restart
config>service>vprn>bgp>group>graceful-restart
config>service>vprn>bgp>group>neighbor>graceful-restart

Description When this command is present, the graceful restart capability sent by this router indicates support for NOTIFICATION messages. If the peer also supports this capability then the session can be restarted gracefully (while preserving forwarding) if either peer needs to sends a NOTIFICATION message due to some type of event or error.

Default no enable-notification

restart-time

Syntax **restart-time** *seconds*
no restart-time

Context config>service>vprn>bgp>graceful-restart
config>service>vprn>bgp>group>graceful-restart
config>service>vprn>bgp>group>neighbor>graceful-restart

Description This command sets the value of the restart-time that is advertised in the router's graceful-restart capability. If this command is not configured, the default is 300.

Default no restart time

Parameters *seconds* — The restart-time that is advertised in the router's graceful-restart capability.

Values 0 — 4095 seconds

Default 300

stale-routes-time

Syntax [**no**] **stale-routes-time** *time*

Context config>service>vprn>bgp>graceful-restart
config>service>vprn>bgp>group>graceful-restart
config>service>vprn>bgp>group>neighbor>graceful-restart

Description This command configures the time period to keep stale routes before the END-OF-RIB message is received from the restarting router.

Parameters *time* — [1..3600 seconds]

Default 360 seconds

error-handling

Syntax **error-handling**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command specifies whether the error handling mechanism for optional transitive path attributes is enabled for this peer group.

update-fault-tolerance

Syntax [**no**] **update-fault-tolerance**

Context config>service>vprn>bgp>error-handling
config>service>vprn>bgp>group>error-handling
config>service>vprn>bgp>group>neighbor>error-handling

Description This command enables **treat-as-withdraw** and other similarly non-disruptive approaches for handling a wide range of UPDATE message errors, as long as there are no length errors that prevent all of the NLRI fields from being correctly identified and parsed.

Default no fault-tolerance

export

Syntax **export** *policy* [*policy*...]
no export

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor
config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command specifies the export policies to be used to control routes advertised to BGP neighbors.

When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of five (5) policy names can be configured. The first policy that matches is applied.

Note that if a non-existent route policy is applied to a VPRN instance, the CLI generates a warning message. This message is only generated at an interactive CLI session and the route policy association is made. No warning message is generated when a non-existent route policy is applied to a VPRN instance in a configuration file or when SNMP is used.

The **no** form of this command removes all route policy names from the export list.

Default no export — BGP advertises routes from other BGP routes but does not advertise any routes from other protocols unless directed by an export policy.

Parameters *policy* — A route policy statement name.

family

Syntax **family** [**ipv4**] [**ipv6**] [**mcast-ipv4**] [**flow-ipv6**] [**flow-ipv4**]
no family

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command specifies the address families to be negotiated with one or more multi-protocol BGP peers of the VPRN.

The **no** form of the command removes the specified address family from the associated BGP sessions.

Default ipv4

Parameters *ipv4* — Provisions IPv4 support.

ipv6 — Provisions IPv6 support.

mcast-ipv4 — Provisions Multicast IPv4 support.

[flow-ipv6] — Exchanges IPv4 flowspec routes belonging to AFI 2 and SAFI 133.

[flow-ipv4] — Specifies to use an address of variable size consisting of 1 or 2-byte NLRI(Network Layer Reachability Information) length followed by a variable length NLRI value.

flowspec-validate

Syntax **flowspec-validate**
no flowspec-validate

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables/disables validation of received flowspec routes. A flow route with a destination prefix subcomponent received from a particular peer is considered valid if and only if that peer also advertised the best unicast route to the destination prefix and any of its more-specific components. If validation is enabled and a flowspec route is not valid, it is not eligible for import into the RIB, it is not used for filtering, and it is not propagated to other flowspec peers.

The **no** form of the command disables the validation procedure.

Default no flowspec-validate

group

Syntax **group** *name* [**dynamic-peer**]

no group

Context config>service>vprn>bgp

Description This command creates a context to configure a BGP peer group.

The **no** form of the command deletes the specified peer group and all configurations associated with the peer group. The group must be shutdown before it can be deleted.

Default None — No peer groups are defined.

Parameters *name* — The peer group name. Allowed values is a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

dynamic-peer — This flag designates that the given BGP group will be used by BGP peers created dynamically based on subscriber-hosts pointing to corresponding BGP peering policy. There can be only one BGP group with this flag set in any given VPRN. No bBGP neighbous can be manually configured in a BGP group with this flag set.

Default disabled

neighbor

Syntax [**no**] **neighbor** *ip-address*

Context config>service>vprn>bgp>group

Description This command creates a BGP peer/neighbor instance within the context of the BGP group.

This command can be issued repeatedly to create multiple peers and their associated configuration.

The **no** form of the command is used to remove the specified neighbor and the entire configuration associated with the neighbor. The neighbor must be administratively **shutdown** before attempting to delete it. If the neighbor is not shutdown, the command will not result in any action except a warning message on the console indicating that neighbor is still administratively up.

Default none — No neighbors are defined.

Parameters *ip-address* — The IP address of the BGP peer router in dotted decimal notation.

Values

ipv4-address :	a.b.c.d
ipv6-address :	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface: 32 chars maximum, mandatory for link local addresses

family

Syntax **family** [**ipv4**] [**ipv6**] [**mcast-ipv4**]
no family

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command specifies the address family or families to be supported over BGP peerings in the base router. This command is additive so issuing the **family** command adds the specified address family to the list.

The **no** form of the command removes the specified address family from the associated BGP peerings. If an address family is not specified, then reset the supported address family back to the default.

Default ipv4

Parameters **ipv4 —** Provisions support for IPv4 routing information.

ipv6 — Exchange IPv6 routing information.

mcast-ipv4 — Provisions Multicast IPv4 support.

hold-time

Syntax **hold-time** *seconds* [**min** *seconds2*]
no hold-time

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the BGP hold time, expressed in seconds.

The BGP hold time specifies the maximum time BGP waits between successive messages (either keepalive or update) from its peer, before closing the connection. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

Even though the router OS implementation allows setting the **keepalive** time separately, the configured **keepalive** timer is overridden by the **hold-time** value under the following circumstances:

1. If the specified hold-time is less than the configured **keepalive** time, then the operational **keepalive** time is set to a third of the **hold-time**; the configured **keepalive** time is not changed.
2. If the **hold-time** is set to zero, then the operational value of the **keepalive** time is set to zero; the configured **keepalive** time is not changed. This means that the connection with the peer is up permanently and no **keepalive** packets are sent to the peer.

The **no** form of the command used at the global level reverts to the default value.
The **no** form of the command used at the group level reverts to the value defined at the global level.
The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default 90 seconds

Parameters *seconds* — The hold-time, in seconds, expressed as a decimal integer. A value of 0 indicates the connection to the peer is up permanently.

Values 0, 3 — 65535

seconds2 — The minimum hold-time that will be accepted for the session. If the peer proposes a hold-time lower than this value the session attempt will be rejected.

ibgp-multipath

Syntax [**no**] **ibgp-multipath**

Context config>service>vprn>bgp

Description This command defines the type of IBGP multipath to use when adding BGP routes to the route table if the route resolving the BGP nexthop offers multiple nexthops.

The **no** form of the command disables the IBGP multipath load balancing feature.

Default none

import

Syntax **import** *policy* [*policy*...]
no import

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command specifies the import policies to be used to control routes advertised to BGP neighbors. Route policies are configured in the **config>router>policy-options** context. When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of five (5) policy names can be specified. The first policy that matches is applied.

The **no** form of this command removes all route policy names from the import list.

Default no import — BGP accepts all routes from configured BGP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

Parameters *policy* — A route policy statement name.

keepalive

Syntax **keepalive** *seconds*
no keepalive

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the BGP keepalive timer. A keepalive message is sent every time this timer expires. The *seconds* parameter can be set at three levels: global level (applies to all peers), group

level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **keepalive** value is generally one-third of the **hold-time** interval. Even though the OS implementation allows the **keepalive** value and the **hold-time** interval to be independently set, under the following circumstances, the configured **keepalive** value is overridden by the **hold-time** value:

If the specified **keepalive** value is greater than the configured **hold-time**, then the specified value is ignored, and the **keepalive** is set to one third of the current **hold-time** value.

If the specified **hold-time** interval is less than the configured **keepalive** value, then the **keepalive** value is reset to one third of the specified **hold-time** interval.

If the **hold-time** interval is set to zero, then the configured value of the **keepalive** value is ignored. This means that the connection with the peer is up permanently and no **keepalive** packets are sent to the peer.

The **no** form of the command used at the global level reverts to the default value.
The **no** form of the command used at the group level reverts to the value defined at the global level.
The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default 30 seconds

Parameters *seconds* — The keepalive timer in seconds, expressed as a decimal integer.

Values 0 — 21845

local-address

Syntax **local-address** *ip-address*
no local-address

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description Configures the local IP address used by the group or neighbor when communicating with BGP peers.

Outgoing connections use the **local-address** as the source of the TCP connection when initiating connections with a peer.

When a local address is not specified, the 7750 SR OS uses the system IP address when communicating with IBGP peers and uses the interface address for directly connected EBGP peers. This command is used at the neighbor level to revert to the value defined under the group level.

The **no** form of the command removes the configured local-address for BGP.
The **no** form of the command used at the group level reverts to the value defined at the global level.
The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default **no local-address** — The router ID is used when communicating with IBGP peers and the interface address is used for directly connected EBGP peers.

ip-address — The local address expressed in dotted decimal notation. Allowed values are a valid routable IP address on the router, either an interface or system IP address.

local-as

Syntax **local-as** *as-number* [**private**] [**no-prepend-global-as**]
no local-as

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures a BGP virtual autonomous system (AS) number.

In addition to the global AS number configured for BGP in the config>router>autonomous-system context, a virtual (local) AS number can be configured to support various AS number migration scenarios.The local AS number is added to the to the beginning the as-path attribute ahead of the router's AS number.

This configuration parameter can be set at three levels: global level (applies to all EBGP peers), group level (applies to all EBGP peers in peer-group) or neighbor level (only applies to EBGP specified peer). Thus, by specifying this at each neighbor level, it is possible to have a separate local-as per EBGP session. The local-as command is not supported for IBGP sessions. When the optional **private** keyword is specified in the command the local-as number is not added to inbound routes from the EBGP peer that has **local-as** in effect.

When a command is entered multiple times for the same AS, the last command entered is used in the configuration. The **private** attribute can be added or removed dynamically by reissuing the command.

Changing the local AS at the global level in an active BGP instance causes the BGP instance to restart with the new local AS number. Changing the local AS at the global level in an active BGP instance causes BGP to re-establish the peer relationships with all peers in the group with the new local AS number. Changing the local AS at the neighbor level in an active BGP instance causes BGP to re-establish the peer relationship with the new local AS number.

This is an optional command and can be used in the following circumstance:

Provider router P is moved from AS1 to AS2. The customer router that is connected to P, however, is configured to belong to AS1. To avoid reconfiguring the customer router, the **local-as** value on router P can be set to AS1. Thus, router P adds AS1 to the as-path message for routes it advertises to the customer router.

The **no** form of the command used at the global level will remove any virtual AS number configured. The **no** form of the command used at the group level reverts to the value defined at the global level. The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default no local-as

Parameters *as-number* — The virtual autonomous system number, expressed as a decimal integer.

Values 1 — 65535

private — Specifies the local-as is hidden in paths learned from the peering.

no-prepend-global-as — Specifies that the global-as is hidden in paths announced to the EBGP peer.

local-preference

Syntax **local-preference** *local-preference*
no local-preference

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables setting the BGP local-preference attribute in incoming routes if not specified and configures the default value for the attribute. This value is used if the BGP route arrives from a BGP peer without the **local-preference** integer set.

The specified value can be overridden by any value set via a route policy. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of the command at the global level specifies that incoming routes with local-preference set are not overridden and routes arriving without local-preference set are interpreted as if the route had local-preference value of 100.

The **no** form of the command used at the group level reverts to the value defined at the global level.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default **no local-preference** — Does not override the local-preference value set in arriving routes and analyze routes without local preference with value of 100.

