



Hewlett Packard
Enterprise

HPE Service Insertion Guide

Wired Switches K/KA/KB/WB 16.01

Abstract

This document describes the general steps and individual commands for enabling Service Insertion on Hewlett Packard Enterprise Switches.

Applicable Products

Aruba 2920 Switch series
Aruba 3810M Switch series
Aruba 5400R series, v2 and v3 modules
HPE Switch 3800 series
HPE 5400 series, v2 modules

Part Number: 5200-0147
Published: January 2016
Edition: 1

© Copyright 2016 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Contents

| | |
|--|-----------|
| 1 Service Insertion | 4 |
| Network device service insertion..... | 4 |
| Hardware IP Tunnels..... | 5 |
| Tunnel Creation..... | 5 |
| Tunnel Deletion..... | 6 |
| Tunnel Aliveness check using OpenFlow..... | 6 |
| OpenFlow and Service Tunnels..... | 7 |
| OpenFlow and Service Intercept Tunnel Restrictions..... | 8 |
| OpenFlow and Service Tap Tunnel Restrictions..... | 8 |
| Service Tunnel restrictions with other features..... | 9 |
| CLI commands..... | 9 |
| show command..... | 9 |
| show interface tunnel command..... | 12 |
| Clear command..... | 14 |
| Show monitor..... | 15 |
| Debug command..... | 15 |
| Show Tech Service Tunnel command..... | 15 |
| Troubleshooting..... | 25 |
| Tunnel creation..... | 26 |
| Tunnel operational status | 28 |
| Encapsulation path - traffic steering to tunnel (via OpenFlow) | 29 |
| Decapsulation path..... | 31 |
| Other tunnel specific troubleshooting commands..... | 32 |
| 2 Support and other resources | 34 |
| Accessing Hewlett Packard Enterprise Support..... | 34 |
| Accessing updates..... | 34 |
| Websites..... | 34 |
| Customer self repair..... | 35 |
| Remote support..... | 35 |
| Documentation feedback..... | 35 |
| Index | 36 |

1 Service Insertion

Service Insertion is transparently inserting an external service into a traffic flow or into the traffic processing pipeline:

- Flows are re-directed to a service for inspection and then re-injected to the forwarding pipeline
- Possible services include IPS, Hewlett Packard Enterprise Network Protector SDN Application, Hewlett Packard Enterprise Network Visualizer SDN Application, Web filtering, and traffic analyzers

Service Insertion is handled by the ASIC via a tunnel or Fast Path, and does not incur any CPU processing overhead. This feature is supported on the Aruba 2920 Switch series, HPE 3800, Aruba 3810M, HPE 5400 , Aruba 5400R v2 and v3 modules. It is not supported in V1-compatible mode.

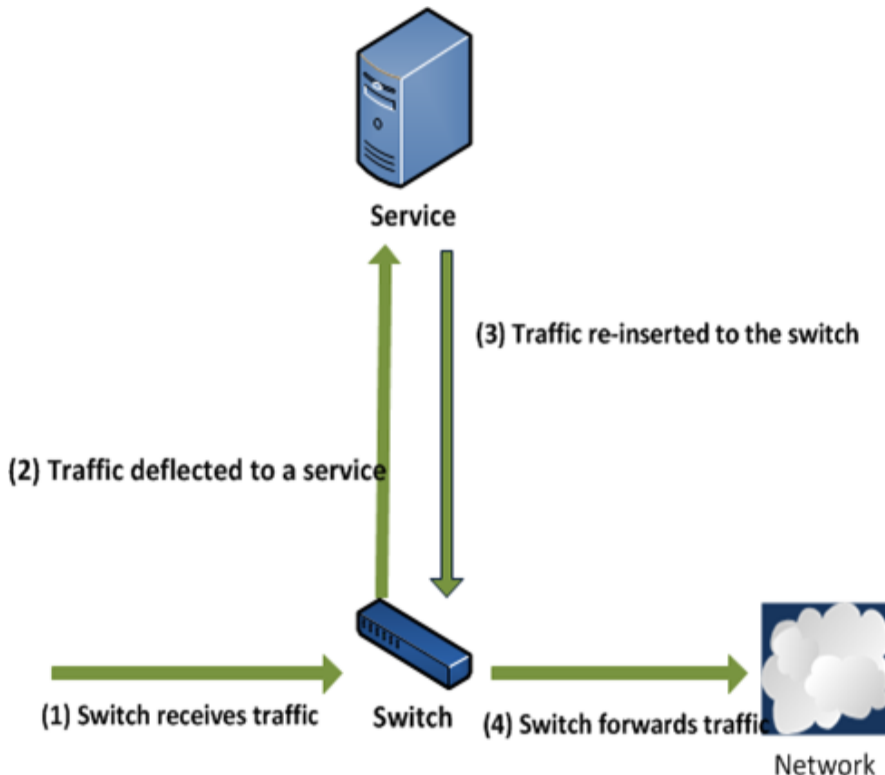
NOTE: For HPE 5400, you must execute the following command before configuring a Service Insertion tunnel:

```
no allow-v1-modules
```

