HLTAPI Cmd Ref Documentation

Release 1

Spirent

May 09, 2020
# 6PE/6VPE Functions

1. **sth::emulation_6pe_6vpe_provider_port_config**
   1.1. **Purpose**
   1.1.2. **Synopsis**
   1.1.3. **Arguments**
   1.1.4. **Return Values**
   1.1.5. **Description**
   1.1.6. **Examples**

1.2. **sth::emulation_6pe_6vpe_cust_port_config**
   1.2.1. **Purpose**
   1.2.2. **Synopsis**
   1.2.3. **Arguments**
   1.2.4. **Return Values**
   1.2.5. **Description**
   1.2.6. **Examples**

1.3. **sth::emulation_6pe_6vpe_config**
   1.3.1. **Purpose**
   1.3.2. **Synopsis**
   1.3.3. **Arguments**
   1.3.4. **Return Values**
   1.3.5. **Description**
   1.3.6. **Examples**

1.4. **sth::emulation_6pe_6vpe_control**
   1.4.1. **Purpose**
   1.4.2. **Synopsis**
   1.4.3. **Arguments**
   1.4.4. **Return Values**
   1.4.5. **Description**
   1.4.6. **Examples**

1.5. **sth::emulation_6pe_6vpe_info**
   1.5.1. **Purpose**
   1.5.2. **Synopsis**
   1.5.3. **Arguments**
   1.5.4. **Return Values**
   1.5.5. **Description**
   1.5.6. **Examples**
2 Indices and tables 37

Index 39
The Spirent TestCenter Automation HLTAPI Command Reference provides basic information about Spirent High Level Test Application Programming Interface (HLTAPI) functions. It also provides descriptions of how to use these functions along with examples of creating and running test configurations. The target audience is test specialists who run automation tests using Spirent TestCenter hardware and software. Users of this manual should have the following knowledge and experience:

- Familiarity with the operating system on your PC or workstation (Microsoft® Windows® or Linux®).
- Moderate familiarity with test equipment.
- Working knowledge of data communications theory and practice.
- Ability to program with the Tcl, Python, or Perl scripting languages.
1.1 sth::emulation_6pe_6vpe_provider_port_config

1.1.1 Purpose

Spirent Extension (for Spirent HLTAPI only).
Configures or deletes an emulated provider-side test port

1.1.2 Synopsis

sth::emulation_6pe_6vpe_provider_port_config
-mode create -port_handle <port_handle> | -mode delete -handle <handle>
[-dut_interface_ipv4_addr <a.b.c.d>]
[-dut_interface_ipv4_addr_step <a.b.c.d>]
[-dut_interface_ipv4_prefix_len <0-32>]
[-sub_interface_enable {true|false}]
[-sub_interface_count <0-255>]
[-vlan_id <0-4095>]

1.1.3 Arguments

-port_handle
   Specifies the test port to be added to the provider side of the 6PE/6VPE network. This argument is mandatory for -mode create.

-mode
   Specifies the action to be performed. This argument is mandatory. Possible values are described below:
create  Adds a provider-side test port. You must specify 
-port_handle.

delete  Deletes specified routers under the provide-side port. 
You must specify -handle.

-handle
  Specifies the handle of routers created under the emulated test port. This argument is mandatory for -mode 
delete.

-dut_interface_ipv4_addr
  Defines the first IPv4 address of the DUT interfaces connected to the port. The default value is 192.85.1.1.

-dut_interface_ipv4_addr_step
  Specifies the step size by which the DUT IPv4 address is incremented. The default value is 0.0.1.0. The number 
of times that the step repeats is the same as the number of sub-interfaces. This argument is available when 
-sub_interface_enable is set to true.

-dut_interface_ipv4_prefix_len
  Specifies the IPv4 address prefix length of DUT interface connected to the port. Possible values range from 0 to 
32. The default value is 24.

-sub_interface_enable
  Enables or disables sub-interface on the DUT. Possible values are true and false. The default value is false. 
When this argument is enabled, you can specify the following arguments:

   -sub_interface_count
   -dut_interface_ipv4_addr_step
   -vlan_id
   -vlan_id_step

-sub_interface_count
  Defines the number of sub-interfaces on the DUT interface. Possible values range from 1 to 255. The default 
value is 1. This argument is available when -sub_interface_enable is set to true.

-vlan_id
  Specifies the starting VLAN ID of DUT interfaces. Possible values range from 0 to 4095. The default value is 
1. This argument is available when -sub_interface_enable is set to true.

-vlan_id_step
  Specifies the step size by which the VLAN ID is incremented. Possible values range from 0 to 4095. The default 
value is 1. This argument is available when -sub_interface_enable is set to true.

1.1.4 Return Values

Depending on the specific language that HLTAPI uses, the function returns a keyed list/dictionary/hash (See Introduc-
tion for more information on return value formats) using the following keys (with corresponding data):

- status  Success (1) or failure (0) of the operation
- log     An error message (if the operation failed)

1.1.5 Description

The sth:: emulation_6pe_6vpe_provider_port_config function configures an emulated provider-side 
port, or deletes the routers under the port (specified by -handle). Use the -port_handle argument to specify the port to
be added. Use the -action argument to specify the action to perform.

1.1.6 Examples

The following example configures a provider-side port:

```
sth::emulation_6pe_6vpe_provider_port_config
  -port_handle $port1
  -mode create
  -dut_interface_ipv4_addr 192.86.1.1
  -dut_interface_ipv4_addr_step 0.0.2.0
  -dut_interface_ipv4_prefix_len 24
  -sub_interface_enable true
  -sub_interface_count 10
  -vlan_id 102
  -vlan_id_step 2
```

Sample output:

```
{status 1}
```

1.2 sth::emulation_6pe_6vpe_cust_port_config

1.2.1 Purpose

Spirent Extension (for Spirent HLTAPI only).

Configures or deletes an emulated customer-side test port

1.2.2 Synopsis

```
sth::emulation_6pe_6vpe_cust_port_config
  -mode create -port_handle <port_handle> [-mode delete -handle <handle>]
  [-dut_interface_ipv6_addr <aaaa.bbbb.cccc.dddd.eeee.ffff.gggg.hhhh>]
  [-dut_interface_ipv6_addr_step <aaaa.bbbb.cccc.dddd.eeee.ffff.gggg.hhhh>]
  [-dut_interface_ipv6_prefix_len <1-128>]
  [-sub_interface_enable {true|false}]
  [-sub_interface_count <0-255>]
  [-vlan_id <0-4095>]
  [-vlan_id_step <0-4095>]
```

1.2.3 Arguments

- **-port_handle**
  Specifies the test port to be added to the customer side of the 6PE/6VPE network. This argument is mandatory for -mode create.

- **-mode**
  Specifies the action to be performed. This argument is mandatory. Possible values are described below:
create Adds a customer-side test port. You must specify -port_handle.

delete Deletes specified routers under the customer-side port. You must specify -handle.

-handle
Specifies the handle of the CE routers. This argument is mandatory for -mode delete.

-dut_interface_ipv6_addr
Specifies the first IPv6 address of the DUT interfaces connected to the port. The default value is ::.

-dut_interface_ipv6_addr_step
Specifies the step value by which to increment subsequent DUT IPv6 addresses. This argument is only available when -sub_interface_enable is set to true. The default value is 0:0:1::.

-dut_interface_ipv6_prefix_len
Specifies the IPv6 address’s prefix length of the DUT connected to the port. Possible values range from 1 to 128. The default value is 64.

-sub_interface_enable
Enables or disables sub-interfaces on the DUT interface. Possible values are true and false. The default value is false.

-sub_interface_count
Defines the number of sub-interfaces to be created for the DUT. Possible values range from 1 to 255. The default value is 1. This argument is available when -sub_interface_enable is set to true.

-vlan_id
Specifies the starting VLAN ID. Possible values range from 0 to 4095. The default value is 1. This argument is available when -sub_interface_enable is set to true.

-vlan_id_step
Defines the step size by which to increment the VLAN ID. Possible values range from 0 to 4095. The default value is 1. This argument is available when -sub_interface_enable is set to true.

1.2.4 Return Values

Depending on the specific language that HLTAPI uses, the function returns a keyed list/dictionary/hash (See Introduction for more information on return value formats) using the following keys (with corresponding data):

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Success (1) or failure (0) of the operation</td>
</tr>
<tr>
<td>log</td>
<td>An error message (if the operation failed)</td>
</tr>
</tbody>
</table>

1.2.5 Description

The sth::emulation_6pe_6vpe_cust_port_config function configures an emulated customer-side port, or deletes the routers under the port (specified by -handle). Use the -port_handle argument to specify the port to be added. Use the -action argument to specify the action to perform.

1.2.6 Examples

The following example configures a customer-side port:
### 1.3 sth::emulation_6pe_6vpe_config

#### 1.3.1 Purpose

Spirent Extension (for Spirent HLTAPI only).

Creates or deletes IPv6 Provider Edge Router (6PE) or IPv6 VPN Provider Edge Router (6VPE) network topologies, mapping the operations of the 6PE or 6VPE Wizard in the Spirent TestCenter GUI.

The function creates emulated and simulated Customer Edge (CE), Provider (P), and Provider Edge (PE) routers, specifies and enables routing and labeling protocols, configures customer and provider side VPNs, and creates the traffic that is sent between VPNs.

#### 1.3.2 Synopsis

```
sth::emulation_6pe_6vpe_config
  -handle <handle>
  -mode <create|delete>
  [-dut_router_id <a.b.c.d>]
  [-dut_as <1-65535>]
  [-dut_4byte_as_enable {true|false}]
  [-dut_4byte_as <65535:65535>]
  [-use_cust_ports {true|false}]
  [-use_provider_ports {true|false}]
  [-igp_protocol {ospf|isis|rip|none}]
  [-mpls_protocol {none|ldp|rsvp|ospf|isis}]

IGP OSPF Router Generation Parameters
```

```
[-igp_ospf_area_id <a.b.c.d>]
[-igp_ospf_network_type {native|broadcast|p2p}]
[-igp_ospf_router_priority <0-255>]
[-igp_ospf_interface_cost <1-65535>]
[-igp_ospf_options <0 - 0x7f >]
[-igp_ospf_auth_mode {none|simple|md5}]
[-igp_ospf_auth_password <password>]
[-igp_ospf_auth_md5_key <0-255>]
```
[-igp_ospf_graceful_restart_enable {true|false}]
[-igp_ospf_graceful_restart_type {none|rfc_standard|ll_signalling}]
[-igp_ospf_bfd_enable {true|false}]

IGP ISIS Router Generation Parameters

[-igp_isis_level {level1|level2|level1_and_2}]
[-igp_isis_network_type {broadcast|p2p}]
[-igp_isis_router_priority <0-127>]
[-igp_isis_area1 <ANY>]
[-igp_isis_area2 <ANY>]
[-igp_isis_area3 <ANY>]
[-igp_isis_circuit_id <0-255>]
[-igp_isis_auth_mode {none|simple|md5}]
[-igp_isis_auth_password <ANY>]
[-igp_isis_auth_md5_key <0-255>]
[-igp_isis_metric_mode {narrow|wide|narrow_and_wide}]
[-igp_isis_11_metric <1-63>]
[-igp_isis_11Wide_metric <0-16777215>]
[-igp_isis_12_metric <1-63>]
[-igp_isis_12Wide_metric <0-16777215>]
[-igp_isis_graceful_restart_enable {true|false}]
[-igp_isis_hello_padding {true|false}]
[-igp_isis_bfd_enable {true|false}]

MPLS RSVP-TE Router Generation Parameters

[-mpls_rsvp_bandwidth_per_link {1-2147483647}]
[-mpls_rsvp_bandwidth_per_tunnel {1-2147483647}]
[-mpls_rsvp_egress_label {next_available|implicit_null|explicit_null}]
[-mpls_rsvp_transit {accept_all|accept_configured}]
[-mpls_rsvp_min_label {1-65535}]
[-mpls_rsvp_max_label {1-65535}]
[-mpls_rsvp_graceful_restart_enable {true|false}]
[-mpls_rsvp_recover_time <0-4294967295>]
[-mpls_rsvp_restart_time <0-4294967295>]
[-mpls_rsvp_bfd_enable {true|false}]
[-mpls_rsvp_request_conf {true|false}]
[-mpls_rsvp_hello_enable {true|false}]
[-mpls_rsvp_hello_interval <1-2147483647>]
[-mpls_rsvp_bundle_interval <1-2147483647>]
[-mpls_rsvp_summary_refresh_interval <1-2147483647>]
[-mpls_rsvp_inter_packet_delay <1-2147483647>]
[-mpls_rsvp_refresh_interval <1-2147483647>]
[-mpls_rsvp_refresh_delivery {true|false}]
[-mpls_rsvp_retrans_interval <1-2147483647>]
[-mpls_rsvp_retrans_limit <0-10>]
[-mpls_rsvp_retrans_delta <0-3>]