Parameters *local-preference* — The local preference value to be used as the override value, expressed as a decimal integer.

Values 0 — 4294967295

loop-detect

Syntax **loop-detect** {**drop-peer** | **discard-route** | **ignore-loop**| **off**}
no loop-detect

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures how the BGP peer session handles loop detection in the AS path.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

Note that dynamic configuration changes of **loop-detect** are not recognized.

The **no** form of the command used at the global level reverts to default, which is **loop-detect ignore-loop**.

The **no** form of the command used at the group level reverts to the value defined at the global level.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default loop-detect ignore-loop

Parameters **drop-peer —** Sends a notification to the remote peer and drops the session.

discard-route — Discards routes received with loops in the AS path.

ignore-loop — Ignores routes with loops in the AS path but maintains peering.

off — Disables loop detection.

med-out

Syntax **med-out** {**number | igp-cost**}
no med-out

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables advertising the Multi-Exit Discriminator (MED) and assigns the value used for the path attribute for the MED advertised to BGP peers if the MED is not already set.

The specified value can be overridden by any value set via a route policy.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of the command used at the global level reverts to default where the MED is not advertised.

The **no** form of the command used at the group level reverts to the value defined at the global level.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default no med-out

Parameters *number* — The MED path attribute value, expressed as a decimal integer.

Values 0 — 4294967295

igp-cost — The MED is set to the IGP cost of the given IP prefix.

min-as-origination

Syntax **min-as-origination** *seconds*
no min-as-origination

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the minimum interval, in seconds, at which a path attribute, originated by the local router, can be advertised to a peer.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of the command used at the global level reverts to default.

The **no** form of the command used at the group level reverts to the value defined at the global level.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default 15 seconds

Parameters *seconds* — The minimum path attribute advertising interval in seconds, expressed as a decimal integer.

Values 2 — 255

min-route-advertisement

Syntax **min-route-advertisement** *seconds*
no min-route-advertisement

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the minimum interval, in seconds, at which a prefix can be advertised to a peer.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of the command reverts to default values.

Default 30 seconds

Parameters *seconds* — The minimum route advertising interval, in seconds, expressed as a decimal integer.

Values 1— 255

multihop

Syntax **multihop** *ttl-value*
no multihop

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the time to live (TTL) value entered in the IP header of packets sent to an EBGP peer multiple hops away.

This parameter is meaningful only when configuring EBGP peers. It is ignored if set for an IBGP peer.

The **no** form of the command is used to convey to the BGP instance that the EBGP peers are directly connected.
The **no** form of the command reverts to default values.

Default **1** — EBGP peers are directly connected.

64 — IBGP

Parameters *ttl-value* — The TTL value, expressed as a decimal integer.

Values 1 — 255

multipath

Syntax **multipath** *max-paths* [**eibgp**]
no multipath

Context config>service>vprn>bgp

Description This command enables BGP multipath.

When multipath is enabled BGP load shares traffic across multiple links. Multipath can be configured to load share traffic across a maximum of 16 routes. If the equal cost routes available are more than the configured value, then routes with the lowest next-hop IP address value are chosen.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

Multipath is effectively disabled if the value is set to one. When multipath is disabled, and multiple equal cost routes are available, the route with the lowest next-hop IP address will be used.

The **no** form of the command used at the global level reverts to default values.

Default **no multipath** — Multipath disabled.

Parameters *integer* — The number of equal cost routes to use for multipath routing. If more equal cost routes exist than the configured value, routes with the lowest next-hop value are chosen. Setting this value to 1 disables multipath.

Values 1 — 16

eibgp — Enables EIBGP load balancing so that routes with both MP-BGP and IPv4 next-hops can be used simultaneously. Enabling this option will disable the nexthop type (MP-BGP or IPv4 and also the next-hop metric comparison).

next-hop-resolution

Syntax **next-hop-resolution**

Context config>service>vprn>bgp

Description This command enables the context to configure next-hop resolution parameters.

next-hop-self

Syntax [**no**] **next-hop-self**

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the group or neighbor to always set the NEXTHOP path attribute to its own physical interface when advertising to a peer.

This is primarily used to avoid third-party route advertisements when connected to a multi-access network.

The **no** form of the command used at the group level allows third-party route advertisements in a multi-access network.
The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default **no next-hop-self** — Third-party route advertisements are allowed.

passive

Syntax [**no**] **passive**

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables passive mode for the BGP group or neighbor.

When in passive mode, BGP will not attempt to actively connect to the configured BGP peers but responds only when it receives a connect open request from the peer.

The **no** form of the command used at the group level disables passive mode where BGP actively attempts to connect to its peers.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default **no passive** — BGP will actively try to connect to all the configured peers.

peer-as

Syntax **peer-as** *as-number*

Context config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Description This command configures the autonomous system number for the remote peer. The peer AS number must be configured for each configured peer.

For EBGP peers, the peer AS number configured must be different from the autonomous system number configured for this router under the global level since the peer will be in a different autonomous system than this router

For IBGP peers, the peer AS number must be the same as the autonomous system number of this router configured under the global level.

This is a required command for each configured peer. This may be configured under the group level for all neighbors in a particular group.

Default No AS numbers are defined.

Parameters *as-number* — The autonomous system number, expressed as a decimal integer.

Values 1 — 65535

policy

Syntax **policy** *policy-name*
no policy

Context config>service>vprn>bgp>next-hop-res

Description This command specifies the name of a policy statement to use with the BGP next-hop resolution process. The policy controls which IP routes in RTM are eligible to resolve the BGP next-hop addresses of IPv4 and IPv6 routes. The policy has no effect on the resolution of BGP next-hops to MPLS tunnels. If a BGP next-hop of an IPv4 or IPv6 route R is resolved in RTM and the longest matching route for the next-hop address is an IP route N that is rejected by the policy then route R is unresolved; if the route N is accepted by the policy then it becomes the resolving route for R.

The default next-hop resolution policy (when the **no policy** command is configured) is to use the longest matching active route in RTM that is not a BGP route (unless **use-bgp-routes** is configured), an aggregate route or a subscriber management route.

Default no policy

Parameters *policy-name* — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>pol¬icy-options** context.

peer-tracking-policy

Syntax **peer-tracking-policy policy-name**
no peer-tracking-policy

Context config>router>bgp
config>service>vprn>bgp

Description This command specifies the name of a policy statement to use with the BGP peer-tracking function on the BGP sessions where this is enabled. The policy controls which IP routes in RTM are eligible to indicate reachability of IPv4 and IPv6 BGP neighbor addresses. If the longest matching route in RTM for a BGP neighbor address is an IP route that is rejected by the policy, or it is a BGP route accepted by the policy, or if there is no matching route, the neighbor is considered unreachable and BGP tears down the peering session and holds it in the idle state until a valid route is once again available and accepted by the policy.

The default peer-tracking policy (when the no peer-tracking-policy command is configured) is to use the longest matching active route in RTM that is not an LDP shortcut route or an aggregate route.

Default no peer-tracking-policy

Parameters *policy-name* — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>pol¬icy-options** context.

preference

Syntax [**no**] **preference** *preference*

Context config>service>vprn>bgp
config>service>vprn>bgp>group

Description This command configures the route preference for routes learned from the configured peer(s).

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The lower the preference the higher the chance of the route being the active route. The OS assigns BGP routes highest default preference compared to routes that are direct, static or learned via MPLS or OSPF.

The **no** form of the command used at the global level reverts to default value.

The **no** form of the command used at the group level reverts to the value defined at the global level.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default 170

Parameters *preference* — The route preference, expressed as a decimal integer.

Values 1 — 255

prefix-limit

Syntax **prefix-limit** *limit* [**log-only**] [**threshold** *percent*] [**idle-timeout** {*minutes* | **forever**}]
no prefix-limit

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command configures the maximum number of routes BGP can learn from a peer.

When the number of routes reaches a certain percentage (default is 90% of this limit), an SNMP trap is sent. When the limit is exceeded, the BGP peering is dropped and disabled.

The **no** form of the command removes the **prefix-limit**.

Default forever

Parameters **log-only —** Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, the BGP peering is not dropped.

percent — The threshold value (as a percentage) that triggers a warning message to be sent.

limit — The number of routes that can be learned from a peer expressed as a decimal integer.

Values 1 — 4294967295

minutes — Specifies duration in minutes before re-establishing a session.

Values 1 — 1024

forever — Specifies that the session is reestablished only after **clear router bgp** command is executed.

rapid-update

Syntax **rapid-update** {[**l2-vpn**] [**mvpn-ipv4**]}
no rapid-update {[**l2-vpn**] [**mvpn-ipv4**]}

Context config>service>vprn>bgp

Description This command enables and disables BGP rapid update for specified address-families. When no parameter is given for the no rapid-update statement, rapid update is disabled for all address-families.

Default no rapid-update

rapid-withdrawal

Syntax [**no**] **rapid-withdrawal**

Context config>service>vprn>bgp

Description This command disables the delay (Minimum Route Advertisement) on sending BGP withdrawals. Normal route withdrawals may be delayed up to the mininum route advertisement to allow for efficient packing of BGP updates.

The **no** form of the command removes this command from the configuration and returns withdrawal processing to the normal behavior.

Default no rapid-withdrawal

remove-private

Syntax [no] **remove-private**

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command allows private AS numbers to be removed from the AS path before advertising them to BGP peers.

When the **remove-private** parameter is set at the global level, it applies to all peers regardless of group or neighbor configuration. When the parameter is set at the group level, it applies to all peers in the group regardless of the neighbor configuration.

The OS software recognizes the set of AS numbers that are defined by IANA as private. These are AS numbers in the range 64512 through 65535, inclusive.

The **no** form of the command used at the global level reverts to default value. The **no** form of the command used at the group level reverts to the value defined at the global level. The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default **no remove-private** — Private AS numbers will be included in the AS path attribute.

split-horizon

Syntax **split-horizon**
no split-horizon

Context config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command enables the use of split-horizon. When applied globally, to a group, or a specific peer, split-horizon prevents routes from being reflected back to a peer that sends the best route. It applies to routes of all address families and to any type of sending peer; confed-EBGP, EBGP and IBGP.

The configuration default is **no split-horizon**, meaning that no effort is taken to prevent a best route from being reflected back to the sending peer.

NOTE: Use of the **split-horizon** command may have a detrimental impact on peer and route scaling and therefore operators are encouraged to use it only when absolutely needed.

The **no** form of the command disables split horizon command which allows the lower level to inherit the setting from an upper level.

Default **no split-horizon**

type

Syntax **[no] type {internal | external}**

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command designates the BGP peer as type internal or external.

The type of **internal** indicates the peer is an IBGP peer while the type of external indicates that the peer is an EBGP peer.

By default, the OS derives the type of neighbor based on the local AS specified. If the local AS specified is the same as the AS of the router, the peer is considered **internal**. If the local AS is different, then the peer is considered **external**.

The **no** form of the command used at the group level reverts to the default value.
The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

Default **no type** — Type of neighbor is derived on the local AS specified.

Parameters **internal —** Configures the peer as internal.

external — Configures the peer as external.

updated-error-handling

Syntax **[no] updated-error-handling**

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description This command controls whether SROS utilizes the new neighbor-complete bit when processing optional transitive path attributes and advertising them to the associated BGP neighbor.

This command also control if SROS utilizes the error handling mechanism for optional-transitive path attributes.

Default no updated-error-handling

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description Configure TTL security parameters for incoming packets.

Parameters *min-ttl-value* — Specify the minimum TTL value for an incoming BGP packet.

Values 1 — 255

Default 1

OSPF Commands

ospf

Syntax [**no**] **ospf**

Context config>service>vprn

Description This command enables access to the context to enable an OSPF protocol instance.

When an OSPF instance is created, the protocol is enabled. To start or suspend execution of the OSPF protocol without affecting the configuration, use the **no shutdown** command.

The **no** form of the command deletes the OSPF protocol instance removing all associated configuration parameters.

Default **no ospf** — The OSPF protocol is not enabled.

ospf3

Syntax **ospf3** [*instance-id*] [*router-id*]
[**no**] **ospf3** *instance-id*

Context config>service>vprn

Description This command creates an OSPFv3 routing instance and then enters the associated context to configure associated protocol parameters.