This command disables all v1 modules.

The figure below shows Inspection Service.

Figure 1 Inspection Service



Network device service insertion

Service Insertion is a feature to insert a packet inspection service into the normal flow of traffic. Utilizing OpenFlow flow rules, traffic can be redirected to a network device like the HPE Network

Protector SDN Application for inspection and decision making. You can use a service insertion tunnel for the following modes:

- Inline inspection called **intercept**, where traffic is redirected to a network device like the HPE Network Protector SDN Application. The network device reinserts legitimate traffic into the switch pipeline to be processed and forwarded as normal.
- Out of line inspection called **tap**, where traffic is mirrored to a network device like the HPE Network Visualizer SDN Application.

Tap tunnels mirror the traffic from switch to the remote endpoint and are uni-directional in nature. The switch will not receive packets back on the tunnel.

Hardware IP Tunnels

HW IP Tunnels are used to enable Service Insertion. They are presented as virtual ports to the OpenFlow agent running on the switch. Once a tunnel is created (by the Network Protector SDN Application, for example) the OpenFlow agent is notified about the presence of the new interface. The OpenFlow agent communicates this interface as a new logical port to the SDN controller. This logical port is advertised over all OpenFlow version 1.3 instances configured on the switch.

If the OpenFlow output port action for a flow rule points to a tunnel logical port, the packets matching that flow rule are diverted to the configured tunnel endpoint via the tunnel interface.

When a frame is encapsulated and sent to the controller, the frame includes the MAC headers and the VLAN tag. Even if the original frame was not VLAN tagged, the switch VLAN tags this frame with VLAN-ID set to the incoming port's default VLAN before encapsulating it. Since frames are encapsulated, the path that the encapsulated packet traverses must be configured with a larger MTU.

Up to 16 unique tunnel interfaces can be created to actively forward traffic.

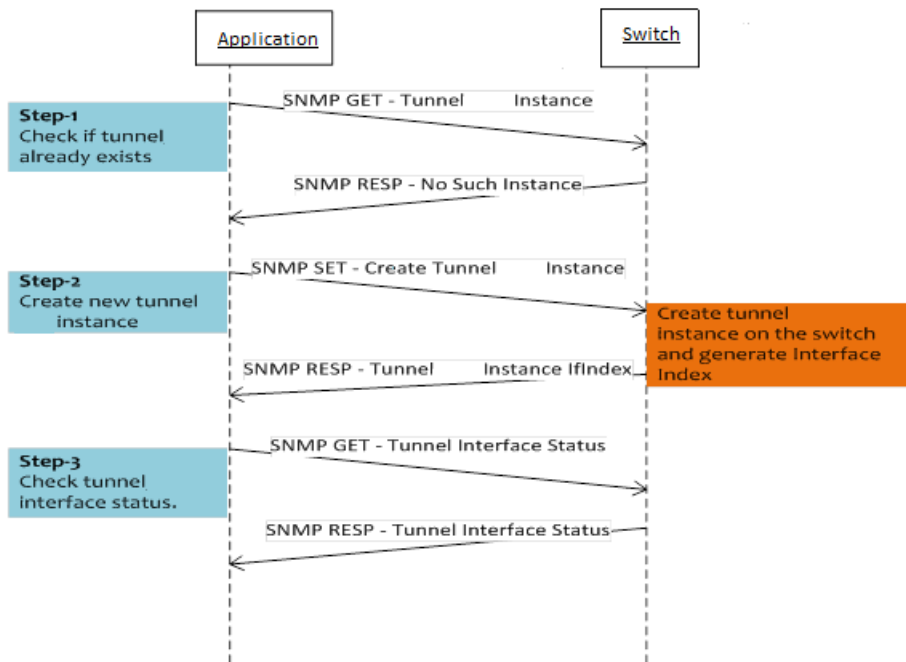
NOTE: Tunnels are IPv4 only. IPv6 tunnels are not supported in the current version.