MPLS LDP Router Generation Parameters

[-mpls_ldp_hello_type { direct|targeted}]
[-mpls_ldp_transport_mode { none|tester_ip|router_id}]
[-mpls_ldp_hello_interval <1-21845>]
[mpls_ldp_keepalive_interval <1-21845>]
[mpls_ldp_egress_label { next_available|implicit_null|explicit_null }]
[mpls_ldp_min_label <1-65535>]
[mpls_ldp_graceful_restart_enable {true|false}]
[mpls_ldp_recover_time <0-4294967>]
[mpls_ldp_reconnect_time <0-4294967>]
[mpls_ldp_bfd_enable {true|false}]
[mpls_ldp_label_adv_mode {downstream_unsolicited|downstream_on_demand}]
[mpls_ldp_auth_mode {none|md5}]
[mpls_ldp_auth_password <ANY>]

**MPLS OSPF-SR Router Generation Parameters**

[mpls_ospf_sr_algorithms <0-4294967295>]
[mpls_ospf_sid_base <0-4294967295>]
[mpls_ospf_sid_range <0-65535>]
[mpls_ospf_node_sid_index <0-4294967295>]
[mpls_ospf_node_sid_index_step <0-4294967295>]

**MPLS ISIS-SR Router Generation Parameters**

[mpls_isis_sr_algorithm <0-4294967295>]
[mpls_isis_sid_base <0-4294967295>]
[mpls_isis_sid_range <0-65535>]
[mpls_isis_node_sid_index <0-4294967295>]
[mpls_isis_node_sid_index_step <0-4294967295>]

**P Router Generation Parameters**

[p_router_enable {true|false}]
[p_router_num_per_subif <1-65535>]
[p_router_topology_type {tree|grid}]
[p_router_id_start <a.b.c.d>]
[p_router_id_step <a.b.c.d>]
[p_router_ipv4_addr <a.b.c.d>]
[p_router_ipv4_prefix_len <0-32>]

**PE Router Generation Parameters**

[pe_router_num_per_subif <1-10000>]
[pe_router_id_start <a.b.c.d>]
[pe_router_id_step <a.b.c.d>]
[vpn_6vpe_enable {true|false}]
[bgp_route_reflector_enable {true|false}]
[bgp_route_reflector_per_subif <1-65535>]
[bgp_route_reflector_per_pe <1-65535>]
[bgp_route_reflector_id_start <a.b.c.d>]
[bgp_route_reflector_id_step <a.b.c.d>]
[bgp_route_reflector_cluster_id <a.b.c.d>]
[bgp_route_reflector_cluster_id_step <a.b.c.d>]
[bgp_route_reflector_ids <a.b.c.d>]
[bgp_route_reflector_mode {stc_as_rr|dut_as_rr}]
[bgp_bfd_enable {true|false}]

1.3. sth::emulation_6pe_6vpe_config
VPN Generation Parameters

[-vrf_count <1-65535>]
[-vrf_rd_assignment {use_rt|manual}]
[-vrf_route_target_start <ANY>]
[-vrf_route_target_step <ANY>]
[-cust_ce_vrf_assignment {round_robin|sequential}]
[-cust_ce_routing_protocol {bgp|ospf|rip|isis|mixed}]
[-cust_ce_bgp_percent <0-100>]
[-cust_ce_rip_percent <0-100>]
[-cust_ce_ospf_percent <0-100>]
[-cust_ce_isis_percent <0-100>]
[-cust_ce_bgp_as <1-65535>]
[-cust_ce_bgp_as_step_per_ce_enable {true|false}]
[-cust_ce_bgp_as_step_per_ce <0-65535>]
[-cust_ce_bgp_as_step_per_vrf_enable {true|false}]
[-cust_ce_bgp_as_step_per_vrf <0-65535>]
[-cust_ce_bgp_4byte_as_enable {true|false}]
[-cust_ce_bgp_4byte_as <ANY>]
[-cust_ce_bgp_4byte_as_step_per_ce_enable {true|false}]
[-cust_ce_bgp_4byte_as_step_per_ce <0-65535>]
[-cust_ce_bgp_4byte_as_step_per_vrf_enable {true|false}]
[-cust_ce_bgp_4byte_as_step_per_vrf <0-65535>]
[-cust_rd_start <ANY>]
[-cust_rd_step_per_vrf_enable {true|false}]
[-cust_rd_step_per_vrf <ANY>]
[-cust_rd_step_per_ce_enable {true|false}]
[-cust_rd_step_per_ce <ANY>]

[-provider_pe_vrf_assignment {vpn_per_pe|pe_per_vpn}]
[-provider_pe_vrf_count <integer>]
[-provider_pe_vrf_all_assign {true|false}]
[-provider_ce_bgp_as_enable {true|false}]

[-provider_ce_bgp_as <1-65535>]
[-provider_ce_bgp_as_step_per_ce_enable {true|false}]
[-provider_ce_bgp_as_step_per_ce <1-65535>]
[-provider_ce_bgp_as_step_per_vrf_enable {true|false}]
[-provider_ce_bgp_as_step_per_vrf <1-65535>]

[-provider_ce_bgp_4byte_as_enable {true|false}]
[-provider_ce_bgp_4byte_as <ANY>]
[-provider_ce_bgp_4byte_as_step_per_ce_enable {true|false}]
[-provider_ce_bgp_4byte_as_step_per_ce <1-65535>]
[-provider_ce_bgp_4byte_as_step_per_vrf_enable {true|false}]
[-provider_ce_bgp_4byte_as_step_per_vrf <1-65535>]

[-provider_rd_start <ANY>]
[-provider_rd_step_per_vrf_enable {true|false}]
[-provider_rd_step_per_vrf <ANY>]
[-provider_rd_step_per_ce_enable {true|false}]
[-provider_rd_step_per_ce <ANY>]

Traffic Generation Parameters

[-traffic_flow_direction {none|fully_meshed|cust_to_core|core_to_customer|bidirectional}]
[-traffic_pattern {one_to_one|one_to_many}]
[-traffic_stream_group_method {aggregate|vpn}]
[-traffic_use_single_stream_per_endpoint_pair {true|false}]
[-traffic_load_percent_provider <0-100>]
[-traffic_load_percent_cust <0-100>]

1.3.3 Arguments

-handle
   Specifies the 6PE/6VPE network configuration handle. This argument is required for -mode delete.

-mode
   Specifies the action to be performed. This argument is mandatory. Possible values are described below:

   create  Creates a 6PE/6VPE network configuration
   delete  Deletes the 6PE/6VPE network configuration specified by -handle

-dut_router_id
   Specifies the router ID for the DUT. The value must be in IPv4 format. The default value is 10.0.0.1.

-dut_as
   The Autonomous System (AS) number of the DUT. Possible values range from 1 to 65535. The default value is 1.

-dut_4byte_as_enable
   Enables or disables the 4-byte AS number on the DUT. Possible values are true (enable) and false (disable). The default value is false.

-dut_4byte_as
   Specifies the 4-byte AS number of the DUT, in the format of <integer>::<integer>. The integer must be less than 65535. The default value is 1:1.

-use_cust_ports
   Determines whether to set the DUT to port connection for customer ports. Possible values are true and false. Set it to false if the test does not use customer-side ports. The default value is true.
-use_provider_ports
   Determines whether to set the DUT to port connection for provider ports. Possible values are true and false. Set it to false if the test does not use provider-side ports. The default value is true.

-igp_protocol
   Specifies the Interior Gateway Protocol (IGP) to be used by the DUT. Possible values are:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>OSPF</td>
</tr>
<tr>
<td>ISIS</td>
<td>ISIS</td>
</tr>
<tr>
<td>RIP</td>
<td>RIP</td>
</tr>
<tr>
<td>NONE</td>
<td>No IGP protocol</td>
</tr>
</tbody>
</table>

   The default value is OSPF.

-mpls_protocol
   Specifies the MPLS protocol to be used by the DUT. Possible values are:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>No MPLS protocol</td>
</tr>
<tr>
<td>LDP</td>
<td>LDP</td>
</tr>
<tr>
<td>RSVP</td>
<td>RSVP-TE</td>
</tr>
<tr>
<td>OSPF</td>
<td>OSPF SR</td>
</tr>
<tr>
<td>ISIS</td>
<td>ISIS SR</td>
</tr>
</tbody>
</table>

   The default value is LDP.

-igp_ospf_area_id
   Specifies the IP address that indicates the customer-side area to which the emulated router belongs. The default value is 0.0.0.0. This argument is available when -igp_protocol is set to OSPF.

-igp_ospf_network_type
   Specifies the network link type to use. Possible values are:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>native</td>
<td>Use the adjacency specified by the port-type</td>
</tr>
<tr>
<td>broadcast</td>
<td>Use a Broadcast adjacency</td>
</tr>
<tr>
<td>p2p</td>
<td>Use a P2P adjacency</td>
</tr>
</tbody>
</table>

   The default value is native. This argument is available when -igp_protocol is set to OSPF.

-igp_ospf_router_priority
   Specifies the router priority of the emulated router. Possible values range from 0 to 255. The default value is 0. This argument is available when -igp_protocol is set to OSPF.

-igp_ospf_interface_cost
   Specifies the cost of the interface connecting the emulated router to the neighbor DUT router. Possible values range from 1 to 65535. The default value is 1. This argument is available when -igp_protocol is set to OSPF.

-igp_ospf_options
   Specifies the Options field that describes the optional OSPF capabilities of the router. Possible values range from 0 to 0x7f. The values are described below:

<table>
<thead>
<tr>
<th>Bit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tbit</td>
<td>Type of Service (TOS) (T,0).</td>
</tr>
<tr>
<td>ebit</td>
<td>Specifies the way AS-external-LSAs are flooded (E,1)</td>
</tr>
<tr>
<td>mcbit</td>
<td>Specifies whether IP multicast datagrams are forwarded (MC,2)</td>
</tr>
<tr>
<td>npbit</td>
<td>Specifies the handling of Type-7 LSAs (NSSA) (N/P,3)</td>
</tr>
<tr>
<td>eabit</td>
<td>Specifies the router's willingness to receive and forward External-Attributes-LSAs (EA,4)</td>
</tr>
<tr>
<td>dcbit</td>
<td>Specifies the router's handling of demand circuits (DC,5)</td>
</tr>
</tbody>
</table>

(continues on next page)
obit Specifies the router's willingness to receive and forward Opaque LSAs as specified in RFC 2370 (0,6)
unused7 This bit is not used

The default for OSPFv2 is 0x02, which sets the E-bit.

-**igp OSPF auth mode**
  Specifies the type of OSPFv2 authentication to be used. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No authentication</td>
</tr>
<tr>
<td>simple</td>
<td>Use simple authentication</td>
</tr>
<tr>
<td>md5</td>
<td>Use MD5 authentication</td>
</tr>
</tbody>
</table>

The default value is none. This argument is available when `-igp_protocol` is set to OSPF.

-**igp OSPF auth password**
  Specifies the password used for OSPFv2 authentication. This argument is available when `-igp OSPF auth mode` is set to simple or md5. When you specify `-igp OSPF auth mode` simple, the value must be of 1-8 alphanumeric characters. When you specify `-igp OSPF auth mode` md5, the value must be of 1-16 alphanumeric characters. The default value is “spirent”.

-**igp OSPF auth md5 key**
  Specifies the MD5 key used for OSPFv2 authentication. Possible values range from 0 to 255. The default value is 1. This argument is available when `-igp OSPF auth mode` is set to md5.

-**igp OSPF graceful restart enable**
  Enables or disables graceful restart for OSPF sessions. Possible values are true (enable) and false (disable). The default value is false. This argument is available when `-igp_protocol` is set to OSPF.

-**igp OSPF graceful restart type**
  Specifies the type of graceful restart to be used by the OSPF session. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No graceful restart</td>
</tr>
<tr>
<td>rfc_standard</td>
<td>RFC3623</td>
</tr>
<tr>
<td>ll_signalling</td>
<td>Link-Layer Signaling</td>
</tr>
</tbody>
</table>

The default value is none.

-**igp OSPF bfd enable**
  Enables or disables Bidirectional Forwarding Detection (BFD) on the OSPF interface. Possible values are true (enable) and false (disable). The default value is false. This argument is available when `-igp_protocol` is set to OSPF.

-**igp isis level**
  Specifies the IS-IS level to be used on the customer side. It defines the type of adjacency that Spirent HLTAPI establishes with the DUT. Possible values are described below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level1</td>
<td>Level 1 (intra-areas)</td>
</tr>
<tr>
<td>level2</td>
<td>Level 2 (inter-areas)</td>
</tr>
<tr>
<td>level1_and_2</td>
<td>Both Level 1 and Level 2</td>
</tr>
</tbody>
</table>

The default value is level2. This argument is available when `-igp_protocol` is set to ISIS.