When an OSPFv3 instance is created, the protocol is enabled. To start or suspend execution of the OSPF.

The **no** form of the command deletes the OSPFv3 protocol instance, removing all associated configuration parameters.

Default **no default**

Parameters *instance-id* — Specify the instance ID for the OSPFv3 instance being created or modified. The instance ID must match the specified range based on the address family. For ipv6-unicast, the instance id must be between 0 and 31. For ipv4-unicast the instance id must be between 64-95.

Values 0 — 31: IPV6 unicast

Values 64—95: IPV4 unicast

area

Syntax [**no**] **area** *area-id*

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command creates the context to configure an OSPF area. An area is a collection of network segments within an AS that have been administratively grouped together. The area ID can be specified in dotted decimal notation or as a 32-bit decimal integer.

The **no** form of the command deletes the specified area from the configuration. Deleting the area also removes the OSPF configuration of all the interfaces, virtual-links, sham-links, and address-ranges etc., that are currently assigned to this area.

Default **no area** — No OSPF areas are defined.

Parameters *area-id* — The OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

Values 0.0.0.0 — 255.255.255.255 (dotted decimal)
0 — 4294967295 (decimal integer)

area-range

Syntax **area-range** *ip-prefix/prefix-length* [**advertise** | **not-advertise**]
no area-range *ip-prefixImask*
area-range *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**]
no area-range *ip-prefixImask*

Context config>service>vprn>ospf>area
ospf>service>vprn>nssa
config>service>vprn>ospf3>area

Description This command creates ranges of addresses on an Area Border Router (ABR) for the purpose of route summarization or suppression. When a range is created, the range is configured to be advertised or not advertised into other areas. Multiple range commands may be used to summarize or hide different ranges. In the case of overlapping ranges, the most specific range command applies.

ABRs send summary link advertisements to describe routes to other areas. To minimize the number of advertisements that are flooded, you can summarize a range of IP addresses and send reachability information about these addresses in an LSA.

The **no** form of the command deletes the range (non) advertisement.

Default **no area-range** — No range of addresses are defined.

Special Cases **NSSA Context —** In the NSSA context, the option specifies that the range applies to external routes (via type-7 LSAs) learned within the NSSA when the routes are advertised to other areas as type-5 LSAs.

Area Context — If this command is not entered under the NSSA context, the range applies to summary LSAs even if the area is an NSSA.

Parameters *ipv6-prefix/prefix-length* — The IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
- x [0..FFFF]H - d [0..255]D
prefix-length - [0..128]

mask — The subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

Values 0 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)

advertise | **not-advertise —** Specifies whether or not to advertise the summarized range of addresses into other areas. The **advertise** keyword indicates the range will be advertised, and the keyword **not-advertise** indicates the range will not be advertised.
The default is **advertise**.

blackhole-aggregate

Syntax [**no**] **blackhole-aggregate**

Context config>service>vprn>ospf>area
config>service>vprn>ospf3>area

Description This command installs a low priority blackhole route for the entire aggregate. Exisiting routes that make up the aggregate will have a higher priority and only the components of the range for which no route exists are blackholed.

It is possible that when performing area aggregation, addresses may be included in the range for which no actual route exists. This can cause routing loops. To avoid this problem configure the blackhole aggregate option.

The **no** form of this command removes this option.

Default blackhole-aggregate

interface

Syntax [**no**] **interface** *ip-int-name* [**secondary**]

Context config>service>vprn>ospf>area
config>service>vprn>ospf3>area

Description This command creates a context to configure an OSPF interface.

By default interfaces are not activated in any interior gateway protocol such as OSPF unless explicitly configured.

The **no** form of the command deletes the OSPF interface configuration for this interface. The **shutdown** command in the **config>router>ospf>interface** context can be used to disable an interface without removing the configuration for the interface.

Default **no interface** — No OSPF interfaces are defined.

Parameters *ip-int-name* — The IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service vprn interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

secondary — Allows multiple secondary adjacencies to be established over a single IP interface.

sham-link

Syntax **sham-link** *ip-int-name ip-address*

Context config>service>vprn>ospf>area

Description This command is similar to a virtual link with the exception that metric must be included in order to distinguish the cost between the MPLS-VPRN link and the backdoor.

Parameters *ip-int-name* — The local interface name used for the sham-link. This is a mandatory parameter and interface names must be unique within the group of defined IP interfaces for **config>router>interface**, **config>service>ies>interface** and **config>service>vprn>interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters, the entire string must be enclosed within double quotes. If the IP interface name does not exist or does not have an IP address configured, an error message will be returned.

ip-address — The IP address of the SHAM-link neighbor in IP address dotted decimal notation. This parameter is the remote peer of the sham link's IP address used to set up the SHAM link. This is a mandatory parameter and must be a valid IP address.

advertise-subnet

Syntax [**no**] **advertise-subnet**

Context config>service>vprn>ospf>area>if

Description This command enables advertising point-to-point interfaces as subnet routes (network number and mask). When disabled, point-to-point interfaces are advertised as host routes.

Note that this command is not supported in the OSPF3 context.

The **no** form of the command disables advertising point-to-point interfaces as subnet routes meaning they are advertised as host routes.

Default **advertise-subnet** — Advertises point-to-point interfaces as subnet routes.

authentication

Syntax **authentication bidirectional** *sa-name*
authentication inbound *sa-name* **outbound** *sa-name*
no authentication

Context config>service>vprn>ospf3>area>if

Description This command configures OPSFv3 confidentiality authentication.

The no form of the command removes the SA name from the configuration.

Parameters **bidirectional** *sa-name* — Specifies the IPSec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

inbound *sa-name* — Specifies the IPSec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

outbound *sa-name* — Specifies the IPSec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
no authentication-key

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf>area>sham-link

Description This command configures the password used by the OSPF interface or virtual-link to send and receive OSPF protocol packets on the interface when simple password authentication is configured.

Note that this command is not valid in the OSPF3 context.

All neighboring routers must use the same type of authentication and password for proper protocol communication. If the **authentication-type** is configured as password, then this key must be configured.

By default, no authentication key is configured.

Note that this command is not supported in the OSPF context.

The **no** form of the command removes the authentication key.

Default **no authentication-key** — No authentication key is defined.

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 8 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

authentication-type

Syntax **authentication-type** {**password** | **message-digest**}
no authentication-type

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link

Description This command enables authentication and specifies the type of authentication to be used on the OSPF interface, virtual-link, and sham-link.

Note that this command is not valid in the OSPF3 context.

Both simple **password** and **message-digest** authentication are supported.

By default, authentication is not enabled on an interface.

The **no** form of the command disables authentication on the interface.

Note that this command is not supported in the OSPF context.

Default **no authentication** — No authentication is enabled on an interface.

Parameters **password —** This keyword enables simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple **password** authentication is enabled.

message-digest — This keyword enables message digest MD5 authentication in accordance with RFC1321. If this option is configured, then at least one message-digest-key must be configured.

bfd-enable

Syntax **bfd-enable** [**remain-down-on-failure**]
no bfd-enable

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if

Description

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

Default **no bfd-enable**

Parameters **remain-down-on-failure —** Forces adjacency down on BFD failure.

dead-interval

Syntax **dead-interval** *seconds*
no dead-interval

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf3>area>if
config>service>vprn>ospf3>area>virtual-link
config>service>vprn>ospf>area>sham-link

Description This command configures the time, in seconds, that OSPF waits before declaring a neighbor router down. If no hello packets are received from a neighbor for the duration of the dead interval, the router is assumed to be down. The minimum interval must be two times the hello interval.

The **no** form of the command reverts to the default value.

Default **40**

Special Cases **OSPF Interface —** If the **dead-interval** configured applies to an interface, then all nodes on the subnet must have the same dead interval.

Virtual Link — If the **dead-interval** configured applies to a virtual link, then the interval on both termination points of the virtual link must have the same dead interval.

Sham-link — If the **dead-interval** configured applies to a sham-link, then the interval on both endpoints of the sham-link must have the same dead interval**.**

Parameters *seconds* — The dead interval expressed as a decimal integer.

Values 2 — 2147483647 seconds

graceful-restart

Syntax [**no**] **graceful-restart**

Context config>service>vprn>ospf

Description This command enables or disables graceful-restart for VPRN OSPF.

This command is not available for OSPF3.

helper-disable

Syntax **helper-disable**

Context config>service>vprn>ospf>graceful-restart

Description This command disables the helper support for graceful restart.

When **graceful-restart** is enabled, the router can be a helper (meaning that the router is helping a neighbor to restart) or be a restarting router or both. The 7750 SR OS supports only helper mode. This facilitates the graceful restart of neighbors but will not act as a restarting router (meaning that the

7750 SR OS will not help the neighbors to restart).

This command is not available for OSPF3.

The **no helper-disable** command enables helper support and is the default when graceful-restart is enabled.

Default **disabled**

ignore-dn-bit

Syntax [**no**] **ignore-dn-bit**

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command specifies whether to suppress the setting of the DN bit for OSPF or OSPF3 LSA packets generated by this instance of OSPF or OSPF3 on the router.

The **no** form of the command enables the OSPF or OSPF3 router to follow the normal proceedure to determine whether to set the DN bit.

Default no ignore-dn-bit

import

Syntax **import** *policy-name* [*policy-name*...(up to 5 max)]
no import

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command applies one or more (up to 5) route polices as OSPF import policies. When a prefix received in an OSPF LSA is accepted by an entry in an OSPF import policy it is installed in the routing table if it is the most preferred route to the destination. When a prefix received in an OSPF LSA is rejected by an entry in an OSPF import policy it is not installed in the routing table, even if it has the lowest preference value among all the routes to that destination. The flooding of LSAs is unaffected by OSPF import policy actions.

Default If an OSPF route has the lowest preference value among all routes to a destination it is installed in the routing table.

Parameters *policy-name* — The import route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

hello-interval

Syntax **hello-interval** *seconds*
no hello-interval

Context config>service>vprn>ospf>area>*if*
config>service>vprn>ospf3>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf3>area>virtual-link
config>service>vprn>ospf>area>sham-link

Description This command configures the interval between OSPF hellos issued on the interface, virtual link, or sham-link.

The hello interval, in combination with the dead-interval, is used to establish and maintain the adjacency. Use this parameter to edit the frequency that hello packets are sent.

Reducing the interval, in combination with an appropriate reduction in the associated **dead-interval**, allows for faster detection of link and/or router failures at the cost of higher processing costs.

The **no** form of this command reverts to the default value.

Default **hello-interval 10** — A 10-second hello interval.

Special Cases **OSPF Interface —** If the **hello-interval** configured applies to an interface, then all nodes on the subnet must have the same hello interval.

Virtual Link — If the **hello-interval** configured applies to a virtual link, then the interval on both termination points of the virtual link must have the same hello interval.

Sham Link — If the hello-interval configured applies to a sham-link, then the interval on both endpoints of the sham-link must have the same hello interval

Parameters *seconds* — The hello interval in seconds expressed as a decimal integer.

Values 1 — 65535

interface-type

Syntax **interface-type** {**broadcast** | **point-to-point**}
no interface-type

Context config>service>vprn>ospf>area>*if*
config>service>vprn>ospf3>area>if

Description This command configures the interface type to be either broadcast or point-to-point.

Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the broadcast adjacency maintenance overhead if the Ethernet link provided the link is used as a point-to-point.

If the interface type is not known at the time the interface is added to OSPF and subsequently the IP interface is bound (or moved) to a different interface type, this command must be entered manually.

The **no** form of the command reverts to the default value.

Default **point-to-point** — If the physical interface is SONET.

broadcast — If the physical interface is Ethernet or unknown.

Special Cases **Virtual-Link —** A virtual link is always regarded as a point-to-point interface and not configurable.

Parameters **broadcast —** Configures the interface to maintain this link as a broadcast network. To significantly improve adjacency forming and network convergence, a network should be configured as point-to-point if only two routers are connected, even if the network is a broadcast media such as Ethernet.

point-to-point — Configures the interface to maintain this link as a point-to-point link.

loopfree-alternate-exclude

Syntax [**no**] **loopfree-alternate-exclude**

Context configure>service>vprn>ospf>area
configure>service>vprn>ospf3>area
configure>service>vprn>ospf>area>interface
configure>service>vprn>ospf3>area>interface

Description This command instructs IGP to not include a specific interface or all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

When an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When it is excluded from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

The **no** form of this command re-instates the default value for this command.