Tunnel Creation

Tunnels can be created using SNMP. The switch manages tunnels, with each tunnel being represented by a unique interface index. First the application (such as the Network Protector SDN Application) queries a switch to determine if it supports configuring tunnels. This is via an SNMP object that returns the number of tunnel interfaces supported on the switch. Once it is determined that tunnels can be configured, the controller can move on to creating the appropriate interface.

The following sequence diagram explains the process of creation of a tunnel.

Figure 2 Tunnel Creation



A switch management module failover results in tunnels being removed from hardware and OpenFlow rules pointing to these tunnels will drop frames.

NOTE: Tunnel-related configuration information is non-volatile and cannot be restored after a device reboot. The controller has to re-create the tunnel interface in the event that the switch reboots and comes back up.

Tunnel Deletion

The application can delete the tunnel interface it created using SNMP. The switch does not check if there are any active OpenFlow rules using that tunnel but goes ahead and deletes the interface. If there are active flow rules that are using a tunnel, traffic matching those flow rules are dropped because the tunnel has been deleted.

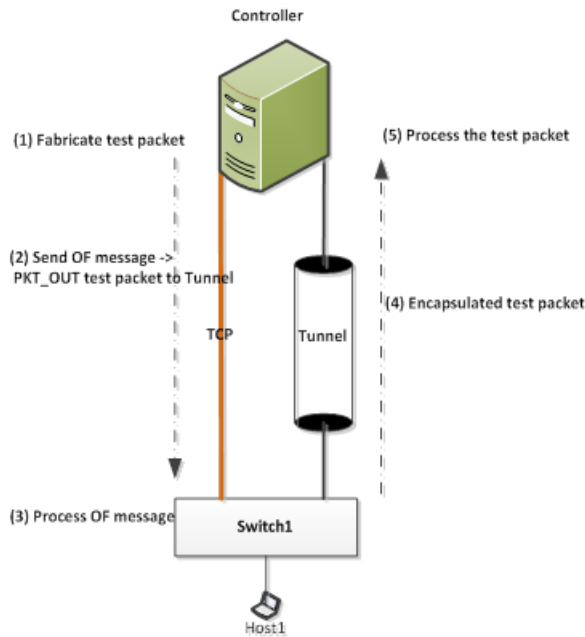
Once a tunnel interface has been deleted, the OpenFlow agent communicates the same to the controller as a logical port removal notification. The agent doesn't remove any flow rules that use these virtual ports in line with the OpenFlow 1.3 Specification. The controller has to remove these flow rules or modify them appropriately.

Tunnel Aliveness check using OpenFlow

Detection of Tunnel connectivity status via OpenFlow message:

If the application does not receive any packet on the tunnel interface for a certain period of time, it can check if the tunnel path is active by crafting a heartbeat packet and sending an OpenFlow packet OUT message to the switch with the output port for the heartbeat packet as the tunnel interface. Once the switch receives the OpenFlow message, it sends the heartbeat frame encapsulated out the tunnel interface to the application. The application can use this message to confirm that the tunnel path is working fine.