-**igp isis network type**
  Specifies the IS-IS network type on the customer side. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Broadcast network</td>
</tr>
<tr>
<td>p2p</td>
<td>P2P network</td>
</tr>
</tbody>
</table>
The default value is broadcast. This argument is available when -igp_protocol is set to ISIS.

-igp_isis_router_priority
Specifies the priority for the emulated IS-IS router. Possible values range from 0 to 127. The default value is 0. This argument is available when -igp_protocol is set to ISIS.

-igp_isis_area1
Specifies the mandatory area address 1. You must specify at least one address. Spirent HLTAPI supports up to three addresses per emulated router. This argument is available when -igp_protocol is set to ISIS.

-igp_isis_area2
Specifies the optional area address 2. This argument is available when -igp_protocol is set to ISIS. The default value is "."

-igp_isis_area3
Specifies the optional area address 3. This argument is available when -igp_protocol is set to ISIS. The default value is "."

-igp_isis_circuit_id
Specifies the circuit ID for the IS-IS session. Possible values range from 0 to 255. The default value is 1. This argument is available when -igp_protocol is set to ISIS.

-igp_isis_auth_mode
Specifies the type of IS-IS authentication to be used. Possible values are:

```
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No authentication</td>
</tr>
<tr>
<td>simple</td>
<td>Use simple authentication</td>
</tr>
<tr>
<td>md5</td>
<td>Use the MD5 key ID</td>
</tr>
</tbody>
</table>
```

The default value is none. This argument is available when -igp_protocol is set to ISIS.

-igp_isis_auth_password
Specifies the password used for IS-IS authentication. This argument is available when -igp_isis_auth_mode is set to simple or md5. When you specify -igp_isis_auth_mode simple, the value must be of 1-8 alphanumeric characters. When you specify -igp_isis_auth_mode md5, the value must be of 1-16 alphanumeric characters. The default value is "spirent".

-igp_isis_auth_md5_key
Specifies the MD5 key used in IS-IS authentication. Possible values range from 0 to 255. The default value is 1. This argument is available when -igp_isis_auth_mode is set to md5.

-igp_isis_metric_mode
Specifies the length of the metric field in the Link State Path (LSP) packet. This argument is available when -igp_protocol is set to ISIS. Possible values are described below:

```
<table>
<thead>
<tr>
<th>Metric Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>narrow</td>
<td>Router advertises routes with a narrow (6-bit) metric</td>
</tr>
<tr>
<td>wide</td>
<td>Router advertises routes with a wide (24 or 32-bit) metric (required for IS-IS TE)</td>
</tr>
<tr>
<td>narrow_and_wide</td>
<td>Router advertises the same route with both metrics</td>
</tr>
</tbody>
</table>
```

The default value is narrow_and_wide.

-igp_isis_l1_metric
Specifies the metric of the emulated router interface. It is blank and disabled if -igp_isis_level is set to level2 or if -igp_isis_metric_mode is set to wide. Possible values range from 1 to 63. The default value is 1.

-igp_isis_l1_wide_metric
Indicates the 3-octet metric of a link from the emulated ISIS router to the DUT. It is blank and disabled if
-igp_isis_level is set to level2 or if -igp_isis_metric_mode is set to narrow. Possible values range from 0 to 16777215. The default value is 1.

-igp_isis_l2_metric
Indicates the metric of the emulated ISIS router interface. It is blank and disabled if -igp_isis_level is set to level1 or if -igp_isis_metric_mode is set to wide. Possible values range from 1 to 63. The default value is 1.

-igp_isis_l2_wide_metric
Indicates the 3-octet traffic engineering metric of a link from the emulated ISIS router to the DUT. It is blank and disabled if -igp_isis_level is set to level1 or if -igp_isis_metric_mode is set to narrow. Possible values range from 0 to 16777215. The default is 1.

-igp_isis_graceful_restart_enable
Enables or disables the IS-IS graceful restart. Possible values are false (disable) and true (enable). The default value is false.

-igp_isis_hello_padding
Enables or disables Hello padding for IS-IS sessions. Possible values are true (enable) and false (disable). The default value is true. This argument is available when you specify -igp_protocol ISIS.

-igp_isis_bfd_enable
Enables or disables BFD on IS-IS interfaces. Possible values are true (enable) and false (disable). The default value is false.

mpls_rsvp_bandwidth_per_link
Specifies the maximum bandwidth per ISIS/OSPFv2 TE link, in bytes per second, for simulated provider router topology links. Possible values range from 1 to 2147483647. The default value is 100000. This argument is available when you specify -mpls_protocol RSVP.

mpls_rsvp_bandwidth_per_tunnel
Specifies the RSVP-TE bandwidth rate, in bytes per second, for provider tunnels. Possible values range from 1 to 2147483647. The default value is 0. This argument is available when you specify -mpls_protocol RSVP.

mpls_rsvp_egress_label
Specifies the label to be advertised when emulated router is at the tail-end of the tunnel. This argument is available when you specify -mpls_protocol rsvp. The values are described below:

<table>
<thead>
<tr>
<th>next_available</th>
<th>Advertises the next available label</th>
</tr>
</thead>
<tbody>
<tr>
<td>implicit_null</td>
<td>Advertises label 3, the implicit null label</td>
</tr>
<tr>
<td>explicit_null</td>
<td>Advertise label 9, the explicit null label</td>
</tr>
</tbody>
</table>

The default value is next_available.

mpls_rsvp_transit
Defines the RESV message sent when emulated router is not the tail-end router for PATH messages it receives. This argument is available when you specify -mpls_protocol rsvp. Possible values are described below:

<table>
<thead>
<tr>
<th>accept_all</th>
<th>The router sends a RESV message with the next available label for every PATH message received by the unique MAC/VLAN combination on the port</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept_configured</td>
<td>The router sends a RESV message with the next available label in response to PATH messages that match one of its egress tunnels</td>
</tr>
</tbody>
</table>

The default value is accept_configured.
-mpls_rsvp_min_label
Defines the minimum label number used by the RSVP session. Possible values range from 1 to 65535. The default value is 16. This argument is available when you specify -mpls_protocol RSVP.

-mpls_rsvp_max_label
Defines the maximum label number used by the RSVP session. Possible values range from 1 to 65535. The default value is 65535. This argument is available when you specify -mpls_protocol RSVP.

-mpls_rsvp_graceful_restart_enable
Enables or disables graceful restart for RSVP. Possible values are false (disable) and true (enable). The default value is false.

-mpls_rsvp_recover_time
Specifies the length of time (in milliseconds) that the sender wants the recipient to re-synchronize RSVP and MPLS forwarding state with the sender, after the re-establishment of Hello synchronization. Possible values range from 0 to 4294967295. The default value is 0. This argument is available when -mpls_rsvp_graceful_restart_enable is set to true.

-mpls_rsvp_restart_time
Specifies the amount of time (in milliseconds) it takes the sender of the object to restart its RSVP component and the communication channel used for RSVP communication. Possible values are 0 to 4294967295. The default value is 3000. This argument is available when -mpls_rsvp_graceful_restart_enable is set to true.

-mpls_rsvp_bfd_enable
Enables or disables BFD on RSVP interfaces. Possible values are true (enable) and false (disable). The default value is false.

-mpls_rsvp_request_conf
Determines whether to include an RESV_CONFIRM object in the RESV message. Possible values are true and false. When it is set to true, an RESV_CONFIRM object will be included in the RESV message. The default value is false.

-mpls_rsvp_hello_enable
Enables or disables Hello packets for RSVP sessions. Possible values are true (enable) and false (disable). The default value is false.

-mpls_rsvp_hello_interval
Specifies the interval between RSVP Hello packets. Possible values range from 1 to 2147483647. The default value is 1000. This argument is available when -mpls_rsvp_hello_enable is set to true.

-mpls_rsvp_bundle_interval
Specifies the time interval (in milliseconds) to wait before sending queued messages. Messages are held in a buffer and are sent out as a bundle after the interval (in ms) expires or when message size exceeds the MTU. Possible values range from 1 to 2147483647. The default value is 1000.

-mpls_rsvp_summary_refresh_interval
Specifies the time interval (in milliseconds) to gather refresh messages that would have been sent out individually. Possible values range from 1 to 2147483647. The default value is 9000.

-mpls_rsvp_inter_packet_delay
Specifies the time delay (in milliseconds) between transmitted RSVP packets. Possible values range from 0 to 2147483647. The default value is 30.

-mpls_rsvp_refresh_interval
Specifies the time interval for a PATH and RESV message to be sent out to the path receiver to refresh the PATH/RESV state along each hop of the path. Possible values range from 1 to 2147483647. The default value is 30000.

-mpls_rsvp_refresh_delivery
Enables or disables reliable delivery for RSVP sessions. Possible values are true (enable) and false (disable).
The default value is false.

- **mpls_rsvp_retrans_interval**
  Specifies the initial retransmission interval (in milliseconds) for unacknowledged messages. Possible values range from 1 to 2147483647. The default value is 500.

- **mpls_rsvp_retrans_limit**
  Specifies the maximum number of times a message is transmitted without being acknowledged. Possible values range from 0 to 10. The default value is 3.

- **mpls_rsvp_retrans_delta**
  Specifies the multiplier by which the retransmission interval is increased each time an unacknowledged message is retransmitted. Possible values range from 0 to 3. The default value is 1.

- **mpls_ldp_hello_type**
  Specifies the type of Hello packets for LDP. Possible values are:
  
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>The Peer IP address is the DUT interface address. Used to locate directly connected neighbors.</td>
</tr>
<tr>
<td>targeted</td>
<td>The Peer IP address is the DUT loopback address. Used to locate neighbors which are not directly connected.</td>
</tr>
</tbody>
</table>

  This argument is available when you specify -mpls_protocol LDP.

- **mpls_ldp_transport_mode**
  Specifies the mode of the LDP Transport Address TLV. Possible values are:
  
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>The Transport Address TLV will not be included in LDP Hello messages</td>
</tr>
<tr>
<td>tester_ip</td>
<td>The LSR will take the emulated router interface address as the transport address and include the Transport Address TLV in LDP Hello messages</td>
</tr>
<tr>
<td>router_id</td>
<td>The LSR will take the emulated router ID, that is, the loopback address as the transport address and include the Transport Address TLV in LDP Hello messages</td>
</tr>
</tbody>
</table>

  The default value is tester_ip. This argument is available when you specify -mpls_protocol LDP.

- **mpls_ldp_hello_interval**
  Specifies the amount of time, in seconds, between Hello messages in an LDP session. Possible values range from 1 to 21845. The default value is 5. This argument is available when you specify -mpls_protocol LDP.

- **mpls_ldp_keepalive_interval**
  Specifies the amount of time, in seconds, between KEEPALIVE messages. Possible values range from 1 to 21845. The default value is 60. This argument is available when you specify -mpls_protocol LDP.

- **mpls_ldp_egress_label**
  Specifies the emulated label to be advertised by the emulated peer. Possible values are described below:
  
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>next_available</td>
<td>Advertises the next available label</td>
</tr>
<tr>
<td>implicit_null</td>
<td>Advertises label 3, the implicit null label</td>
</tr>
<tr>
<td>explicit_null</td>
<td>Advertises label 9, the explicit null label</td>
</tr>
</tbody>
</table>

  The default value is next_available. This argument is available when you specify -mpls_protocol LDP.
-mpls_ldp_min_label
Defines the minimum label number used by the LDP session. Possible values range from 1 to 65535. The
default value is 16. This argument is available when you specify -mpls_protocol LDP.

-mpls_ldp_graceful_restart_enable
Enables or disables graceful restart for LDP sessions. Possible values are true (enable) and false (disable). The
default value is false. This argument is available when you specify -mpls_protocol LDP.

-mpls_ldp_recover_time
Specifies the length of time (in milliseconds) that the sender desires for the recipient to re-synchronize LDP and
MPLS forwarding state with the sender, after the re-establishment of Hello synchronization. Possible values are
0 to 4294967. The default value is 140. This argument is available when -mpls_ldp_graceful_restart_enable is
set to true.

-mpls_ldp_reconnect_time
Specifies the amount of time, in seconds, it takes Spirent HLTAPI to reconnect after a graceful restart. To
use this argument, you must set -mpls_ldp_graceful_restart_enable to true and specify a value for the
-mpls_ldp_recover_time argument. Possible values range from 0 to 4294967. The default value is 60.

-mpls_ldp_bfd_enable
Enables or disables BFD on LDP interfaces. Possible values are true (enable) and false (disable). The default
value is false. This argument is available when -mpls_protocol is set to LDP.

-mpls_ldp_label_adv_mode
Specifies the label advertisement mode for LDP sessions. Possible values are downstream_unsolicited and
downstream_on_demand. The default value is downstream_on_demand.