Default no loopfree-alternate-exclude.

lsa-filter-out

Syntax **lsa-filter-out [all | except-own-rtrlsa | except-own-rtrlsa-and-defaults]**
no lsa-filter-out

Context config>router>ospf>area>interface
config>router>ospf3>area>interface
config>service>vprn>ospf>area>interface
config>service>vprn>ospf3>area>interface

Description This command enables filtering of outgoing OSPF LSAs on the selected OSPFv2 or OSPFv3 interface. Three filtering options are provided:

- Do not flood any LSAs out the interface. This option is suitable if the neighbor is simply-connected and has a statically configured default route with the address of this interface as next-hop.

- Flood the router's own router-LSA out the interface and suppress all other flooded LSAs. This option is suitable if the neighbor is simply-connected and has a statically configured default route with a loopback or system interface address (contained in the router-LSA) as next-hop.
- Flood the router's own router-LSA and all self-generated type-3, type-5 and type-7 LSAs advertising a default route (0/0) out the interface; suppress all other flooded LSAs. This option is suitable if the neighbor is simply-connected and does not have a statically configured default route.

The **no** form of this command disables OSPF LSA filtering (normal operation).

Default no lsa-filter-out

multicast-import

Syntax [**no**] **multicast-import**

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command enables the submission of routes into the multicast Route Table Manager (RTM) by OSPF.

The **no** form of the command disables the submission of routes into the multicast RTM.

Default **no multicast-import**

message-digest-key

Syntax **message-digest-key** *keyid* **md5** [*key* | *hash-key*] [**hash**]
no message-digest-key *keyid*

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf>area>sham-link

Description This command configures a message digest key when MD5 authentication is enabled on the interface, virtual-link or sham-link. Multiple message digest keys can be configured.

Note that this command is not valid in the OSPF3 context.

The **no** form of the command removes the message digest key identified by the *key-id*.

Default No message digest keys are defined.

Parameters **keyid —** The *keyid* is expressed as a decimal integer.

Values 1 — 255

md5 *key* **—** The MD5 key. The *key* can be any alphanumeric string up to 16 characters in length.

md5 *hash-key* — The MD5 hash key. The key can be any combination of ASCII characters up to 32 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

metric

Syntax **metric** *metric*
no metric

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if
config>service>vprn>ospf>area>sham-link

Description This command configures an explicit route cost metric for the OSPF interface that overrides the metrics calculated based on the speed of the underlying link.

The **no** form of the command deletes the manually configured interface metric, so the interface uses the computed metric based on the **reference-bandwidth** command setting and the speed of the underlying link.

Default **no metric** — The metric is based on **reference-bandwidth** setting and the link speed.

Parameters *metric* — The metric to be applied to the interface expressed as a decimal integer.

Values 1 — 65535

mtu

Syntax **mtu** *bytes*
no mtu

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if

Description This command configures the OSPF packet size used on this interface. If this parameter is not configured OSPF derives the MTU value from the MTU configured (default or explicitly) in the following contexts:

config>port>ethernet
config>port>sonet-sdh>path
config>port>tdm>t3-e3
config>port>tdm>t1-e1>channel-group

If this parameter is configured, the smaller value between the value configured here and the MTU configured (default or explicitly) in an above-mentioned context is used.

To determine the actual packet size add 14 bytes for an Ethernet packet and 18 bytes for a tagged Ethernet packet to the size of the OSPF (IP) packet MTU configured in this command.

Use the **no** form of this command to revert to default.

Default **no mtu** — Uses the value derived from the MTU configured in the **config>port** context.

Parameters *bytes* — The MTU to be used by OSPF for this logical interface in bytes.

Values 512 — 9198 (9212-14) (Depends on the physical media)

passive

Syntax [**no**] **passive**

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if

Description This command adds the passive property to the OSPF interface where passive interfaces are advertised as OSPF interfaces but do not run the OSPF protocol.

By default, only interface addresses that are configured for OSPF will be advertised as OSPF interfaces. The **passive** parameter allows an interface to be advertised as an OSPF interface without running the OSPF protocol.

While in passive mode, the interface will ignore ingress OSPF protocol packets and not transmit any OSPF protocol packets.

The **no** form of the command removes the passive property from the OSPF interface.

Default Service interfaces defined in **config>router>service-prefix** are passive.

All other interfaces are not passive.

priority

Syntax **priority** *number*
no priority

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if

Description This command configures the priority of the OSPF interface that is used an election of the designated router on on the subnet.

This parameter is only used if the interface is of type broadcast. The router with the highest priority interface becomes the designated router. A router with priority 0 is not eligible to be Designated Router or Backup Designated Router.

The **no** form of the command reverts the interface priority to the default value.

Default **priority 1**

Parameters *number* — The interface priority expressed as a decimal integer. A value of 0 indicates the router is not eligible to be the Designated Router of Backup Designated Router on the interface subnet.

Values 0 — 255

retransmit-interval

Syntax **retransmit-interval** *seconds*
no retransmit-interval

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf3>area>if
config>service>vprn>ospf3>area>virtual-link
config>service>vprn>ospf>area>sham-link

Description This command specifies the length of time, in seconds, that OSPF will wait before retransmitting an unacknowledged link state advertisement (LSA) to an OSPF neighbor.

The value should be longer than the expected round trip delay between any two routers on the attached network. Once the retransmit-interval expires and no acknowledgement has been received, the LSA will be retransmitted.

The **no** form of this command reverts to the default interval.

Default **retransmit-interval 5**

Parameters *seconds* — The retransmit interval in seconds expressed as a decimal integer.

Values 1 — 3600

transit-delay

Syntax **transit-delay** *seconds*
no transit-delay

Context config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf3>area>virtual-link
config>service>vprn>ospf>area>sham-link

Description This command configures the estimated time, in seconds, that it takes to transmit a link state advertisement (LSA) on the interface or virtual link or sham-link.

The **no** form of this command reverts to the default delay time.

Default **transit-delay 1**

Parameters *seconds* — The transit delay in seconds expressed as a decimal integer.

Values 0 — 3600

key-rollover-interval

Syntax **key-rollover-interval** *key-rollover-interval*

Context config>service>vprn>ospf3>area

Description This command configures the key rollover interval.

The **no** form of the command reverts to the default.

Default 10

Parameters *key-rollover-interval* — Specifies the time, in seconds, after which a key rollover will start.

Values 10 — 300

loopfree-alternate-exclude

Syntax [**no**] **loopfree-alternate-exclude**

Context config>service>vprn>ospf3>area

Description This command specifies whether or not the OSPF area should be excluded during LFA calculations. When enabled, the OSPF area is excluded from LFA calculations. When disabled (the default), the OSPF area is included in LFA calculations.

The **no** form of the command includes the OSPF area in LFA calculations.

Default disabled

nssa

Syntax [**no**] **nssa**

Context config>service>vprn>ospf>area
config>service>vprn>ospf3>area

Description This command creates the context to configure an OSPF Not So Stubby Area (NSSA) and adds/removes the NSSA designation from the area.

NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is an NSSA has the capability to flood external routes that it learns throughout its area and via an ABR to the entire OSPF domain.

Existing virtual links of a non-stub or NSSA area will be removed when the designation is changed to NSSA or stub.

An area can be designated as stub or NSSA but never both at the same time.

By default, an area is not configured as an NSSA area.

The **no** form of the command removes the NSSA designation and configuration context from the area.

Default **no nssa** — The OSPF area is not an NSSA.

originate-default-route

Syntax **originate-default-route** [**type-7**]
no originate-default-route

Context config>service>vprn>ospf>area>nssa
config>service>vprn>ospf3>area>nssa

Description This command enables the generation of a default route and its LSA type (3 or 7) into a Not So Stubby Area (NSSA) by an NSSA Area Border Router (ABR)

When configuring an NSSA with no summaries, the ABR will inject a type 3 LSA default route into the NSSA area. Some older implementations expect a type 7 LSA default route.

The **no** form of the command disables origination of a default route.

Default **no originate-default-route** — A default route is not originated.

Parameters **type-7 —** Specifies a type 7 LSA should be used for the default route.

Configure this parameter to inject a type-7 LSA default route instead the type 3 LSA into the NSSA configured with no summaries.
To revert to a type 3 LSA, enter **originate-default-route** without the **type-7** parameter.

Default Type 3 LSA for the default route.

redistribute-external

Syntax [**no**] **redistribute-external**

Context config>service>vprn>ospf>area>nssa
config>service>vprn>ospf3>area>nssa

Description This command enables the redistribution of external routes into the Not So Stubby Area (NSSA) or an NSSA area border router (ABR) that is exporting the routes into non-NSSA areas.

NSSA or Not So Stubby Areas are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is that the NSSA has the capability to flood external routes that it learns (providing it is an ASBR) throughout its area and via an Area Border Router to the entire OSPF domain.

The **no** form of the command disables the default behavior to automatically redistribute external routes into the NSSA area from the NSSA ABR.

Default **redistribute-external** — External routes are redistributed into the NSSA.

summaries

Syntax [**no**] **summaries**

Context config>service>vprn>ospf>area>nssa
config>service>vprn>ospf>area>stub
config>service>vprn>ospf3>area>nssa

Description This command enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR). This parameter is particularly useful to reduce the size of the routing and Link State Database (LSDB) tables within the stub or nssa area. By default, summary route advertisements are sent into the stub area or NSSA.

The **no** form of the command disables sending summary route advertisements and, for stub areas, only the default route is advertised by the ABR.

Default **summaries** — Summary routes are advertised by the ABR into the stub area or NSSA.

stub

Syntax [**no**] **stub**

Context config>service>vprn>ospf>area
config>service>vprn>ospf3>area

Description This command enables access to the context to configure an OSPF stub area and adds/removes the stub designation from the area. External routing information is not flooded into stub areas. All routers in the stub area must be configured with the **stub** command. An OSPF area cannot be both an NSSA and a stub area. Existing virtual links of a non STUB or NSSA area will be removed when its designation is changed to NSSA or STUB.

By default, an area is not a stub area.

The **no** form of the command removes the stub designation and configuration context from the area.

Default **no stub** — The area is not configured as a stub area.

default-metric

Syntax **default-metric** *metric*
no default-metric

Context config>service>vprn>ospf>area>stub
config>service>vprn>ospf3>area>stub

Description This command configures the metric used by the area border router (ABR) for the default route into a stub area. The default metric should only be configured on an ABR of a stub area. An ABR generates a default route if the area is a **stub** area.

The **no** form of the command reverts to the default value.

Default default-metric 1

Parameters *metric* — The metric expressed as a decimal integer for the default route cost to be advertised into the stub area.

Values 1 — 16777215

virtual-link

Syntax [**no**] **virtual-link** *router-id* **transit-area** *area-id*

Context config>service>vprn>ospf>area
config>service>vprn>ospf3>area

Description This command configures a virtual link to connect area border routers to the backbone via a virtual link. The backbone area (area 0.0.0.0) must be contiguous and all other areas must be connected to the backbone area. If it is not practical to connect an area to the backbone (see area 0.0.0.2 in the picture below) then the area border routers (routers 1 and 2 in the picture below) must be connected via a virtual link. The two area border routers will form a point-to-point like adjacency across the transit area (area 0.0.0.1 in the picture below). A virtual link can only be configured while in the area 0.0.0.0 context.

The *router-id* specified in this command must be associated with the virtual neighbor. The transit area cannot be a stub area or a Not So Stubby Area (NSSA).

The **no** form of the command deletes the virtual link.

Default No virtual link is defined.

Parameters *router-id* — The router ID of the virtual neighbor in IP address dotted decimal notation.

transit-area *area-id* — The area-id specified identifies the transit area that links the backbone area with the area that has no physical connection with the backbone.

The OSPF backbone area, area 0.0.0.0, must be contiguous and all other areas must be connected to the backbone area. The backbone distributes routing information between areas. If it is not practical to connect an area to the backbone (see Area 0.0.0.5 in Figure 113) then the area border routers (such as routers Y and Z) must be connected via a virtual link. The two area border routers form a point-to-point-like adjacency across the transit area (see Area 0.0.0.4).

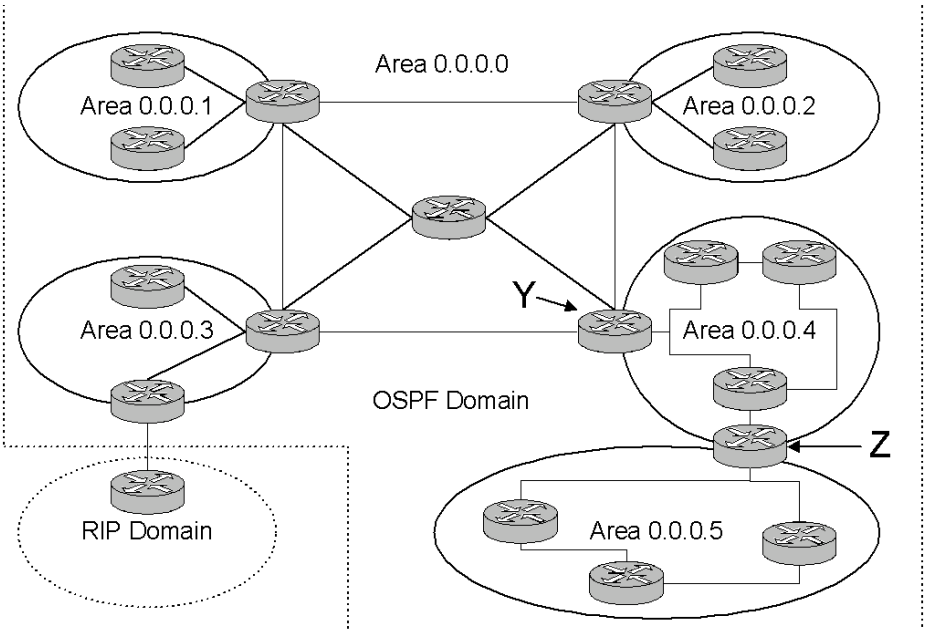

Figure 113: OSPF Areas

compatible-rfc1583

Syntax [**no**] **compatible-rfc1583**

Context config>service>vprn>ospf

Description This command enables OSPF summary and external route calculations in compliance with RFC1583 and earlier RFCs.

RFC1583 and earlier RFCs use a different method to calculate summary and external route costs. To avoid routing loops, all routers in an OSPF domain should perform the same calculation method.

Although it would be favorable to require all routers to run a more current compliancy level, this command allows the router to use obsolete methods of calculation.

This command is not supported in OSPF3.

The **no** form of the command enables the post-RFC1583 method of summary and external route calculation.

Default **compatible-rfc1583** — RFC1583 compliance is enabled.

export

Syntax **export** *policy-name* [*policy-name…*]
no export

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command associates export route policies to determine which routes are exported from the route table to OSPF. Export polices are only in effect if OSPF is configured as an ASBR.

If no export policy is specified, non-OSPF routes are not exported from the routing table manager to OSPF.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of the command removes all policies from the configuration.

Default **no export** — No export route policies specified.

Parameters *policy-name* — The export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

external-db-overflow

Syntax **external-db-overflow** *limit interval*
no external-db-overflow

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command enables limits on the number of non-default AS-external-LSA entries that can be stored in the LSDB and specifies a wait timer before processing these after the limit is exceeded.

The *limit* value specifies the maximum number of non-default AS-external-LSA entries that can be stored in the link-state database (LSDB). Placing a limit on the non-default AS-external-LSAs in the LSDB protects the router from receiving an excessive number of external routes that consume excessive memory or CPU resources. If the number of routes reach or exceed the *limit*, the table is in an overflow state. When in an overflow state, the router will not originate any new AS-external-LSAs. In fact, it withdraws all the self-originated non-default external LSAs.

The *interval* specifies the amount of time to wait after an overflow state before regenerating and processing non-default AS-external-LSAs. The waiting period acts like a dampening period preventing the router from continuously running Shortest Path First (SPF) calculations caused by the excessive number of non-default AS-external LSAs.

The **external-db-overflow** must be set identically on all routers attached to any regular OSPF area. OSPF stub areas and not-so-stubby areas (NSSAs) are excluded.

The **no** form of the command disables limiting the number of non-default AS-external-LSA entries.

Default **no external-db-overflow** — No limit on non-default AS-external-LSA entries.

Parameters *limit* — The maximum number of non-default AS-external-LSA entries that can be stored in the LSDB before going into an overflow state expressed as a decimal integer.

Values -1 — 2147483647

interval — The number of seconds after entering an overflow state before attempting to process non-default AS-external-LSAs expressed as a decimal integer.

Values 0 — 2147483647

external-preference

Syntax **external-preference** *preference*
no external-preference

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command configures the preference for OSPF external routes.

A route can be learned by the router from different protocols in which case the costs are not comparable; when this occurs the preference is used to decide which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the following table. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the **ecmp** in the config>router context.

The **no** form of the command reverts to the default value.

Default **external-preference 150** — OSPF external routes have a default preference of 150.

Parameters *preference* — The preference for external routes expressed as a decimal integer.

Route Type	Preference	Configurable
Direct attached	0	No
Static routes	5	Yes
OSPF internal	10	Yes[a]
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

a. Preference for OSPF internal routes is configured with the **preference** command.

Values 1 — 255

ignore-dn-bit

Syntax [**no**] **ignore-dn-bit**

Context config>service>vprn>ospf

Description This command specifies whether to ignore the DN bit for OSPF LSA packets for this instance of OSPF on the router. When enabled, the DN bit for OSPF LSA packets will be ignored. When disabled, the DN bit will not be ignored for OSPF LSA packets.

loopfree-alternate

Syntax [**no**] **loopfree-alternate**

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command enables Loop-Free Alternate (LFA) computation by SPF under the IS-IS routing protocol level, or under the OSPF routing protocol instance level.

When this command is enabled, it instructs the IGP SPF to attempt to pre-compute both a primary next-hop and an LFA next-hop for every learned prefix. IS-IS computes the primary SPF first and then computes the LFA SPF. The LFA backup next-hop is only available after the LFA SPF is completed. When found, the LFA next-hop is populated into the routing table along with the primary next-hop for the prefix.

The **no** form of this command disables the LFA computation by IGP SPF.

Default no loopfree-alternate

overload

Syntax **overload** [**timeout** *seconds*]
no overload

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command changes the overload state of the local router so that it appears to be overloaded. When overload is enabled, the router can participate in OSPF routing, but is not used for transit traffic. Traffic destined to directly attached interfaces continue to reach the router.

To put the IGP in an overload state enter a timeout value. The IGP will enter the overload state until the timeout timer expires or a **no overload** command is executed.

If the **overload** command is encountered during the execution of an **overload-on-boot** command then this command takes precedence. This could occur as a result of a saved configuration file where both parameters are saved. When the file is saved by the system the **overload-on-boot** command is saved after the **overload** command.

Use the **no** form of this command to return to the default. When the **no overload** command is executed, the overload state is terminated regardless the reason the protocol entered overload state.

Default no overload

Parameters **timeout** *seconds* — Specifies the number of seconds to reset overloading.

Values 60 —1800

Default 60

overload-include-stub

Syntax [**no**] **overload-include-stub**

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command is used to to determine if the OSPF stub networks should be advertised with a maximum metric value when the system goes into overload state for any reason. When enabled, the system uses the maximum metric value. When this command is enabled and the router is in overload, all stub interfaces, including loopback and system interfaces, will be advertised at the maximum metric.

Default no overload-include-stub

overload-on-boot

Syntax **overload-on-boot** [**timeout** *seconds*]
no overload

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description When the router is in an overload state, the router is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

- The timeout timer expires.
- A manual override of the current overload state is entered with the **no overload** command.

  The **no overload** command does not affect the **overload-on-boot** function.

The **no** form of the command removes the overload-on-boot functionality from the configuration.

Default no overload-on-boot

Parameters **timeout** *seconds* — Specifies the number of seconds to reset overloading.

Values 60 —1800

Default 60

preference

Syntax **preference** *preference*
no preference

Context config>service>vprn>ospf
config>service>vprn>ospf3

This command configures the preference for OSPF internal routes.

A route can be learned by the router from different protocols in which case the costs are not comparable, when this occurs the preference is used to decide to which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the following table. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the **ecmp** in the config>router context.

The **no** form of the command reverts to the default value.

Default **preference 10** — OSPF internal routes have a preference of 10.

Parameters *preference* — The preference for internal routes expressed as a decimal integer. Defaults for different route types are listed in the following table.

Route Type	Preference	Configurable
Direct attached	0	No
Static routes	5	Yes
OSPF internal	10	Yes[a]
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

a. Preference for OSPF internal routes is configured with the **preference** command.

Values 1 — 255

reference-bandwidth

Syntax **reference-bandwidth** *reference-bandwidth*
no reference-bandwidth

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command configures the reference bandwidth in kilobits per second (Kbps) that provides the reference for the default costing of interfaces based on their underlying link speed.

The default interface cost is calculated as follows:

cost = reference-bandwidth ÷ bandwidth

The default *reference-bandwidth* is 100,000,000 Kbps or 100 Gbps, so the default auto-cost metrics for various link speeds are as as follows:

- 10 Mbs link default cost of 10000
- 100 Mbs link default cost of 1000
- 1 Gbps link default cost of 100
- 10 Gbps link default cost of 10

The **reference-bandwidth** command assigns a default cost to the interface based on the interface speed. To override this default cost on a particular interface, use the **metric** *metric* command in the **config>router>ospf>area>interface** *ip-int-name* context.

The **no** form of the command reverts the reference-bandwidth to the default value.

Default **reference-bandwidth 100000000** — Reference bandwidth of 100 Gbps.

Parameters *reference-bandwidth* — The reference bandwidth in kilobits per second expressed as a decimal integer.

Values 1 — 1000000000

super-backbone

Syntax [**no**] **super-backbone**

Context config>service>vprn>ospf

Description This command specifies whether CE-PE functionality is required or not. The OSPF super backbone indicates the type of the LSA generated as a result of routes redistributed into OSPF. When enabled, the redistributed routes are injected as summary, external or NSSA LSAs. When disabled, the redistributed routes are injected as either external or NSSA LSAs only.

Default no super-backbone

suppress-dn-bit

Syntax [**no**] **suppress-dn-bit**

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command specifies whether to suppress the setting of the DN bit for OSPF LSA packets generated by this instance of OSPF on the router. When enabled, the DN bit for OSPF LSA packets generated by this instance of the OSPF router will not be set. When disabled, this instance of the OSPF router will follow the normal proceedure to determine whether to set the DN bit.

Default no suppress-dn-bit

timers

Syntax **timers**

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command enables the context that allows for the configuration of OSPF timers. Timers control the delay between receipt of a link state advertisement (LSA) requiring a Dijkstra (Shortest Path First (SPF)) calculation and the minimum time between successive SPF calculations.

Changing the timers affect CPU utilization and network reconvergence times. Lower values reduce convergence time but increase CPU utilization. Higher values reduce CPU utilization but increase reconvergence time.

Default none

spf-wait

Syntax **spf-wait** *max-spf-wait* [*spf-initial-wait* [*spf-second-wait*]]
no spf-wait

Context config>service>vprn>ospf>timers
config>service>vprn>ospf3>timers

Description This command defines the maximum interval between two consecutive SPF calculations in milliseconds. Timers that determine when to initiate the first, second, and subsequent SPF calculations after a topology change occurs can be controlled with this command. Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the *spf-second-wait* interval. For example, if the *spf-second-wait* interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, etc., until it reaches the **spf-wait** value. The SPF interval will stay at the **spf-wait** value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to *spf-initial-wait*.

The timer must be entered in increments of 100 milliseconds. Values entered that do not match this requirement will be rejected.

Use the **no** form of this command to return to the default.

Default no spf-wait

Parameters *max-spf-wait* — Specifies the maximum interval in milliseconds between two consecutive SPF calculations.