-mpls_ldp_auth_mode
Specifies the authentication type for LDP. Possible values are:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No authentication</td>
</tr>
<tr>
<td>md5</td>
<td>MD5 authentication</td>
</tr>
</tbody>
</table>

The default value is none.

-mpls_ldp_auth_password
Specifies the password used for LDP authentication. This argument is available when -mpls_ldp_auth_mode is
set to md5. The default value is “Spirent”.

-mpls_ospf_sr_algorithms
A comma-separated list of integers to specify the algorithm to calculate the reachability to other nodes or to
prefixes attached to these nodes. Possible values range from 0 to 255. The default value is 0. This argument is
available when -mpls_protocol is set to OSPF.

-mpls_ospf_sid_base
Specifies the base value for the SID/Label range. Possible values range from 0 to 4294967295. The default
value is 100. This argument is available when -mpls_protocol is set to OSPF.

-mpls_ospf_sid_range
Specifies the size of the SID/Label range for OSPF SR. Possible values range from 0 to 65535. The default
value is 100. This argument is available when -mpls_protocol is set to OSPF.

-mpls_ospf_node_sid_index
Specifies the index value for the SID sub-TLV of OSPF SR. Possible values range from 0 to 4294967295. The
default value is 0. This argument is available when -mpls_protocol is set to OSPF.

-mpls_ospf_node_sid_index_step
Specifies the increment value with which to create subsequent SID indexes of ISIS SR. Possible values range
from 0 to 4294967295. The default value is 1. This argument is available when -mpls_protocol is set to OSPF.
-mpls_isis_sr_algorithm
Specifies the ISIS SR algorithm, in string format. The default value is 0. This argument is available when
-mpls_protocol is set to ISIS.

-mpls_isis_sid_base
Specifies the base value for the SID/Label range of OSPF SR. Possible values range from 0 to 4294967295. The
default value is 100. This argument is available when -mpls_protocol is set to ISIS.

-mpls_isis_sid_range
Specifies the size of the SID/Label range for OSPF SR. Possible values range from 0 to 65535. The default
value is 100. This argument is available when -mpls_protocol is set to ISIS.

-mpls_isis_node_sid_index
Specifies the index value for the SID sub-TLV of ISIS SR. Possible values range from 0 to 4294967295. The
default value is 0. This argument is available when -mpls_protocol is set to ISIS.

-mpls_isis_node_sid_index_step
Specifies the increment value with which to create subsequent SID indexes of the ISIS SR. Possible values range
from 0 to 4294967295. The default value is 1. This argument is available when -mpls_protocol is set to ISIS.

-p_router_enable
Enables or disables the emulation of provider (P) routers in the test. Possible values are true and false. When it
is set to false, only provider edge routers will be emulated or simulated. The default value is true.

-p_router_num_per_subif
Specifies the number of P routers per sub-interface on the provider side. Only one emulated P router can be
created per sub-interface. If this number is greater than 1, the additional P routers are simulated through the IGP
protocol routes. The topology for the additional P routers is determined by the -p_router_topology_type option.
Possible values range from 1 to 65535. The default value is 1. This argument is available when -p_router_enable
is set to true.

-p_router_topology_type
Defines the topology of the provider network. Possible values are tree and grid. The default value is tree.

-p_router_id_start
Defines the first loopback address of emulated P routers. The value must be in IPv4 format. The default value
is 192.0.1.1. This argument is available when -p_router_enable is set to true.

-p_router_id_step
Specifies the step value by which to generate additional loopback addresses for the emulated P routers. The
value must be in IPv4 format. The default value is 0.0.1.0. This argument is available when -p_router_enable is
set to true.

-p_router_ipv4_addr
Specifies the starting IPv4 interface address of the emulated P routers. The default value is 1.0.0.1. This
argument is available when -p_router_enable is set to true.

-p_router_ipv4_prefix_len
Specifies the IP prefix length on the simulated P router. Possible values range from 0 to 32. The default value is
24. This argument is available when -p_router_enable is set to true.

-pe_router_num_per_subif
Defines the number of PE routers created on each provider sub-interface. Possible values range from 1 to 65535.
The default value is 1. This argument is available when -p_router_enable is set to true.

-pe_router_id_start
Specifies the starting IPv4 address for the PE router. The default is 10.0.0.2. This argument is available when
-p_router_enable is set to true.
-pe_router_id_step
Defines the step size by which the provider-side PE router is incremented. The default value is 0.0.0.1. This argument is available when -p_router_enable is set to true.

-vpn_6vpe_enable
Determines whether to use 6PE or 6VPE in the test. Possible values are true (6VPE) and false (6PE). The default value is false.

-bgp_route_reflector_enable
Enables or disables route reflectors on the core side. Possible values are true (enable) and false (disable). The default value is false.

-bgp_route_reflector_per_subif
Specifies the number of route reflectors per provider sub-interface. Possible values range from 1 to 65535. The default is 1. This argument is available when -bgp_route_reflector_enable is set to true.

-bgp_route_reflector_per_pe
Specifies the number of route reflectors per PE router. Possible values range from 0 to 65535. The default value is 1. This argument is available when -bgp_route_reflector_enable is set to true.

-bgp_route_reflector_id_start
Specifies the starting loopback IPv4 address of route reflectors. The default value is 7.7.7.7. This argument is available when -bgp_route_reflector_enable is set to true.

-bgp_route_reflector_id_step
The amount by which to increment the loopback IP address (-bgp_route_reflector_loopback_ipv4_addr) for each subsequent route reflector. The value must be in IPv4 format. The default value is 0.0.0.1. This argument is available when -bgp_route_reflector_enable is set to true.

-bgp_route_reflector_cluster_id
Specifies the starting cluster ID for route reflectors. This ID enables route reflectors to recognize route updates from route reflectors in the same cluster. The default value is 0.0.0.0. This argument is available when - bgp_route_reflector_enable is set to true.

-bgp_route_reflector_cluster_id_step
The amount by which to increment the cluster ID (-bgp_route_reflector_cluster_id) for each subsequent route reflector. The default value is 0.0.0.1. This argument is available when -mpls_protocol is set to BGP.

-bgp_route_reflector_ids
Specifies the BGP route reflector ID. The value must be in IPv4 format. The default value is 0.0.0.0.

-bgp_route_reflector_mode
Specifies the BGP reflector mode. Possible values are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dut_as_rr</td>
<td>Specify the DUT as the route reflector</td>
</tr>
<tr>
<td>stc_as_rr</td>
<td>Specify Spirent TestCenter as the route reflector</td>
</tr>
</tbody>
</table>

The default value is stc_as_rr. This argument is available when -mpls_protocol is set to BGP.

-bgp_bfd_enable
Enables or disables BFD on BGP interfaces. Possible values are true (enable) and false (disable). The default value is false. This argument is available when -mpls_protocol is set to BGP.

-vrf_count
Specifies the number of VPN Routing and Forwarding tables (VRFs) to be configured. Possible values range from 1 to 65535. The default is 1.

-vrf_rd_assignment
Specifies the route distinguisher assignment mode. Possible values are:
use_rt | Use the route target field for all route distinguishers in the VPN

manual | Manually configure route distinguishers

The default value is use_rt.

-vrf_route_target_start
Specifies the starting route target for the VPN, in the format of AS-Number:Value or IPv4-Address:Value. The default value is 1:00.

-vrf_route_target_step
Specifies the step size by which the route target is incremented. The value must be in the format of AS-Number:Value or IPv4-Address:Value. The default value is 1:00.

cust_vrf_assignment
Determines how VRFs are assigned to CE routers on the customer side. Possible values are:

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>round_robin</td>
<td>The first CE created is assigned to the first VRF. The second CE created is assigned to the second VRF, and so forth. When the specified number of VRFs is reached, the VRF assignment repeats from the first VRF.</td>
</tr>
<tr>
<td>sequential</td>
<td>CEs created are assigned to the first VRF until the calculated number of CEs per VRF is reached. Additional CEs are assigned to the second and subsequent VRFs in the same fashion.</td>
</tr>
</tbody>
</table>

cust_routing_protocol
Defines the interior gateway routing protocol to be used by CEs on the customer side. Possible values are bgp, ospf, rip, isis, and mixed. The default value is bgp.

cust_bgp_percent
Specifies the percentage of customer-side CEs using BGP. This argument is available when cust_routing_protocol is set to mixed. Possible values range from 0 to 100. The default value is 0.

cust_rip_percent
Specifies the percentage of customer-side CEs using RIP. This argument is available when cust_routing_protocol is set to mixed. Possible values range from 0 to 100. The default value is 0.

cust_ospf_percent
Specifies the percentage of customer-side CEs using OSPFv2. This argument is available when cust_routing_protocol is set to mixed. Possible values range from 0 to 100. The default value is 0.

cust_isis_percent
Specifies the percentage of customer-side CEs using IS-IS. This argument is available when cust_routing_protocol is set to mixed. Possible values range from 0 to 100. The default value is 0.

cust_bgp_as
Specifies the starting BGP AS number on the customer side. Possible values range from 1 to 65535. The default value is 1.

cust_bgp_as_step_per_ce_enable
Enables or disables the step value for additional AS numbers across CE routers on the customer side. Possible values are true and false. The default value is false. This argument is available when cust_routing_protocol is set to BGP or mixed.
-cust_ce_bgp_as_step_per_ce
   Specifies the step value by which to generate additional AS numbers across CE routers on the customer side. Possible values range from 0 to 65535. The default value is 1. This argument is available when -cust_ce_bgp_as_step_per_ce_enable is set to true.

-cust_ce_bgp_as_step_per_vrf_enable
   Enables or disables the step value for additional CE AS numbers across VPNs on the customer side. Possible values are true (enable) and false (disable). The default value is true. This argument is available when -cust_ce_routing_protocol is set to BGP or mixed.

-cust_ce_bgp_as_step_per_vrf
   Specifies the step value by which to generate additional CE AS numbers across VPNs on the customer side. Possible values range from 0 to 65535. The default value is 1. This argument is available when -cust_ce_bgp_as_step_per_vrf_enable is set to true.

-cust_ce_bgp_4byte_as_enable
   Enables or disables 4-byte AS numbers on the customer side. Possible values are true (enable) and false (disable). The default value is false. This argument is available when -cust_ce_routing_protocol is set to bgp or mixed.

-cust_ce_bgp_4byte_as
   Specifies the starting CE 4-byte AS number on the customer side. The default value is 1:01. This argument is available when -cust_ce_bgp_4byte_as_enable is set to true.

-cust_ce_bgp_4byte_as_step_per_ce_enable
   Enables or disables the step value for additional CE 4-byte AS numbers across CE routers on the customer side. Possible values are true (enable) and false (disable). The default value is false. This argument is available when -cust_ce_routing_protocol is set to bgp or mixed and -cust_ce_bgp_4byte_as_enable is set to true.

-cust_ce_bgp_4byte_as_step_per_ce
   Specifies the step value by which to generate additional CE 4-byte AS numbers across CE routers on the customer side. Possible values range from 0 to 65535. The default value is 1. This argument is available when -cust_ce_bgp_4byte_as_step_per_ce_enable is set to true.

-cust_ce_bgp_4byte_as_step_per_vrf_enable
   Enables or disables the step value for additional CE 4-byte AS numbers across VPNs on the customer side. Possible values are true (enable) and false (disable). The default value is true. This argument is available when -cust_ce_routing_protocol is set to bgp or mixed and -cust_ce_bgp_4byte_as_enable is set to true.

-cust_ce_bgp_4byte_as_step_per_vrf
   Specifies the step value by which to generate additional CE 4-byte AS numbers across VPNs on the customer side. Possible values range from 0 to 65535. The default value is 1. This argument is available when -cust_ce_bgp_4byte_as_step_per_vrf_enable is set to true.

-cust_rd_start
   Specifies the starting route distinguisher on the customer side. This argument is available when -vrf_rd_assignment is set to MANUAL. The default value is 1:0.

-cust_rd_step_per_vrf_enable
   Enables or disables the step value for additional customer-side route distinguishers per VPN. Possible values are true and false. The default value is true.

-cust_rd_step_per_vrf
   Specifies the step value by which to generate additional customer-side route distinguishers per VPN. The default value is 1:0.

-cust_rd_step_per_ce_enable
   Enables or disables the step value for additional customer-side route distinguishers per CE. Possible values are true and false. The default value is false.
-cust_rd_step_per_ce
Specifies the step value by which to generate additional customer-side route distinguishers per CE. The default value is 0:0. This argument is available when -cust_rd_step_per_ce_enable is set to true.

-cust_route_count_per_ce
Specifies the number of routes that will be added to each customer-side CE. The default value is 1.

-provider_pe_vrf_assignment
Specifies how VPNs are assigned to PE routers. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn_per_pe</td>
<td>VPNs will be distributed across a set of PEs</td>
</tr>
<tr>
<td>pe_per_vpn</td>
<td>PEs will be distributed across a set of VPNs</td>
</tr>
</tbody>
</table>

The default value is vpn_per_pe.

-provider_pe_vrf_count
Specifies the number of items (VPNs or PEs) assigned to each target (VPN or PE). When -provider_pe_vrf_assignment is set to vpn_per_pe, this argument indicates the number of VPNs assigned to each PE, and possible values range from 1 to the number of VPNs. When -provider_pe_vrf_assignment is set to pe_per_vpn, this argument indicates the number of PEs assigned to each VPN, and possible values range from 1 to the number of PEs. The default value is 1.

If the value is less than the maximum number of items, and there is more than one target, the specified number of items are assigned in a round-robin fashion to each target. This argument is available when -provider_pe_vrf_all_assign is set to false.

-provider_pe_vrf_all_assign
Determines whether each PE uses all VPNs. Possible values are true and false. If it is set to false, you can manually set the number of VPNs that each PE will advertise routes for. The default value is false.

-provider_ce_bgp_as_enable
Enables or disables BGP AS numbers for CEs on the provider side. Possible values are true (enable) and false (disable). The default value is false.

-provider_ce_bgp_as
Specifies the starting BGP AS number on the provider side. Possible values range from 1 to 65535. The default value is 1. This argument is available when -provider_ce_bgp_as_enable is set to true.

-provider_ce_bgp_as_step_per_ce_enable
Enables or disables the step value for additional CE BGP AS numbers across CEs on the provider side. Possible values are true (enable) and false (disable). The default value is false.

-provider_ce_bgp_as_step_per_ce
Specifies the step value by which to generate additional CE BGP AS numbers across CEs on the provider side. Possible values range from 1 to 65535. The default value is 1. This argument is available when -provider_ce_bgp_as_step_per_ce_enable is set to true.

-provider_ce_bgp_as_step_per_vrf_enable
Enables or disables the step value for additional CE BGP AS numbers across VPNs on the provider side. Possible values are true (enable) and false (disable). The default value is true.

-provider_ce_bgp_as_step_per_vrf
Specifies the step value by which to generate additional CE BGP AS numbers across VPNs on the provider side. Possible values range from 1 to 65535. The default value is 1.

-provider_ce_bgp_4byte_as_enable
Enables or disables 4-byte AS numbers for CE routers on the provider side. Possible values are true (enable) and false (disable). The default value is false.
-provider_ce_bgp_4byte_as
  Defines the first 4-byte AS number for CEs on the provider side. The default value is 1:01. This argument is available when -provider_ce_bgp_4byte_as_enable is set to true.

-provider_ce_bgp_4byte_as_step_per_ce_enable
  Enables or disables the step value for additional CE 4-byte AS numbers across CEs on the provider side. Possible values are true (enable) and false (disable). The default value is false.

-provider_ce_bgp_4byte_as_step_per_ce
  Specifies the step value by which to generate additional CE 4-byte AS numbers across CEs on the provider side. Possible values range from 1 to 65535. The default value is 1. This argument is available when -provider_ce_bgp_4byte_as_step_per_ce_enable is set to true.

-provider_ce_bgp_4byte_as_step_per_ce
  Specifies the step value for additional CE 4-byte AS numbers across CE routers on the provider side. Possible values range from 0 to 65535. The default value is 1. This argument is available when -provider_ce_bgp_4byte_as_step_per_ce_enable is set to true.

-provider_ce_bgp_4byte_as_step_per_vrf_enable
  Enables or disables the step value for additional CE 4-byte AS numbers per VPN on the provider side. Possible values are true (enable) and false (disable). The default value is true.

-provider_ce_bgp_4byte_as_step_per_vrf
  Specifies the step value by which to generate additional CE 4-byte AS numbers across VPNs on the provider side. Possible values range from 1 to 65535. The default value is 1.

-provider_rd_start
  Specifies the starting route distinguisher for provider sites. The default value is 1:0.

-provider_rd_step_per_vrf_enable
  Enables or disables the step value for additional route distinguishers per VPN on the provider side. Possible values are true (enable) and false (disable). The default value is true.

-provider_rd_step_per_vrf
  Specifies the step value by which to generate additional route distinguishers across VPNs on the provider side. The default value is 1:0.

-provider_rd_step_per_ce_enable
  Enables or disables the step value for additional route distinguishers across CE routers on the provider side. Possible values are true (enable) and false (disable). The default value is false.

-provider_rd_step_per_ce
  Specifies the step value by which to generate additional route distinguishers across CE routers on the provider side. The default value is 0:0.

-cust_ipv6_vpn_route_start
  Specifies the first IPv6 route advertised by emulated CE routers. The value must be in IPv6 format. The default value is 2001::.

-cust_ipv6_vpn_route_step
  Identifies which part of the IPv6 address to increment for subsequent routes on the customer side. The default value is 1.

-cust_ipv6_vpn_route_prefix_len
  Identifies the IPv6 network portion of the starting route identifier on the customer side. Possible values range from 1 to 128. The default value is 64.

-cust_ipv6_vpn_route_overlap
  Determines how routes are advertised on the customer side. Possible values are true and false. When set to true, all VPNs advertise the same routes. When set to false, each VPN advertises unique routes. The default value is false.
**-cust_ipv6_ce_route_type**

Specifies the type of IPv6 routes to be advertised by emulated CEs on the customer side. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>The route and the CE that advertise the route are in the same AS</td>
</tr>
<tr>
<td>external</td>
<td>The route and the CE that advertise the route are not in the same AS</td>
</tr>
</tbody>
</table>

The default value is internal. This argument is available when `-cust_ce_routing_protocol` is set to OSPF or ISIS.

**-provider_ipv6_vpn_route_start**

Specifies the first IPv6 route advertised by emulated PE routers on the provider side. The value must be in IPv6 format. The default value is 2001::.

**-provider_ipv6_vpn_route_step**

Identifies which part of the IPv6 address to increment for subsequent routes on the provider side. The default value is 1.

**-provider_ipv6_vpn_route_prefix_len**

Identifies the IPv6 network portion of the starting route identifier on the provider side. Possible values range from 1 to 128. The default value is 64.

**-provider_ipv6_vpn_route_overlap**

Determines how routes are advertised on the provider side. Possible values are true and false. When set to true, all VPNs advertise the same routes. When set to false, each VPN advertises unique routes. The default value is false.

**-provider_route_count_per_ce**

Specifies the number of routes that will be added to each CE router on the provider side. The default value is 1.

**-vrf_route_mpls_label_type**

Defines the method by which labels are assigned within a traffic block. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label_per_site</td>
<td>All routes in one traffic route are advertised with the same label</td>
</tr>
<tr>
<td>label_per_route</td>
<td>Each route in one traffic route is advertised with a unique label</td>
</tr>
</tbody>
</table>

The default value is label_per_site.

**-vrf_route_mpls_label_start**

Specifies the first MPLS label to be assigned to VPN routes on the provider side. Possible values range from 1 to 1048575. The default value is 16.

**-traffic_flow_direction**

Specifies the type of traffic flows to create. This argument is available when `-traffic_enable` is set to true. Possible values are described below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cust_to_core</td>
<td>Traffic is created from the customer side to the core side</td>
</tr>
<tr>
<td>core_to_cust</td>
<td>Traffic is created from the core side to the customer side</td>
</tr>
<tr>
<td>bidirectional</td>
<td>Traffic is created from both directions</td>
</tr>
<tr>
<td>fully_meshed</td>
<td>Traffic is created in a fully meshed pattern</td>
</tr>
</tbody>
</table>

(continues on next page)
The default value is bidirectional.

**-traffic_pattern**

Specifies the traffic mapping method to be used within each host block. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>one_to_one</td>
<td>Every endpoint within the source endpoint block transmits traffic to the corresponding endpoint within the destination endpoint block</td>
</tr>
<tr>
<td>one_to_many</td>
<td>Every endpoint within the source endpoint block transmits traffic to all endpoints within the destination endpoint block</td>
</tr>
</tbody>
</table>

**-traffic_stream_group_method**

Determines how to aggregate streams in a streamblock. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregate</td>
<td>Aggregates all streams into a single streamblock</td>
</tr>
<tr>
<td>vpn</td>
<td>Aggregates all streams for a single VPN into a single stream block</td>
</tr>
</tbody>
</table>

**-traffic_use_single_stream_per_endpoint_pair**

Determines whether Spirent HLTAPI will assign a single stream ID to each endpoint pair. Possible values are true and false. The default value is false.

**-traffic_load_percent_provider**

Specifies the load percentage for test traffic from each provider-side port. Possible values range from 0 to 100. The default value is 10.

**-traffic_load_percent_cust**

Specifies the load percentage for test traffic from each customer-side port. Possible values range from 0 to 100. The default value is 10.

### 1.3.4 Return Values

Depending on the specific language that HLTAPI uses, the function returns a keyed list/dictionary/hash (See Introduction for more information on return value formats) using the following keys (with corresponding data):

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>handle</td>
<td>6PE/6VPE network configuration handle created by this function</td>
</tr>
<tr>
<td>status</td>
<td>Success or Failure of the operation</td>
</tr>
<tr>
<td>log</td>
<td>Error message if command returns {status 0}</td>
</tr>
</tbody>
</table>

The following keys are returned when you specify -mode create:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ce_router</td>
<td>CE router handle</td>
</tr>
<tr>
<td>p_router</td>
<td>P router handle</td>
</tr>
<tr>
<td>rr_router</td>
<td>RR router handle</td>
</tr>
<tr>
<td>pe_router</td>
<td>PE router handle</td>
</tr>
<tr>
<td>vpn</td>
<td>VPN handle</td>
</tr>
<tr>
<td>ospf</td>
<td>OSPF SR handle</td>
</tr>
<tr>
<td>isis</td>
<td>ISIS SR handle</td>
</tr>
<tr>
<td>ldp</td>
<td>LDP handle</td>
</tr>
</tbody>
</table>
1.3.5 Description

The `sth::emulation_6pe_6vpe_config` function creates or deletes 6PE/6VPE network topologies, mapping the operations of the 6PE or 6VPE Wizard in the Spirent TestCenter GUI. Use the `-mode` argument to specify the action to perform.

Before you use the function, you must configure customer and provider test ports using the `sth::emulation_6pe_6vpe_cust_port_config` and `sth::emulation_6pe_6vpe_provider_port_config` functions.

If the operation fails, Spirent HLTAPI returns an error message.

1.3.6 Examples

The following example creates a 6VPE network topology:

```shell
sth::emulation_6pe_6vpe_config
  -mode create
  -dut_router_id 10.0.0.1
  -dut_as 2
  -dut_4byte_as_enable true
  -cust_use_ports_enable true
  -provider_use_ports_enable true
  -igp_protocol ospf
  -mpls_protocol ospf
  -igp_ospf_area_id 0.0.0.0
  -igp_ospf_network_type native
  -igp_ospf_router_priority 0
  -igp_ospf_interface_cost 1
  -igp_ospf_options 0x42
  -igp_ospf_auth_mode md5
  -igp_ospf_auth_password abc
  -igp_ospf_auth_md5_key 1
  -igp_ospf_bfd_enable true
  -p_router_enable true
  -vpn_6vpe_enable true
  -bgp_route_reflector_enable true
  -bgp_bfd_enable true
  -cust_ce_bgp_as_step_per_ce_enable true
  -cust_ce_bgp_as_step_per_vrf_enable true
  -cust_ce_bgp_4byte_as_enable true
  -cust_ce_bgp_4byte_as_step_per_ce_enable true
  -cust_ce_bgp_4byte_as_step_per_vrf_enable true
  -cust_rd_step_per_vrf_enable true
  -cust_rd_step_per_ce_enable true
  -provider_pe_vrf_all_assign true
  -provider_ce_bgp_as_enable true
  -provider_ce_bgp_as_step_per_ce_enable true
```

(continues on next page)
-provider_ce_bgp_as_step_per_vrf_enable true
-provider_ce_bgp_4byte_as_enable true
-provider_ce_bgp_4byte_as_step_per_ce_enable true
-provider_ce_bgp_4byte_as_step_per_vrf_enable true
-provider_rd_step_per_vrf_enable true
-provider_rd_step_per_vrf 1:1
-provider_rd_step_per_ce_enable true
-cust_ipv6 vpn route overlap true
-provider_ipv6 vpn route overlap true
-traffic_use_single_stream_per_endpoint_pair true