Values 10 — 120000

Default 10000

spf-initial-wait — Specifies the initial SPF calculation delay in milliseconds after a topology change.

Values 10 — 100000

Default 1000

spf-second-wait — Specifies the hold time in milliseconds between the first and second SPF calculation.

Values 10 — 100000

Default 1000

unicast-import-disable

Syntax [**no**] **unicast-import-disable**

Context config>service>vprn>ospf

Description This command allows one IGP to import its routes into RPF RTM while another IGP imports routes only into the unicast RTM.

Import policies can redistribute routes from an IGP protocol into the RPF RTM (the multicast routing table). By default, the IGP routes will not be imported into RPF RTM as such an import policy must be explicitly configured

Default no unicast-import-disable

vpn-domain

Syntax **vpn-domain** [*type* {**0005** | **0105** | **0205** | **8005**}] **id** *id*
no vpn-domain

Context config>service>vprn>ospf

Description This command specifies type of the extended community attribute exchanged using BGP to carry the OSPF VPN domain ID. This applies to VPRN instances of OSPF only. An attempt to modify the value of this object will result in an inconsistent value error when is not a VPRN instance. The parameters are mandatory and can be entered in either order. This command is not applicable in the **config>service>vprn>ospf3** context.

This command is not supported in OSPF3.

Default no vpn-domain

Parameters *id* — Specifies the OSPF VPN domain in the "xxxx.xxxx.xxxx" format. This is exchanged using BGP in the extended community attribute associated with a prefix. This object applies to VPRN instances of OSPF only.

type — Specifies the type of the extended community attribute exchanged using BGP to carry the OSPF VPN domain ID.

Values 0005, 0105, 0205, 8005

vpn-tag

Syntax **vpn-tag** *vpn-tag*
no vpn-tag

Context config>service>vprn>ospf

Description This command specifies the route tag for an OSPF VPN on a PE router. This field is set in the tag field of the OSPF external LSAs generated by the PE. This is mainly used to prevent routing loops. This applies to VPRN instances of OSPF only. An attempt to modify the value of this object will result in an inconsistent value error when is not a VPRN instance.

This command is not supported in OSPF3.

Default vpn-tag 0

lsa-arrival

Syntax **lsa-arrival** *lsa-arrival-time*
no lsa-arrival

Context config>service>vprn>ospf>timers
config>service>vprn>ospf3>timers

Description This parameter defines the minimum delay that must pass between receipt of the same Link State Advertisements (LSAs) arriving from neighbors. It is recommended that the neighbors configured (**lsa-generate**) *lsa-second-wait* interval is equal or greater then the **lsa-arrival** timer configured here.

Use the **no** form of this command to return to the default.

Default no lsa-arrival

Parameters *lsa-arrival-time* — Specifies the timer in milliseconds. Values entered that do not match this requirement will be rejected.

Values 0 — 600000

lsa-generate

Syntax **lsa-generate** *max-lsa-wait* [*lsa-initial-wait* [*lsa-second-wait*]]
no lsa-generate-interval

Context config>service>vprn>ospf>timers
config>service>vprn>ospf3>timers

Description This parameter customizes the throttling of OSPF LSA-generation. Timers that determine when to generate the first, second, and subsequent LSAs can be controlled with this command. Subsequent LSAs are generated at increasing intervals of the *lsa-second-wait* timer until a maximum value is reached. Configuring the **lsa-arrival** interval to equal or less than the *lsa-second-wait* interval configured in the **lsa-generate** command is recommended.

Use the **no** form of this command to return to the default.

Default no lsa-generate

Parameters *max-lsa-wait* — Specifies the maximum interval, in milliseconds, between two consecutive ocurrences of an LSA being generated.

The timer must be entered as either 1 or in millisecond increments. Values entered that do not match this requirement will be rejected.

Values 1 — 600000

RIP Commands

rip

Syntax [**no**] **rip**

Context config>service>vprn

Description This command enables the RIP protocol on the given VPRN IP interface.

The **no** form of the command disables the RIP protocol from the given VPRN IP interface.

Default no rip

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash | hash2**]
no authentication-key

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command sets the authentication password to be passed between RIP neighbors.

The authentication type and authentication key must match exactly for the RIP message to be considered authentic and processed.

The **no** form of the command removes the authentication password from the configuration and disables authentication.

Default **no authentication-key** — Authentication is disabled and the authentication password is empty.

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 16 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 33 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

authentication-type

Syntax **authentication-type** {**none** | **password** | **message-digest**}
no authentication-type

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command defines the type of authentication to be used between RIP neighbors. The type and password must match exactly for the RIP message to be considered authentic and processed.

The **no** form of the command removes the authentication type from the configuration and effectively disables authentication.

Default no authentication-type

Parameters *none* — No authentication is used.

simple — A simple clear-text password is sent.

md5 — MD5 authentication is used.

check-zero

Syntax **check-zero** {**enable | disable**}
no check-zero

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command enables checking for zero values in fields specified to be zero by the RIPv1 and RIPv2 specifications.

The **no** form of the command disables this check and allows the receipt of RIP messages even if the mandatory zero fields are non-zero.

Default no check-zero

Parameters **enable —** Enables checking of the mandatory zero fields in the RIPv1 and RIPv2 specifications and rejecting non-compliant RIP messages.

disable — Disables the checking and allows the receipt of RIP messages even if the mandatory zero fields are non-zero.

split-horizon

Syntax **split-horizon** {**enable** | **disable**}
no split-horizon

Context config>service>vprn>rip

config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command enables the use of split-horizon. RIP uses split-horizon with poison-reverse to protect from such problems as "counting to infinity". Split-horizon with poison reverse means that routes learned from a neighbor through a given interface are advertised in updates out of the same interface but with a metric of 16 (infinity).

The **split-horizon disable** command enables split horizon without poison reverse. This allows the routes to be re-advertised on interfaces other than the interface that learned the route, with the advertised metric equaling an increment of the metric-in value.

This configuration parameter can be set at three levels: global level (applies to all groups and neighbor interfaces), group level (applies to all neighbor interfaces in the group) or neighbor level (only applies to the specified neighbor interface). The most specific value is used. In particular if no value is set (**no split-horizon**), the setting from the less specific level is inherited by the lower level.

The **no** form of the command disables split horizon command which allows the lower level to inherit the setting from an upper level.

Default enabled

export

Syntax **export** *policy* [*policy...*]
no export

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command specifies the export policies to be used to control routes advertised to RIP neighbors. By default, RIP advertises routes from other RIP routes but does not advertise any routes from other protocols unless directed by an export policy.

The **no** form of the command removes all route policy names from the export list.

Default no export

Parameters *policy* — A route policy statement name.

export-limit

Syntax **export-limit** *number* [**log** *percentage*]
no export-limit

Context config>service>vprn>rip

Description This command configures the maximum number of routes (prefixes) that can be exported into RIP from the route table.

The **no** form of the command removes the parameters from the configuration.

Default no export-limit, the export limit for routes or prefixes is disabled..

Parameters *number* — Specifies the maximum number of routes (prefixes) that can be exported into RIP from the route table.

Values 1 — 4294967295

log *percentage* **—** Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.

Values 1 — 100

import

Syntax **import** *policy* [*policy*...]
no import

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command specifies the import policies to be used to control routes advertised from RIP neighbors. By default, RIP accepts all routes from configured RIP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

The **no** form of the command removes all route policy names from the import list.

Default no import

Parameters *policy* — A route policy statement name.

message-size

Syntax **message-size** *max-num-of-routes*
no message-size

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command sets the maximum number of routes per RIP update message.

The **no** form of the command resets the maximum number of routes back to the default of 25.

Default no message-size

Parameters *size* — Integer.

Default 25

Values 25 — 255

metric-in

Syntax **metric-in** *metric*
no metric-in

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command sets the metric added to routes that were received from a RIP neighbor.

The **no** form of the command reverts the *metric* value back to the default.

Default no metric-in

Parameters *metric* — The value added to the metric of routes received from a RIP neighbor, expressed as a decimal integer.

Values 1 — 16

metric-out

Syntax **metric-out** *metric*
no metric-out

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command sets the metric added to routes that were exported into RIP and advertised to RIP neighbors.

The **no** form of the command removes the command from the config and resets the metric-in value back to the default.

Default no metric-out

Parameters *metric* — The value added to the metric for routes exported into RIP and advertised to RIP neighbors, expressed as a decimal integer.

Values 1 — 16

preference

Syntax **preference** *preference*
no preference

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command sets the route preference assigned to RIP routes. This value can be overridden by route policies.

The **no** form of the command resets the *preference* to the default.

Default no preference

Parameters *preference* — An integer.

Values 1 — 255

Default 100

propagate-metric

Syntax **[no] propagate-metric**

Context config>service>vprn>rip

Description This command allows the RIP metric to be used to set the MP-BGP MED attribute when RIP is used as the CE-PE routing protocols for VPRNs. This is similar to the way the OSPF metric can be used to set the MP-BGP metric when OSPF is used as the CE-PE protocol.

MP-BGP will use the RIP metric to set the MED attribute, this attribute gets flooded through out the MP-BGP peers and will then be used to set the RIP metric at the other end and re-advertise the RIP metric to the far-end RIP neighbors.

receive

Syntax **receive** {**both** | **none** | **version-1** | **version-2**}
no receive

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command configures the type(s) of RIP updates that will be accepted and processed.

If **both** or **version-2** is specified, the RIP instance listens for and accepts packets sent to the broadcast and multicast (224.0.0.9) addresses.

If **version-1** is specified, the router only listens for and accepts packets sent to the broadcast address.

This control can be issued at the global, group or interface level. The default behavior accepts and processes both RIPv1 and RIPv2 messages.

The **no** form of the command resets the type of messages accepted to both.

Default **no receive** — Accepts both formats.

Parameters **both —** Receive RIP updates in either Version 1 or Version 2 format.

none — Do not accept and RIP updates.

version-1 — Router should only accept RIP updates in Version 1 format.

version-2 — Router should only accept RIP updates in Version 2 format.

send

Syntax **send** {**broadcast** | **multicast** | **none** | **version-1** | **both**}
no send

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command specifies the type of RIP messages sent to RIP neighbors. This control can be issued at the global, group or interface level. The default behavior sends RIPv2 messages with the multicast (224.0.0.9) destination address.

If **version-1** is specified, the router only listens for and accepts packets sent to the broadcast address.

The **no** form of this command resets the type of messages sent back to the default value.

Default **no send —** Sends RIPv2 to the broadcast address.

Parameters **broadcast —** Send RIPv2 formatted messages to the broadcast address.

multicast — Send RIPv2 formatted messages to the multicast address.

none — Do not send any RIP messages (i.e. silent listener).

version-1 — Send RIPv1 formatted messages to the broadcast address.

both — Send both RIP v1 & RIP v2 updates to the broadcast address.

timers

Syntax **timers** *update timeout flush*
no timers

Context config>service>vprn>rip
config>service>vprn>rip>group
config>service>vprn>rip>group>neighbor

Description This command sets the values for the update, timeout, and flush timers.

- Update timer — Determines how often RIP updates are sent.
- Timeout timer — If a router is not updated by the time the timer expires, the route is declared invalid, but maintained in the RIP database.
- Flush timer — Determines how long a route is maintained in the RIP database, after it has been declared invalid. Once this timer expires it is flushed from the RIP database completely.

The **no** form of the command resets all timers to their default values of 30, 180, and 120 seconds respectively.

Default no timers

Parameters *update* — The RIP update timer value in seconds.

Values 1 — 600

Default 30

timeout — The RIP timeout timer value in seconds.

Values 1 — 1200

Default 180

flush — The RIP flush timer value in seconds.

Values 1 — 1200

Default 120

group

Syntax [**no**] **group** *group-name*

Context config>service>vprn>rip

Description This command creates a context for configuring a RIP group of neighbors. RIP groups are a way of logically associating RIP neighbor interfaces to facilitate a common configuration for RIP interfaces.

The **no** form of the command deletes the RIP neighbor interface group. Deleting the group will also remove the RIP configuration of all the neighbor interfaces currently assigned to this group.