Sample output:

```json
{status 1} {handle {{vpn {vpnidgroup1 vpnidgroup2 vpnidgroup3 vpnidgroup4
vpnidgroup5 vpnidgroup6 vpnidgroup7 vpnidgroup8 vpnidgroup9 vpnidgroup10}}
{ce router {router1 router2 router3 router4 router5 router6 router7 router8 router9 router10 router11 router12 router13 router14 router15 router16 router17 router18 router19 router20} {p_router {router1 router2 router3 router4 router5 router6 router7 router8 router9 router10 router11 router12 router13 router14 router15 router16 router17 router18 router19} {rr_router {router1 router2 router3 router4 router5 router6 router7 router8 router9 router10 router11 router12 router13 router14 router15 router16 router17 router18 router19}} {pe_router {} {ospf {ospfv2routerconfig1 ospfv2routerconfig2 ospfv2routerconfig3
ospfv2routerconfig4 ospfv2routerconfig5 ospfv2routerconfig6 ospfv2routerconfig7
ospfv2routerconfig8 ospfv2routerconfig9 ospfv2routerconfig10}} {isis {} {ldp {}}} {rsvp {} {bgp {bgprouterconfig1 bgprouterconfig2 bgprouterconfig3
bgprouterconfig4 bgprouterconfig5 bgprouterconfig6 bgprouterconfig7
bgprouterconfig8 bgprouterconfig9 bgprouterconfig10 bgprouterconfig11
bgprouterconfig12 bgprouterconfig13 bgprouterconfig14 bgprouterconfig15
bgprouterconfig16 bgprouterconfig17 bgprouterconfig18 bgprouterconfig19
bgprouterconfig20}} {bfd {bfdrouterconfig1 bfdrouterconfig2 bfdrouterconfig3
bfdrouterconfig4 bfdrouterconfig5 bfdrouterconfig6 bfdrouterconfig7
bfdrouterconfig8 bfdrouterconfig9 bfdrouterconfig10 bfdrouterconfig11
bfdrouterconfig12 bfdrouterconfig13 bfdrouterconfig14 bfdrouterconfig15
bfdrouterconfig16 bfdrouterconfig17 bfdrouterconfig18 bfdrouterconfig19
bfdrouterconfig20}} {rip {}} {stream_id {streamblock1 streamblock2}}}}}
```

### 1.4 sth::emulation_6pe_6vpe_control

#### 1.4.1 Purpose

Spirent Extension (for Spirent HLTAPI only).

Starts or stops the specified 6PE/6VPE topology

#### 1.4.2 Synopsis

```
sth::emulation_6pe_6vpe_control
   -port_handle <port_handle> | -handle <handle>
   -action {start|stop}
```
1.4.3 Arguments:

- **port_handle**
  Specifies the port on which routers will start or stop. You must specify either -handle or -port_handle, but not both.

- **handle**
  Specifies the routers to start or stop. You must specify either -handle or -port_handle, but not both.

- **action**
  Specifies the action to performed. This argument is mandatory. Possible values are described below:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Starts the specified 6PE/6VPE network</td>
</tr>
<tr>
<td>stop</td>
<td>Stops the specified 6PE/6VPE network</td>
</tr>
</tbody>
</table>

1.4.4 Return Values

Depending on the specific language that HLTAPI uses, the function returns a keyed list/dictionary/hash (See Introduction for more information on return value formats) using the following keys (with corresponding data):

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Success (1) or failure (0) of the operation</td>
</tr>
<tr>
<td>log</td>
<td>An error message (if the operation failed)</td>
</tr>
</tbody>
</table>

1.4.5 Description

The **sth::emulation_6pe_6vpe_control** function controls the configured 6PE/6VPE topology. Use the -action argument to start or stop the test.

1.4.6 Examples

Sample Input:

```bash
sth::emulation_6pe_6vpe_control
  -port_handle $port1 $port2
  -action start
```

Sample Output:

```
{status 1}
```

1.5 sth::emulation_6pe_6vpe_info

1.5.1 Purpose

Spirent Extension (for Spirent HLTAPI only).
Retrieves statistics for the 6PE/6VPE test
1.5.2 Synopsis

```
sth::emulation_6pe_6vpe_info
   -handle <handle> | -port_handle <port_handle>
   -mode {rsvp|ldp|isis|ospfv2|ospfv3|bgp|rip|bfd|summary}
```

1.5.3 Arguments

- **-handle**
  Specifies the router from which to retrieve statistics. You must specify either -handle or -port_handle, but not both.

- **-port_handle**
  Specifies the port from which to retrieve statistics

- **-mode**
  Determines the protocol for which statistics will be retrieved. This argument is mandatory. Possible values are rsvp, ldp, isis, ospfv2, bgp, rip, bfd, and summary.

1.5.4 Return Values

Depending on the specific language that HLTAPI uses, the function returns a keyed list/dictionary/hash (See Introduction for more information on return value formats) using the following keys (with corresponding data):

```
status Success () or failure () of the operation
log An error message (if the operation failed)
```

The following keys are returned when you specify -mode rsvp:

```
EventInProgress Event in progress
TxPath Number of PATH messages sent
RxPath Number of PATH messages received
TxReservation Number of Reservation messages sent
RxReservation Number of Reservation messages received
TxPathError Number of PATH Error messages sent
RxPathError Number of PATH Error messages received
TxReservationError Number of Reservation Error messages sent
RxReservationError Number of Reservation Error messages received
TxReservationConfirmation Number of Reservation Confirm messages sent
RxReservationConfirmation Number of Reservation Confirm messages received
TxPathTeardown Number of PATH Tear Down messages sent
RxPathTeardown Number of PATH Tear Down messages received
TxReservationTeardown Number of Reservation Tear Down messages sent
RxReservationTeardown Number of Reservation Tear Down messages received
LspUpCount Number of LSPs in Up state
LspDownCount Number of LSPs in Down state
LspConnectingCount Number of LSPs in Connecting state
MinLspSetupTime Minimum time (in ms) to set up an LSP on the session
MaxLspSetupTime Maximum time (in ms) to set up an LSP on the session
AvgLspSetupTime Average time (in ms) to set up an LSP on the session
LastTxReservationErrorCode Reports the last Reservation Error message code sent
LastRxReservationErrorCode Reports the last Reservation Error message code received
LastTxPathErrorCode Reports the last PATH Error message code sent
```

(continues on next page)
LastRxPathErrorCode Reports the last PATH Error message code received
TxHello Number of Hello packets sent
RxHello Number of Hello packets received
TxPathRecovery Number of PATH Recovery packets sent
RxPathRecovery Number of PATH Recovery packets received
EgressLspUpCount Number of egress LSPs in Up state
TxNotify Number of Notify packets sent
RxNotify Number of Notify packets received
Timestamp Timestamp of the results

The following keys are returned when you specify -mode ldp:::

TxDirectHellosCount Number of direct Hellos sent
TxIpv4DirectHellosCount Number of IPv4 direct Hellos sent
TxIpv6DirectHellosCount Number of IPv6 direct Hellos sent
RxDirectHellosCount Number of direct Hellos received
RxIpv4DirectHellosCount Number of IPv4 direct Hellos received
RxIpv6DirectHellosCount Number of IPv6 direct Hellos received
TxTargetedHellosCount Number of targeted Hellos sent
TxIpv4TargetedHellosCount Number of IPv4 targeted Hellos sent
TxIpv6TargetedHellosCount Number of IPv6 targeted Hellos sent
RxTargetedHellosCount Number of targeted Hellos received
RxIpv4TargetedHellosCount Number of IPv4 targeted Hellos received
RxIpv6TargetedHellosCount Number of IPv6 targeted Hellos received
LspUpCount Number of LSPs in Up state
NumLspDownCount Number of LSPs in Down state
TxKeepAliveCount Number of Keepalives sent
RxKeepAliveCount Number of Keepalives received
TxLabelRequestsCount Number of Label Requests sent
RxLabelRequestsCount Number of Label Requests received
TxLabelMappingCount Number of Label Mapping messages sent
RxLabelMappingCount Number of Label Mapping messages received
TxLabelAbortCount Number of Label Abort requests sent
RxLabelAbortCount Number of Label Abort requests received
TxLabelWithdrawCount Number of Label Withdraw messages sent
RxLabelWithdrawCount Number of Label Withdraw messages received
TxLabelReleaseCount Number of Label Release messages sent
RxLabelReleaseCount Number of Label Release messages received
TxNotificationCount Number of Notification messages sent
RxNotificationCount Number of Notification messages received
TxAddrWithdrawCount Number of Address Withdraw messages sent
RxAddrWithdrawCount Number of Address Withdraw messages received
TxNotifyCode Notification code sent in string format
RxNotifyCode Notification code received in string format
LdpSessionVersion LDP session version

The following keys are returned when you specify -mode isis:

TpPtpHelloCount Number of point-to-point Hellos sent to the SUT
RxpPtpHelloCount Number of point-to-point Hellos received from the SUT
TxLlIlanHelloCount Number of LI Tx LAN Hellos sent to the SUT
RxLlIlanHelloCount Number of LI Rx LAN Hellos received from the SUT
TxLlLspCount Number of LI Tx LSPs sent to the SUT
RxLlLspCount Number of LI Rx LSPs received from the SUT
TxLlCsnpCount Number of LI Tx CSNPs sent to the SUT
RxLlCsnpCount Number of LI Rx CSNPs received from the SUT
TxLlPsnpCount Number of LI Tx PSNPs sent to the SUT
RxLlPsnpCount Number of LI Rx PSNPs received from the SUT

(continues on next page)
### HLTAPI Cmd Ref Documentation, Release 1

(continued from previous page)

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxL1PsnpCount</td>
<td>Number of L1 Rx PSNPs received from the SUT</td>
</tr>
<tr>
<td>TxL2LanHelloCount</td>
<td>Number of L2 Tx LAN Hellos sent to the SUT</td>
</tr>
<tr>
<td>RxL2LanHelloCount</td>
<td>Number of L2 Rx LAN Hellos received from the SUT</td>
</tr>
<tr>
<td>TxL2LspCount</td>
<td>Number of L2 Tx LSPs sent to the SUT</td>
</tr>
<tr>
<td>RxL2LspCount</td>
<td>Number of L2 Rx LSPs received from the SUT</td>
</tr>
<tr>
<td>TxL2CsnpCount</td>
<td>Number of L2 Tx CSNPs sent to the SUT</td>
</tr>
<tr>
<td>RxL2CsnpCount</td>
<td>Number of L2 Rx CSNPs received from the SUT</td>
</tr>
<tr>
<td>TxL2PsnpCount</td>
<td>Number of L2 Tx PSNPs sent to the SUT</td>
</tr>
<tr>
<td>RxL2PsnpCount</td>
<td>Number of L2 Rx PSNPs received from the SUT</td>
</tr>
<tr>
<td>AdjacencyLevel</td>
<td>Adjacency level</td>
</tr>
</tbody>
</table>

The following keys are returned when you specify `-mode ospfv2`:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxHello</td>
<td>Number of Hello packets sent by the emulated router</td>
</tr>
<tr>
<td>RxHello</td>
<td>Number of Hello packets received by the emulated router</td>
</tr>
<tr>
<td>TxRouterLsa</td>
<td>Number of Router LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxRouterLsa</td>
<td>Number of Router LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxNetworkLsa</td>
<td>Number of Network LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxNetworkLsa</td>
<td>Number of Network LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxSummaryLsa</td>
<td>Number of Summary LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxSummaryLsa</td>
<td>Number of Summary LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxAsbrSummaryLsa</td>
<td>Number of ASBR-Summary LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxAsbrSummaryLsa</td>
<td>Number of ASBR-Summary LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxAsExternalLsa</td>
<td>Number of External LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxAsExternalLsa</td>
<td>Number of External LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxNssaLsa</td>
<td>Number of NSSA LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxNssaLsa</td>
<td>Number of NSSA LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxAck</td>
<td>Number of LSA packets sent by the emulated router</td>
</tr>
<tr>
<td>RxAck</td>
<td>Number of LSA packets received by the emulated router</td>
</tr>
<tr>
<td>TxRequest</td>
<td>Number of LS Request packets sent by the emulated router</td>
</tr>
<tr>
<td>RxRequest</td>
<td>Number of LS Request packets received by the emulated router</td>
</tr>
<tr>
<td>TxUpdate</td>
<td>Number of Update messages sent</td>
</tr>
<tr>
<td>RxUpdate</td>
<td>Number of Update messages received</td>
</tr>
<tr>
<td>TxTlsa</td>
<td>Number of TE-LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxTlsa</td>
<td>Number of TE-LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxRiLsa</td>
<td>Number of Router Info LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxRiLsa</td>
<td>Number of Router Info LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxEplLsa</td>
<td>Number of Extended Prefix LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxEplLsa</td>
<td>Number of Extended Prefix LSAs received by the emulated router</td>
</tr>
<tr>
<td>TxElLsa</td>
<td>Number of Extended Link LSAs sent by the emulated router</td>
</tr>
<tr>
<td>RxElLsa</td>
<td>Number of Extended Link LSAs received by the emulated router</td>
</tr>
<tr>
<td>SessionUpCount</td>
<td>Session up count</td>
</tr>
</tbody>
</table>