Default **no group** — No group of RIP neighbor interfaces defined

Parameters *group-name* — The RIP group name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

neighbor

Syntax [**no**] **neighbor** *ip-int-name*

Context config>service>vprn>rip>group

Description This command creates a context for configuring a RIP neighbor interface.
By default, interfaces are not activated in any interior gateway protocol such as RIP unless explicitly configured.

The **no** form of the command deletes the RIP interface configuration for this interface. The **shutdown** command in the **config>router>rip>group** *group-name*>**neighbor** *ip-int-name* context can be used to disable an interface without removing the configuration for the interface.

Default **no neighbor** — No RIP interfaces defined

Parameters *ip-int-name* — The IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service vprn interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32

characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

IPSec Configuration Commands

ipsec

Syntax **ipsec**

Context config>service>vprn>ipsec

Description This command enables the context to configure IPSec policies.

Default none

security-policy

security-policy *security-policy-id* [**create**]
no security-policy *security-policy-id*

Context config>service>vprn>ipsec

Description This command configures a security policy to use for an IPSec tunnel.

Default none

Parameters *security-policy-id* — specifies a value to be assigned to a security policy.

Values 1 — 8192

create — Keyword used to create the security policy instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context config>service>vprn>ipsec>sec-plcy

Description This command configures an IPSec security policy entry.

Parameters *entry-id* — Specifies the IPSec security policy entry.

Values 1 — 16

create — Keyword used to create the security policy entry instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

local-ip

Syntax **local-ip** {*ip-prefix/prefix-length* | *ip-prefix netmask* | **any**}

Context config>service>vprn>ipsec>sec-plcy>entry

Description This command configures the local (from the VPN) IP prefix/mask for the policy parameter entry.

Only one entry is necessary to describe a potential flow. The **local-ip** and **remote-ip** commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.

Parameters *ip-prefix* — The destination address of the aggregate route in dotted decimal notation.

Values a.b.c.d (host bits must be 0)
prefix-length 1 — 32

netmask — The subnet mask in dotted decimal notation.

any — keyword to specify that it can be any address.

remote-ip

Syntax **remote-ip** *ip-prefix/prefix-length* | *ip-prefix netmask* | **any**}

Context config>service>vprn>ipsec>sec-plcy>entry

Description This command configures the remote (from the tunnel) IP prefix/mask for the policy parameter entry.

Only one entry is necessary to describe a potential flow. The **local-ip** and **remote-ip** commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.

Parameters *ip-prefix* — The destination address of the aggregate route in dotted decimal notation.

Values a.b.c.d (host bits must be 0)
prefix-length 1 — 32

netmask — The subnet mask in dotted decimal notation.

any — keyword to specify that it can be any address.

ipsec-interface

Syntax **ipsec-interface** *ip-int-name* [**create**]
no ipsec-interface *ip-int-name*

Context config>service>vprn

Description This command configures an IPSec interface.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 1 — 32 characters maximum

create — Keyword used to create the IPSec interface instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

address

Syntax [**no**] **address** {*ip-address/mask* | *ip-address netmasks*}

Context config>service>vprn>ipsec-if

Description This command assigns an IP address/IP subnet to the interface

Parameters *ip-address* — Specifies the base IP address of the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

mask — The subnet mask in dotted decimal notation. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context config>service>vprn>ipsec-if

Description This command configures the IP maximum transmit unit (packet) for this interface.

The **no** form of the command returns the default value.

Default no ip-mtu

Parameters *octets* — Specifies the MTU size for this interface.

Values 512 — 9000

tunnel

Syntax **tunnel** *ipsec-tunnel-name* [**create**]
no tunnel *ipsec-tunnel-name*

Context config>service>vprn>ipsec-if>sap

Description This command specifies an IPSec tunnel name. An IPSec client sets up the encrypted tunnel across public network. The 7750-SR IPSec MDA acts as a concentrator gathering, and terminating these IPSec tunnels into an IES or VPRN service. This mechanism allows as service provider to offer a global VPRN service even if node of the VPRN are on an uncontrolled or insecure portion of the network.

Default none

Parameters *ipsec-tunnel-name* — Specifies an IPSec tunnel name up to 32 characters in length.

create — Keyword used to create the IPSec tunnel instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

bfd-designate

Syntax [**no**] **bfd-designate**

Context config>service>vprn>ipsec-if>sap>tunnel

Description This command specifies whether this IPSec tunnel is the BFD designated tunnel.

Default none

bfd-enable

Syntax [**no**] **bfd-enable service** *service-id* **interface** *interface-name* **dst-ip** *ip-address*

Context config>service>vprn>ipsec-if>sap>tunnel

Description This command assign a BFD session provide heart-beat mechanism for given IPsec tunnel. There can be only one BFD session assigned to any given IPsec tunnel, but there can be multiple IPsec tunnels using same BFD session. BFD control the state of the associated tunnel, if BFD session goes down, system will also bring down the associated non-designated IPsec tunnel.

Default none

Parameters **service *service-id*** **—** Specifies where the service-id that the BFD session resides.

interface *interface-name* — Specifies the name of the interface used by the BFD session.

dst-ip *ip-address* — Specifies the destination address to be used for the BFD session.

clear-df-bit

Syntax [**no**] **clear-df-bit**

Context config>service>vprn>ipsec-if>sap>tunnel
config>service>interface>vprn>sap>ip-tunnel

Description This command specifies whether to clear the Do not Fragment (DF) bit in the outgoing packets in this tunnel.

dynamic-keying

Syntax [**no**] **dynamic-keying**

Context config>service>vprn>ipsec-if>sap>tunnel

Description This command enables dynamic keying for the IPsec tunnel.

Default none

auto-establish

Syntax [**no**] **auto-establish**

Context config>service>vprn>ipsec-if>sap>tunnel

Description This command specifies whether to attempt to establish a phase 1 exchange automatically.

The **no** form of the command disables the automatic attempts to establish a phase 1 exchange.

Default no auto-establish

local-id

Syntax [**no**] **local-id type** {**ipv4** <*v4address*> | **fqdn** <*fqdn-value*>}

Context config>service>vprn>ipsec-if>sap>tunnel>dynamic-keying

Description This command specifies the local id of 7750 used for IDi or IDr for IKEv2 tunnels.

The local-id command can only be changed or removed when tunnel or gw is shutdown. The default value depends on the local-auth-method such as:

- Psk:local tunnel ip address
- Cert-auth: subject of the local certificate

Default no local-id

Parameters **type —** Specifies the type of local ID payload, it could be ipv4 address.

ipv4 — Specifies IPv4 as the local ID type. The default value is the local tunnel end-point address

v4address — Specifies an IPv4 address. A value must be configured.

fqdn — Specifies FQDN as the local ID type. A value must be configured.

fqdn-value — Specifies a FQDN vaue. A value must be configured.

transform

Syntax **transform** *transform-id* [*transform-id*...(up to 4 max)]
no transform

Context config>service>vprn>ipsec-if>sap>tunnel>dynamic-keying

Description This command associates the IPSec transform sets allowed for this tunnel. A maximum of four transforms can be specified. The transforms are listed in decreasing order of preference (the first one specified is the most preferred).

Default none

Parameters *transform-id* — Specifies the value used for transforms for dynamic keying.

Values 1 — 2048

local-gateway-address

Syntax **local-gateway-address** *ip-address* **peer** *ip-address* **delivery-service** *service-id*
no local-gateway-address

Context config>service>vprn>ipsec-if>sap>tunnel

Description This command specifies the local gateway address used for the tunnel and the address of the remote security gateway at the other end of the tunnelremote peer IP address to use.

Default The base routing context is used if the delivery-router option is not specified.

Parameters *ip-address* — IP address of the local end of the tunnel.

delivery-service *service-id* **—** The ID of the IES or VPRN (front-door) delivery service of this tunnel. Use this service-id to find the VPRN used for delivery.

Values *service-id*: 1 — 2147483648
svc-name: Specifies an existing service name up to 64 characters in length.

manual-keying

Syntax [**no**] **manual-keying**

Context config>service>vprn>ipsec-if>sap>tunnel

Description This command configures Security Association (SA) for manual keying. When enabled, the command specifies whether this SA entry is created manually by the user or dynamically by the IPsec sub-system.

Default none

security-association

Syntax **security-association** *security-entry-id* **authentication-key** *authentication-key* **encryption-key** *encryption-key* **spi** *spi* **transform** *transform-id* **direction** {**inbound** | **outbound**}
no security-association *security-entry-id* **direction** {**inbound** | **outbound**}

Context config>service>vprn>ipsec-if>sap>tunnel>manual-keying

Description This command configures the information required for manual keying SA creation.

Default none

Parameters *security-entry-id* — Specifies the ID of an SA entry.

Values 1 — 16

encryption-key *encryption-key* **—** specifies the key used for the encryption algorithm.

Values none or 0x0..0xFFFFFFFF...(max 64 hex nibbles)

authentication-key *authentication-key* **—**

Values none or 0x0..0xFFFFFFFF...(max 40 hex nibbles)

spi *spi* **—** Specifies the SPI (Security Parameter Index) used to look up the instruction to verify and decrypt the incoming IPSec packets when the direction is inbound. When the direction is outbound, the SPI that will be used in the encoding of the outgoing packets. The remote node can use this SPI to lookup the instruction to verify and decrypt the packet.

Values 256 — 16383

transform *transform-id* **—** specifies the transform entry that will be used by this SA entry. This object should be specified for all the entries created which are manual SAs. If the value is dynamic, then this value is irrelevant and will be zero.

Values 1 — 2048

direction {**inbound** | **outbound**} **—** Specifies the direction of an IPsec tunnel.

replay-window

Syntax **replay-window** {**32** | **64** | **128** | **256** | **512**}
no replay-window

Context config>service>vprn>ipsec-if>sap>tunnel

Description This command specifies the size of the anti-replay window. The anti-replay window protocol secures IP against an entity that can inject messages in a message stream from a source to a destination computer on the Internet.

Default none

Parameters {**32** | **64** | **128** | **256** | **512**} — Specifies the size of the SA anti-replay window.

security-policy

Syntax **security-policy** *security-policy-id*

no security-policy

Context config>service>vprn>ipsec-if>sap>tunnel

Description This command configures an IPSec security policy. The policy may then be associated with tunnels defined in the same context.

Default none

Parameters *security-policy-id* — Specifies the IPSec security policy entry that the tunnel will use.

Values 1 — 8192

Threat Management Service Interface Commands

tms-interface

Syntax **tms-interface** *interface-name* [**create**] [**off-ramp-vprn** *off-ramp-svc*] [**mgmt-vprn** *mgmt-svc*]
no tms-interface *interface-name*

Context config>service>vprn

Description This command configure a Threat Managment Service interface.

The **no** form of the command removes the interface name from the configuration.

Parameters *interface-name* — Specifies the interface name up to 22 characters in length.

create — Keyword used to create the interface name. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

off-ramp-vprn *off-ramp-svc* **—**

mgmt-vprn *mgmt-svc* **—**

address

Syntax **address** {*ip-address*/*mask*|*ip-address netmask*}
no address

Context config>service>vprn>tms-if

Description This command assigns an IP address/IP subnet/broadcast address to the TMS instance for communications between Arbor CP collectors/managers and the TMS instance operating within the Service Router.

The **no** form of the command removes the IP address information from the interface configuration.

Parameters *ip-address*/*mask* ip-address netmask

Specifies IP address information.

Values	<ip-address[/mask]>	ip-address a.b.c.d
	mask	32
	<netmask>	a.b.c.d (all 1 bits)

description

Syntax **description** *long-description-string*
no description

Context config>service>vprn>tms-if

Description This command configures a description for the interface.

The **no** form of the command removes the description from the interface configuration.

ipv6

Syntax [**no**] **ipv6**

Context config>service>vprn>tms-if

Description This command configures IPv6 for a threat-management service interface.

The **no** form of the command removes the IP address information from the interface configuration.

tms-egress-filter

Syntax [**no**] **tms-egress-filter** *filter-name*

Context config>service>vprn>tms-if

Description This command configures an egress filter for a threat-management service interface.

The **no** form of the command removes the filter from the interface configuration.

Parameters *filter-name* — Specifies the name of the filter for the TMS configuration.

password

Syntax **password** [*password*]
no password

Context config>service>vprn>tms-if

Description This command configures a password for the user.

The **no** form of the command removes the password.

Parameters *password* — Specifies the password for the TMS configuration.

Values <password>key1<delim>value1 key2<delim>value2 ...
<delim> is one of the following:
'=' value is unencrypted and remain unencrypted
':' value is unencrypted and to be encrypted
'%' value is encrypted and remain encrypted

port

Syntax **port** *mda-id*
no port

Context config>service>vprn>tms-if

Description This command specifies a chassis slot and MDA to bind the interface to a physical port.

The no form of the command removes the MDA ID from the interface configuration.

Parameters *mda-id* — Specifies the chassis slot and MDA.

Values <slot>/<mda> slot [1..10]
mda [1..2]

RADIUS Proxy Commands

radius-proxy

Syntax **radius-proxy**

Context config>service>vprn

Description This command enables the context to configure RADIUS proxy commands.

server

Syntax **server** *server-name* [**create**] [**purpose** {[**accounting**][**authentication**]}]
no server *server-name*

Context config>service>vprn>radius-proxy

Description This command configures the name of this RADIUS proxy server.

Parameters **purpose accounting —** Specifies that this RADIUS proxy server will be used for accounting purposes.

purpose authentication — Specifies that this RADIUS proxy server will be used for authentication purposes.

cache

Syntax **cache**

Context config>service>vprn>radius-proxy>server

Description This command enables the context to configure caching parameters.

The **no** form of the command disables caching.

key

Syntax **key** *packet-type* {**accept**|**request**} **attribute-type** *attribute-type* [**vendor-id** *vendor-id*]
no key

Context config>service>vprn>radius-proxy>server>cache

Description This command configures cache key parameters.

The **no** form of the command removes the parameters from the configuration.

Default no key

Parameters *packet-type* — specifies the packet type of the RADIUS messages to use to generate the key for the cache of this RADIUS proxy server.

In order to generate the key associated with a RADIUS Access-Accept message, the system uses the attribute of the type specified by the value of tmnxRadProxSrvCacheKeyAttrType, within the associated RADIUS message of the type specified by the value of tmnxRadProxSrvCacheKeyPktType.

Values accept, request

attribute-type *attribute-type* — specifies the RADIUS attribute type to cache for this RADIUS Proxy server.

In order to generate the key associated with a RADIUS Access-Accept message, the system uses the attribute of the type specified by the value of tmnxRadProxSrvCacheKeyAttrType, within the associated RADIUS message of the type specified by the value of tmnxRadProxSrvCacheKeyPktType.

Values 1 — 255

vendor-id *vendor-id* — specifies the RADIUS Vendor-Id.

If the value of tmnxRadProxSrvCacheKeyVendorId is equal to zero, the attribute type specified by tmnxRadProxSrvCacheKeyAttrType must be used if it appears outside of a Vendor-Specific attribute.

If the value of tmnxRadProxSrvCacheKeyVendorId is not equal to zero, the attribute type specified by tmnxRadProxSrvCacheKeyAttrType must be used if it appears as a sub-attribute within a Vendor-Specific attribute with Vendor-Id equal to the value of tmnxRadProxSrvCacheKeyVendorId.

Values 1 — 16777215, alu

timeout

Syntax **timeout** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no timeout

Context config>service>vprn>radius-proxy>server>cache

Description This command configures the timeout, in seconds, after which an entry in the cache will expire.

The **no** form of the command reverts to the default.

Default 300

Parameters *timeout* — Configures the timeout.

Values		
	hours	1..1
	minutes	1 — 59
	seconds	1 — 59

track-accounting

Syntax **track-accounting** [**start**] [**stop**] [**interim-update**]
no track-accounting

Context config>service>vprn>radius-proxy>server>cache

Description This command specifies which RADIUS accounting packets have impact on the cache of this RADIUS proxy server. Configure what RADIUS accounting packets have impact on the cache

The **no** form of the command reverts to the default.

Default no track-accounting

Default none

Parameters **start —**

stop —

interim-update —

default-accounting-server-policy

Syntax **default-accounting-server-policy** *policy-name*
no default-accounting-server-policy

Context config>service>vprn>radius-proxy>server

Description This command configures the name of the default RADIUS server policy associated with this RADIUS proxy server for accounting purposes.

This default policy is used if no policy can be derived from the user name.

The **no** form of the command removes the policy from the configuration.

Parameters *policy-name* — Specifies the default accounting RADIUS server policy up to 32 characters in length.

default-authentication-server-policy

Syntax **default-authentication-server-policy** *policy-name*
no default-authentication-server-policy

Context config>service>vprn>radius-proxy>server

Description This command configures the name of the default RADIUS server policy associated with this RADIUS proxy server for authentication purposes.

This default policy is used if no policy can be derived from the user name.

The **no** form of the command removes the policy from the configuration.

Parameters *policy-name* — Specifies the default authentication RADIUS server policy up to 32 characters in length.

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>service>vprn>radius-proxy>server

Description This command associates an interface to the proxy server.

The no form of the command removes the interface name from the proxy server configuration.

Default none

Parameters *ip-int-name* — Specifies the name of the IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

load-balance-key

Syntax **load-balance-key vendor** *vendor-id* [*vendor-id*...(up to 5 max)] **attribute-type** *attribute-type* [*attribute-type*...(up to 5 max)]
load-balance-key *source-ip-udp*
no load-balance-key

Context config>service>vprn>radius-proxy>server

Description This command configures how to construct the key for load-balancing RADIUS messages between RADIUS servers.

Default load-balance-key

Parameters **vendor** *vendor-id* **—** Specifies the RADIUS Vendor-Id.

Values 0 — 16777215

attribute-type *attribute-type* **—** Specifies a RADIUS attribute that must be used to construct the key for load-balancing RADIUS messages between RADIUS servers.

Values 1 — 255

secret

Syntax **secret** *secret* [**hash**|**hash2**]
no secret

Context config>service>vprn>radius-proxy>server

Description This command configures the secret key associated with the RADIUS server.

The no form of the command removes the key from the configuration.

Parameters *secret* — The secret key (password) to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values Up to 32 characters in length.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

send-accounting-response

Syntax [**no**] **send-accounting-response**

Context config>service>vprn>radius-proxy>server

Description This command specifies if this RADIUS proxy server itself responds with an Accounting-Response message to each received Accounting-Request instead of proxying them to a configured RADIUS server.

The **no** form of the command disables the accounting response messages.

Default disabled

username

Syntax **username** [1..32] **prefix-string** [128 chars max] [**accounting-server-policy** *policy-name*] [**authentication-server-policy** *policy-name*]
no username [1..32]

Context config>service>vprn>radius-proxy>server

Description This command configures username-to-RADIUS-server-policy associations.

The **no** form of the comand removes the associations from the configuration.

Default none

Parameters **username —**

Values 1 — 32

prefix-string —

Values 128 characters, maximum

accounting-server-policy *policy-name* **—**

authentication-server-policy *policy-name* **—**

radius-server

Syntax **radius-server**

Context config>service>vprn

Description This command enables the context to configure RADIUS server parameters.

server

Syntax **server** *server-name* [**address** *ip-address*] [**secret** *key*] [**hash**|**hash2**] [**port** *port*] [**create**]
no server *server-name*

Context config>service>vprn>radius-server

Description This command configures RADIUS server parameters.

The **no** form of the command removes the parameters from the configuration.

Parameters *server-name* — Specifies the name of this RADIUS server.

address *ip-address* **—** Specifies the IP address of the RADIUS server.

secret *key* **—** Specifies the secret key (password) to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values Up to 32 characters in length.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

port *port* **—** Specifies the UDP port number on which to contact the RADIUS server.

accept-coa

Syntax [**no**] **accept-coa**

Context config>service>vprn>radius-server

Description This command specifies if this RADIUS server is allowed to process Change of Authorization messages.

coa-script-policy

Syntax **coa-script-policy** *script-policy-name*
no coa-script-policy

Context config>service>vprn>radius-server

Description This command specifies the RADIUS script policy used to change the RADIUS attributes of the Change-of-Authorization messages.

The **no** form of the command removes the script policy from the configuration.

Default none

Parameters *script-policy-name* — Specifies a Python script policy to modify Change-of-Authorization messages.

pending-requests-limit

Syntax **pending-requests-limit** *limit*
no pending-requests-limit

Context config>router
config>service>vprn>radius-server>server

Description This command specifies the limit of the number of pending RADIUS authentication requests.

Default 4096

Parameters *limit* — Configure the limit of the number of pending RADIUS requests.

Values 1 — 4096

wpp

Syntax [**no**] **wpp**

Context config>router
config>service>vprn

Description This command enters the configuration context of web portal protocol (WPP) under router or vprn.

The **no** form of this command removes configuration under wpp.

Default no

portals

Syntax **portals**

Context config>router>wpp
config>service>vprn>wpp

Description This command enters the configuration context of web portal server.

portal

Syntax **portal** *name* **address** *ip-address* [**create**]
portal *name*
no portal *name*

Context config>router>wpp>portals
config>service>vprn>wpp>portals

Description This command either creates a new web portal server or enters an existing web portal server.

Default no

Parameters *name* — Specifies the name of the web portal server.

ip-address — Specifies IPv4 address of the web portal server.

shutdown

Syntax [**no**] **shutdown**

Context config>router>wpp>portals>portal
config>service>vprn>wpp>portals>portal

Description This command cause system stops receiving web portal protocol packet from the web portal server.

Default shutdown

shutdown

Syntax [**no**] **shutdown**

Context config>router>wpp
config>service>vprn>wpp

Description This command cause system stops receiving web portal protocol packet from all web portal servers defined in the routing instance

Default shutdown

wpp

Syntax [**no**] **wpp**

Context config>service>ies>sub-if>grp-if>
config>service>vprn>sub-if>grp-if>

Description This command enters the configuration context of web portal protocol (WPP) under group-interface.

The **no** form of this command removes configuration under WPP.

Default no

initial-app-profile

Syntax **initial-app-profile** *profile-name*
no initial-app-profile

Context config>service>ies>sub-if>grp-if>wpp
config>service>vprn>sub-if>grp-if>wppp

Description This command specifies the initial app-profile for the hosts created on the group-interface. This initial app-profile is replaced after hosts pass the web portal authentication.

Default no

Parameters *profile-name* — Specifies the name of app-profile.

initial-sla-profile

Syntax **initial-sla-profile** *profile-name*
no initial-sla-profile

Context config>router>wpp
config>service>vprn>wpp

Description This command specifies the initial sla-profile for the hosts created on the group-interface. This initial sla-profile is replaced after hosts pass the web portal authentication.

Default no

Parameters *profile-name* — Specifies the name of sla-profile.

initial-sub-profile

Syntax **initial-sub-profile** *profile-name*
no initial-sub-profile

Context config>service>ies>sub-if>grp-if>wpp
config>service>vprn>sub-if>grp-if>wpp

Description This command specifies the initial sub-profile for the hosts created on the group-interface. This initial sub-profile will be replaced after hosts pass web portal authentication.

Default no

Parameters *profile-name* — Specifies the name of sub-profile.

portal

Syntax **portal router** *router-instance* **name** *wpp-portal-name*
no portal

Context config>service>ies>sub-if>grp-if>wpp
config>service>vprn>sub-if>grp-if>wpp

Description This command specifies the web portal server that system talks to for the hosts on the group-interface.

Default no

Parameters *router-instance* — Specifies the routing-instance that web portal server is defined.

profile-name — Specifies the name of the web portal server.

restore-disconnected

Syntax [**no**] **restore-disconnected**

Context config>service>ies>sub-if>grp-if>wpp
config>service>vprn>sub-if>grp-if>wpp

Description This command enable the behavior that system will restore the initial-sla-profile/initial-sub-profile/ initial-aa-prfofile when hosts disconnects instead of removing them.

Default restore-disconnected

shutdown

Syntax [**no**] **shutdown**

Context config>service>ies>sub-if>grp-if>wpp
config>service>vprn>sub-if>grp-if>wpp

Description This command disables web port protocol for the group-interface.

Default shutdown