(continues on next page)
### HLTAPI Cmd Ref Documentation, Release 1

(areaId | Area ID
ipv4SrcAddr | IPv4 source address

The following keys are returned when you specify `-mode ospfv3`:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxHello</td>
<td>Number of Hello packets sent</td>
</tr>
<tr>
<td>RxHello</td>
<td>Number of Hello packets received</td>
</tr>
<tr>
<td>TxDd</td>
<td>Number of Database Description packets sent</td>
</tr>
<tr>
<td>RxDd</td>
<td>Number of Database Description packets received</td>
</tr>
<tr>
<td>TxRouterLsa</td>
<td>Number of Router LSAs sent</td>
</tr>
<tr>
<td>RxRouterLsa</td>
<td>Number of Router LSAs received</td>
</tr>
<tr>
<td>TxNetworkLsa</td>
<td>Number of Network LSAs sent</td>
</tr>
<tr>
<td>RxNetworkLsa</td>
<td>Number of Network LSAs received</td>
</tr>
<tr>
<td>TxSummaryLsa</td>
<td>Number of Summary LSAs sent</td>
</tr>
<tr>
<td>RxSummaryLsa</td>
<td>Number of Summary LSAs received</td>
</tr>
<tr>
<td>TxAsbrSummaryLsa</td>
<td>Number of ASBR-Router LSAs sent</td>
</tr>
<tr>
<td>RxAsbrSummaryLsa</td>
<td>Number of ASBR-Router LSAs received</td>
</tr>
<tr>
<td>TxAsExternalLsa</td>
<td>Number of External LSAs sent</td>
</tr>
<tr>
<td>RxAsExternalLsa</td>
<td>Number of External LSAs received</td>
</tr>
<tr>
<td>TxNssaLsa</td>
<td>Number of NSSA LSAs sent</td>
</tr>
<tr>
<td>RxNssaLsa</td>
<td>Number of NSSA LSAs received</td>
</tr>
<tr>
<td>TxAck</td>
<td>Number of LSA packets sent</td>
</tr>
<tr>
<td>RxAck</td>
<td>Number of LSA packets received</td>
</tr>
<tr>
<td>TxRequest</td>
<td>Number of LS Request packets sent</td>
</tr>
<tr>
<td>RxRequest</td>
<td>Number of LS Request packets received</td>
</tr>
<tr>
<td>TxUpdate</td>
<td>Number of Update messages sent</td>
</tr>
<tr>
<td>RxUpdate</td>
<td>Number of Update messages received</td>
</tr>
<tr>
<td>TxIntraAreaPrefixLsa</td>
<td>Number of Intra-Area-Prefix LSAs sent</td>
</tr>
<tr>
<td>RxIntraAreaPrefixLsa</td>
<td>Number of Intra-Area-Prefix LSAs received</td>
</tr>
<tr>
<td>TxInterAreaPrefixLsa</td>
<td>Number of inter-area-prefix LSAs sent</td>
</tr>
<tr>
<td>RxInterAreaPrefixLsa</td>
<td>Number of inter-area-prefix LSAs received</td>
</tr>
<tr>
<td>TxInterAreaRouterLsa</td>
<td>Number of inter-area-router LSAs sent</td>
</tr>
<tr>
<td>RxInterAreaRouterLsa</td>
<td>Number of inter-area-router LSAs received</td>
</tr>
<tr>
<td>TxLinkLsa</td>
<td>Number of link LSAs sent</td>
</tr>
<tr>
<td>RxLinkLsa</td>
<td>Number of link LSAs received</td>
</tr>
<tr>
<td>TxNssaLsa</td>
<td>Number of NSSA LSAs sent</td>
</tr>
<tr>
<td>RxNssaLsa</td>
<td>Number of NSSA LSAs received</td>
</tr>
<tr>
<td>TxERouterLsa</td>
<td>Number of Extended Router LSAs sent</td>
</tr>
<tr>
<td>RxERouterLsa</td>
<td>Number of Extended Router LSAs received</td>
</tr>
<tr>
<td>TxENetworkLsa</td>
<td>Number of Extended Network LSAs sent</td>
</tr>
<tr>
<td>RxENetworkLsa</td>
<td>Number of Extended Network LSAs received</td>
</tr>
<tr>
<td>TxEIntraAreaPrefixLsa</td>
<td>Number of Extended Intra-Area Prefix LSAs sent</td>
</tr>
<tr>
<td>RxEIntraAreaPrefixLsa</td>
<td>Number of Extended Intra-Area Prefix LSAs received</td>
</tr>
<tr>
<td>TxEInterAreaPrefixLsa</td>
<td>Number of Extended Inter-Area Prefix LSAs sent</td>
</tr>
<tr>
<td>RxEInterAreaPrefixLsa</td>
<td>Number of Extended Inter-Area Prefix LSAs received</td>
</tr>
<tr>
<td>TxEInterAreaRouterLsa</td>
<td>Number of Extended Inter-Area Router LSAs sent</td>
</tr>
<tr>
<td>RxEInterAreaRouterLsa</td>
<td>Number of Extended Inter-Area Router LSAs received</td>
</tr>
<tr>
<td>TxELinkLsa</td>
<td>Number of Extended Link LSAs sent</td>
</tr>
<tr>
<td>RxELinkLsa</td>
<td>Number of Extended Link LSAs received</td>
</tr>
</tbody>
</table>

The following keys are returned when you specify `-mode bgp`:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxAdvertisedRouteCount</td>
<td>Total cumulative feasible routes the emulated router has sent out in all UPDATE packets</td>
</tr>
<tr>
<td>RxAdvertisedRouteCount</td>
<td>Total cumulative feasible routes received by the emulated router</td>
</tr>
</tbody>
</table>
| TxWithdrawnRouteCount | Total number of unfeasible routes the emulated router
has sent out in all UPDATE packets

**RxWithdrawnRouteCount** Total cumulative unfeasible routes received by the emulated router

**TxNotificationCount** Number of Notification packets sent from the emulated router

**RxNotificationCount** Number of Notification packets received by the emulated router

**TxAdvertisedUpdateCount** Total number of UPDATE packets with feasible routes sent to the DUT

**RxAdvertisedUpdateCount** Number of Update packets received from DUT

**RxWithdrawnUpdateCount** Total number of UPDATE packets with unfeasible routes sent to the DUT (route flapping)

**TxKeepAliveCount** Total number of KEEPALIVE packets sent to the DUT

**RxKeepAliveCount** Total number of KEEPALIVE packets received from the DUT during the test

**TxOpenCount** Total number of OPEN packets sent to the DUT

**RxOpenCount** BGP Open messages received from DUT

**TxRouteRefreshCount** Number of advertised Route Refresh messages transmitted

**RxRouteRefreshCount** Number of advertised Route Refresh messages received

**OutstandingRouteCount** Number of routes that should be in the DUT's current route table

**LastRxUpdateRouteCount** Number of routes in the last-received UPDATE message

**TxNotifyCode** Last Notification code the emulated router sent to the DUT

**TxNotifySubCode** Sub-code for the last Notification sent to the DUT

**RxNotifyCode** Last Notification code the emulated router received from the DUT

**RxNotifySubCode** Sub-code for the last Notification received from the DUT

**TxRtConstraintCount** Number of RT-Constraint routes sent for this router

**RxRtConstraintCount** Number of RT-Constraint routes received for this router

**SessionUpCount** Number of router sessions within the router block in Established state

The following keys are returned when you specify -mode rip:

**TxAdvertisedUpdateCount** Number of advertised routes sent by the emulated router

**RxAdvertisedUpdateCount** Number of advertised routes received by the emulated router

**TxWithdrawnUpdateCount** Number of unreachable (metric 16) routes sent by the emulated router

**RxWithdrawnUpdateCount** Number of unreachable (metric 16) routes received by the emulated router

The following keys are returned when you specify -mode bfd:

**TimeoutCount** Number of timeout conditions detected by BFD

**FlapCount** Number of times a flap event was detected by BFD

**TxCount** Number of BFD packets sent on this router

**RxCount** Number of BFD packets received on this router

The following keys are returned when you specify -mode summary:

**ldp_summaryportxSessionDownCount** Number of routers in SessionDown state

**ldp_summaryportxSessionUpCount** Number of routers in SessionUp state

**ldp_summaryportxSessionFailedCount** Number of routers in SessionFailed state

**ldp_summaryportxSessionOpenCount** Number of routers in SessionOpen state

**ldp_summaryportxSessionConnectCount** Number of routers in SessionConnect state

**ldp_summaryportxSessionRestartCount** Number of routers in SessionRestart state
### 1.5.5 Description

The `sth::emulation_mvpn_info` function provides information about the configured 6PE/6VPE network topology.

### 1.5.6 Examples

The following example retrieves OSPFv2 statistics from a specified router:
sth::emulation_6pe_6vpe_info
  -handle $routerList
  -mode ospfv2]

Sample output:

```json
{ospf_results
  {port1
    {router1
      {TxHello 2} {RxHello 0} {TxDd 0} {RxDd 0}
      {TxRouterLsa 0} {RxRouterLsa 0} {TxNetworkLsa 0} {RxNetworkLsa 0} {TxSummaryLsa 0} {RxSummaryLsa 0} {TxAsbrSummaryLsa 0} {RxAsbrSummaryLsa 0} {TxAsExternalLsa 0} {RxAsExternalLsa 0} {TxNSSalSa 0} {RxNSSalSa 0} {TxAck 0} {RxAck 0} {TxRequest 0} {RxRequest 0} {TxUpdate 0} {RxUpdate 0} {TxTeLsa 0} {RxTeLsa 0} {TxRiLsa 0} {RxRiLsa 0} {TxEpLsa 0} {RxEpLsa 0} {TxE1Lsa 0} {RxE1Lsa 0} {SessionUpCount 0} {areaId 0.0.0.0} {ipv4SrcAddr 192.85.1.2})} {status 1}
```
CHAPTER 2

Indices and tables

- modindex
- search
Symbols

- action
  command line option, 29
- bgp_bfd_enable
  command line option, 20
- bgp_route_reflector_cluster_id
  command line option, 20
- bgp_route_reflector_cluster_id_step
  command line option, 20
- bgp_route_reflector_enable
  command line option, 20
- bgp_route_reflector_id_start
  command line option, 20
- bgp_route_reflector_id_step
  command line option, 20
- bgp_route_reflector_ids
  command line option, 20
- bgp_route_reflector_mode
  command line option, 20
- bgp_route_reflector_per_pe
  command line option, 20
- bgp_route_reflector_per_subif
  command line option, 20
- cust_ce_bgp_4byte_as
  command line option, 22
- cust_ce_bgp_4byte_as_enable
  command line option, 22
- cust_ce_bgp_4byte_as_step_per_ce
  command line option, 22
- cust_ce_bgp_4byte_as_step_per_ce_enable
  command line option, 22
- cust_ce_bgp_4byte_as_step_per_vrf
  command line option, 22
- cust_ce_bgp_4byte_as_step_per_vrf_enable
  command line option, 22
- cust_ce_bgp_as_step_per_ce
  command line option, 21
- cust_ce_bgp_as_step_per_vrf
  command line option, 22
- cust_ce_bgp_as_step_per_vrf_enable
  command line option, 22
- cust_ce_bgp_percent
  command line option, 21
- cust_ce_isis_percent
  command line option, 21
- cust_ce_ospf_percent
  command line option, 21
- cust_ce_rip_percent
  command line option, 21
- cust_ce_routing_protocol
  command line option, 21
- cust_ce_vrf_assignment
  command line option, 21
- cust_ipv6_ce_route_type
  command line option, 21
- cust_ipv6_vpn_route_overlap
  command line option, 24
- cust_ipv6_vpn_route_prefix_len
  command line option, 24
- cust_ipv6_vpn_route_start
  command line option, 24
- cust_ipv6_vpn_route_step
  command line option, 24
- cust_rd_start
  command line option, 22
- cust_rd_step_per_ce
  command line option, 22
- cust_rd_step_per_ce_enable
  command line option, 22
- cust_rd_step_per_vrf
  command line option, 22
- cust_rd_step_per_vrf_enable
  command line option, 22
- cust_route_count_per_ce
  command line option, 23
<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-dut_4byte_as</code></td>
<td>11</td>
</tr>
<tr>
<td><code>-dut_4byte_as_enable</code></td>
<td>11</td>
</tr>
<tr>
<td><code>-dut_as</code></td>
<td>11</td>
</tr>
<tr>
<td><code>-dut_interface_ipv4_addr</code></td>
<td>4</td>
</tr>
<tr>
<td><code>-dut_interface_ipv4_addr_step</code></td>
<td>4</td>
</tr>
<tr>
<td><code>-dut_interface_ipv4_prefix_len</code></td>
<td>4</td>
</tr>
<tr>
<td><code>-dut_interface_ipv6_addr</code></td>
<td>6</td>
</tr>
<tr>
<td><code>-dut_interface_ipv6_addr_step</code></td>
<td>6</td>
</tr>
<tr>
<td><code>-dut_interface_ipv6_prefix_len</code></td>
<td>6</td>
</tr>
<tr>
<td><code>-dut_router_id</code></td>
<td>11</td>
</tr>
<tr>
<td><code>-handle</code></td>
<td>4, 6, 11, 29, 30</td>
</tr>
<tr>
<td><code>-igp_isis_areal</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_areal1</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_areal2</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_areal3</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_auth_md5_key</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_auth_mode</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_auth_password</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_bfd_enable</code></td>
<td>15</td>
</tr>
<tr>
<td><code>-igp_isis_circuit_id</code></td>
<td>15</td>
</tr>
<tr>
<td><code>-igp_isis_graceful_restart_enable</code></td>
<td>15</td>
</tr>
<tr>
<td><code>-igp_isis_hello_padding</code></td>
<td>15</td>
</tr>
<tr>
<td><code>-igp_isis_l1_metric</code></td>
<td>15</td>
</tr>
<tr>
<td><code>-igp_isis_l1_wide_metric</code></td>
<td>15</td>
</tr>
<tr>
<td><code>-igp_isis_level</code></td>
<td>13</td>
</tr>
<tr>
<td><code>-igp_isis_metric_mode</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_network_type</code></td>
<td>13</td>
</tr>
<tr>
<td><code>-igp_isis_router_priority</code></td>
<td>14</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_area_id</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_auth_md5_key</code></td>
<td>13</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_auth_mode</code></td>
<td>13</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_auth_password</code></td>
<td>13</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_bfd_enable</code></td>
<td>13</td>
</tr>
<tr>
<td>`-igp_isis_ospf_graceful_restart_enable</td>
<td>13</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_graceful_restart_type</code></td>
<td>13</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_interface_cost</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_network_type</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_options</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_options</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_router_priority</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_router_priority</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_protocol</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_protocol</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_network_type</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-igp_isis_ospf_options</code></td>
<td>12</td>
</tr>
<tr>
<td><code>-mode</code></td>
<td>3, 5, 11, 30</td>
</tr>
<tr>
<td><code>-mpls_isis_node_sid_index</code></td>
<td>19</td>
</tr>
<tr>
<td><code>-mpls_isis_node_sid_index_step</code></td>
<td>19</td>
</tr>
<tr>
<td><code>-mpls_isis_node_sid_base</code></td>
<td>19</td>
</tr>
<tr>
<td><code>-mpls_isis_node_sid_range</code></td>
<td>19</td>
</tr>
<tr>
<td><code>-mpls_isis_sr_algorithm</code></td>
<td>19</td>
</tr>
<tr>
<td><code>-mpls_isis_sr_algorithm</code></td>
<td>19</td>
</tr>
<tr>
<td><code>-mpls_ldp_auth_mode</code></td>
<td>18</td>
</tr>
<tr>
<td><code>-mpls_ldp_auth_mode</code></td>
<td>18</td>
</tr>
<tr>
<td><code>-mpls_ldp_auth_password</code></td>
<td>18</td>
</tr>
<tr>
<td><code>-mpls_ldp_auth_password</code></td>
<td>18</td>
</tr>
<tr>
<td><code>-mpls_ldp_bfd_enable</code></td>
<td>18</td>
</tr>
<tr>
<td><code>-mpls_ldp_bfd_enable</code></td>
<td>18</td>
</tr>
<tr>
<td><code>-mpls_ldp_egress_label</code></td>
<td>17</td>
</tr>
<tr>
<td><code>-mpls_ldp_egress_label</code></td>
<td>17</td>
</tr>
<tr>
<td><code>-mpls_ldp_graceful_restart_enable</code></td>
<td>18</td>
</tr>
<tr>
<td><code>-mpls_ldp_graceful_restart_enable</code></td>
<td>18</td>
</tr>
<tr>
<td><code>-mpls_ldp_hello_interval</code></td>
<td>17</td>
</tr>
<tr>
<td><code>-mpls_ldp_hello_interval</code></td>
<td>17</td>
</tr>
<tr>
<td><code>-mpls_ldp_hello_type</code></td>
<td>17</td>
</tr>
<tr>
<td><code>-mpls_ldp_hello_type</code></td>
<td>17</td>
</tr>
</tbody>
</table>
-mpls_ldp_keepalive_interval
  command line option, 17
-mpls_ldp_label_adv_mode
  command line option, 18
-mpls_ldp_min_label
  command line option, 17
-mpls_ldp_reconnect_time
  command line option, 18
-mpls_ldp_recover_time
  command line option, 18
-mpls_ldp_transport_mode
  command line option, 17
-mpls OSPF_node_sid_index
  command line option, 18
-mpls OSPF_node_sid_index_step
  command line option, 18
-mpls OSPF_sid_base
  command line option, 18
-mpls OSPF_sid_range
  command line option, 18
-mpls OSPF_sr_algorithms
  command line option, 18
-mpls_protocol
  command line option, 12
-mpls RSVP_bandwidth_per_link
  command line option, 15
-mpls RSVP_bandwidth_per_tunnel
  command line option, 15
-mpls RSVP_bfd_enable
  command line option, 16
-mpls RSVP_bundle_interval
  command line option, 16
-mpls RSVP_egress_label
  command line option, 15
-mpls RSVP_graceful_restart_enable
  command line option, 16
-mpls RSVP_hello_enable
  command line option, 16
-mpls RSVP_hello_interval
  command line option, 16
-mpls RSVP_inter_packet_delay
  command line option, 16
-mpls RSVP_max_label
  command line option, 16
-mpls RSVP_min_label
  command line option, 15
-mpls RSVP_recover_time
  command line option, 16
-mpls RSVP_refresh_delivery
  command line option, 16
-mpls RSVP_refresh_interval
  command line option, 16
-mpls RSVP_request_conf
  command line option, 16
-mpls RSVP_restart_time
  command line option, 16
-mpls RSVP_retrans_delta
  command line option, 16
-mpls RSVP_retrans_interval
  command line option, 17
-mpls RSVP_retrans_limit
  command line option, 17
-mpls RSVP_summary_refresh_interval
  command line option, 16
-mpls RSVP_transit
  command line option, 16
-p_router_enable
  command line option, 15
-p_router_id_start
  command line option, 19
-p_router_id_step
  command line option, 19
-p_router_ipv4_addr
  command line option, 19
-p_router_ipv4_prefix_len
  command line option, 19
-p_router_num_per_subif
  command line option, 19
-p_router_topology_type
  command line option, 19
-pe_router_id_start
  command line option, 19
-pe_router_id_step
  command line option, 19
-pe_router_num_per_subif
  command line option, 19
-port_handle
  command line option, 3, 5, 29, 30
-provider ce bgp 4byte_as
  command line option, 23
-provider ce bgp 4byte_as_enable
  command line option, 23
-provider ce bgp 4byte_as_step_per_ce
  command line option, 23
-provider ce bgp 4byte_as_step_per_ce_enable
  command line option, 23
-provider ce bgp 4byte_as_step_per_vrf
  command line option, 23
-provider ce bgp 4byte_as_step_per_vrf_enable
  command line option, 23
-provider ce bgp as
  command line option, 23
-provider ce bgp as_enable
  command line option, 23
-provider ce bgp as_step_per_ce
  command line option, 23
-provider ce bgp as_step_per_ce_enable
  command line option, 23
-index 41
-provider_ce_bgp_as_step_per_vrf
  command line option, 23
-provider_ce_bgp_as_step_per_vrf_enable
  command line option, 23
-provider_ipv6_vpn_route_overlap
  command line option, 25
-provider_ipv6_vpn_route_prefix_len
  command line option, 25
-provider_ipv6_vpn_route_start
  command line option, 25
-provider_ipv6_vpn_route_step
  command line option, 25
-provider_pe_vrf_all_assign
  command line option, 23
-provider_pe_vrf_assignment
  command line option, 23
-provider_pe_vrf_count
  command line option, 23
-provider_rd_start
  command line option, 24
-provider_rd_step_per_ce
  command line option, 24
-provider_rd_step_per_ce_enable
  command line option, 24
-provider_rd_step_per_vrf
  command line option, 24
-provider_rd_step_per_vrf_enable
  command line option, 24
-provider_route_count_per_ce
  command line option, 25
-sub_interface_count
  command line option, 4, 6
-sub_interface_enable
  command line option, 4, 6
-traffic_flow_direction
  command line option, 25
-traffic_load_percent_cust
  command line option, 26
-traffic_load_percent_provider
  command line option, 26
-traffic_pattern
  command line option, 26
-traffic_stream_group_method
  command line option, 26
-traffic_use_single_stream_per_endpoint_pair
  command line option, 26
-use_cust_ports
  command line option, 11
-use_provider_ports
  command line option, 11
-vlan_id
  command line option, 4, 6
-vlan_id_step
  command line option, 4, 6
-vpn_6vpe_enable
  command line option, 20
-vrf_count
  command line option, 20
-vrf_rd_assignment
  command line option, 20
-vrf_route_mpls_label_start
  command line option, 25
-vrf_route_mpls_label_type
  command line option, 25
-vrf_route_target_start
  command line option, 21
-vrf_route_target_step
  command line option, 21
-vrf_route_target_step
  command line option, 21
-vrf_6vpe_disable
  command line option, 20
-cust_ce_bgp_4byte_as
  command line option, 22
-cust_ce_bgp_4byte_as_enable
  command line option, 22
-cust_ce_bgp_4byte_as_step_per_ce
  command line option, 22
-cust_ce_bgp_4byte_as_step_per_ce_enable
  command line option, 22
-cust_ce_bgp_4byte_as_step_per_vrf
  command line option, 22
-cust_ce_bgp_4byte_as_step_per_vrf_enable
  command line option, 22
-cust_ce_bgp_as
  command line option, 21
-cust_ce_bgp_as_step_per_ce
  command line option, 21
-cust_ce_bgp_as_step_per_ce_enable
  command line option, 21
-cust_ce_bgp_as_step_per_vrf
  command line option, 22
-cust_ce_bgp_as_step_per_vrf_enable
  command line option, 22
-cust_ce_bgp_percent
  command line option, 21
-cust_ce_isis_percent
  command line option, 21
-cust_ce_ospf_percent
  command line option, 21
-cust_ce_rip_percent
  command line option, 21
-cust_ce_routing_protocol
  command line option, 21
-cust_ce_vrf_assignment
  command line option, 21
-cust_ipv6_ce_route_type
  command line option, 24
-cust_ipv6_vpn_route_overlap
  command line option, 24
-cust_ipv6_vpn_route_prefix_len, 24
-cust_ipv6_vpn_route_start, 24
-cust_ipv6_vpn_route_step, 24
-cust_rd_start, 22
-cust_rd_step_per_ce, 22
-cust_rd_step_per_ce_enable, 22
-cust_rd_step_per_vrf, 22
-cust_rd_step_per_vrf_enable, 22
-cust_route_count_per_ce, 23
-dut_4byte_as, 11
-dut_4byte_as_enable, 11
-dut_interface_ipv4_addr, 4
-dut_interface_ipv4_addr_step, 4
-dut_interface_ipv4_prefix_len, 4
-dut_interface_ipv6_addr, 6
-dut_interface_ipv6_addr_step, 6
-dut_interface_ipv6_prefix_len, 6
-dut_router_id, 11
-handle, 4, 6, 11, 29, 30
-igp_isis_area1, 14
-igp_isis_area2, 14
-igp_isis_area3, 14
-igp_isis_auth_md5_key, 14
-igp_isis_auth_mode, 14
-igp_isis_auth_password, 14
-igp_isis_bfd_enable, 15
-igp_isis_circuit_id, 14
-igp_isis_graceful_restart_enable, 15
-igp_isis_hello_padding, 15
-igp_isis_hello_padding_11, 14
-igp_isis_hello_padding_12, 15
-igp_isis_level, 13
-igp_isis_metric_mode, 14
-igp_isis_network_type, 13
-igp_isis_router_priority, 14
-igp_ospf_area_id, 12
-igp_ospf_auth_md5_key, 13
-igp_ospf_auth_mode, 13
-igp_ospf_auth_password, 13
-igp_ospf_bfd_enable, 13
-igp_ospf_graceful_restart_enable, 13
-igp_ospf_graceful_restart_type, 13
-igp_ospf_interface_cost, 12
-igp_ospf_network_type, 12
-igp_ospf_options, 12
-igp_ospf_router_priority, 12
-igp_protocol, 12
-mode, 3, 5, 11, 30
-mpls_isis_node_sid_index, 19