Figure 3 Tunnel heartbeat via OpenFlow message



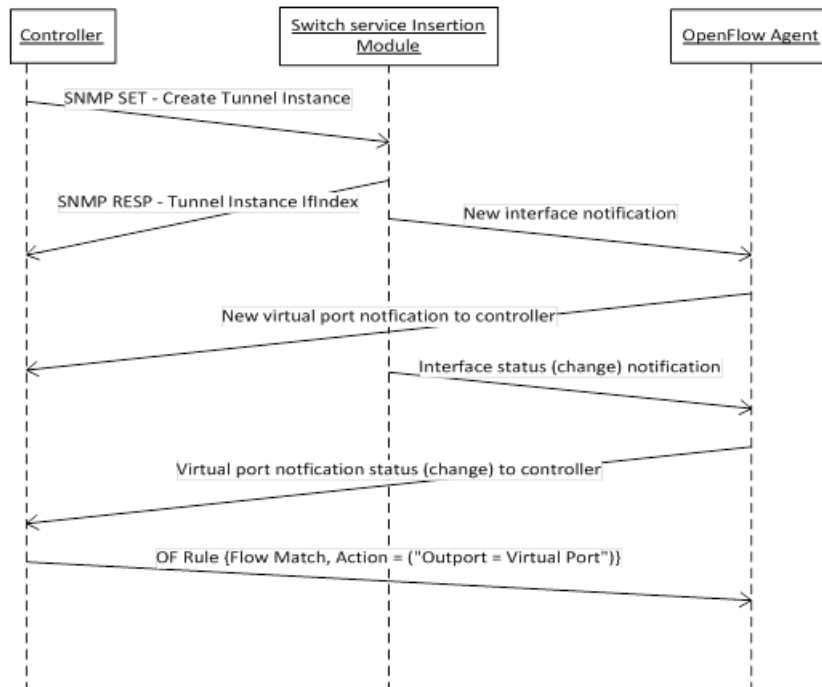
OpenFlow and Service Tunnels

The switch notifies the OpenFlow controller about tunnel interface status changes (UP/DOWN) as well.

Once the controller is notified of the tunnel instance via the OpenFlow switch agent, it can use the same as a valid output port in its FLOW-MOD messages it pushes to the switch.

If the OpenFlow output action for a flow rule points to a tunnel virtual port, the packets matching that flow rule are rerouted to the controller via the tunnel interface.

Figure 4 Integration with OpenFlow



OpenFlow and Service Intercept Tunnel Restrictions

1. A tunnel interface cannot be part of a multi-port output action.
2. A flow-rule's output action of sending packets to a tunnel cannot be combined with "Normal" or "SendToController" actions.
3. A tunnel interface cannot be part of FLOOD action.
4. Re-directing packets to SI tunnels on an OpenFlow 1.0 instance is not supported. Tunnels are only supported on OpenFlow 1.3 instances.
5. OpenFlow pipeline is bypassed for packets coming back on a tunnel. The device forwarding tables are used to determine how to forward these packets.
6. The switch does not remove the flows referencing tunnels when tunnel interfaces are deleted. The controller has to come back and delete those flows.
7. The tunnel interfaces are only supported on the Policy Engine (TCAM) tables and not with the software tables.
8. In the event of management card failover (on platforms with redundant management card support), tunnel interfaces are removed but OpenFlow does not delete any flows referencing tunnel interfaces. Once the application recreates those tunnels, traffic forwarding to tunnels will resume.
9. OpenFlow Port mod requests are not supported on tunnel interfaces.
10. A tunnel interface cannot be used as a match parameter in any flow programmed by the OpenFlow controller.
11. When using Service Insertion, VLAN interfaces that have a DHCP address and OOBM interfaces cannot be used to create a tunnel between device and the application.

OpenFlow and Service Tap Tunnel Restrictions

1. The OpenFlow action `OutPort = Mirror tunnel` is not supported for flow rules programmed on the OpenFlow software tables.
2. If there is a flow rule whose action is `Normal + Mirror Tunnel` and a packet matching that flow rule is dropped (based on its `Normal` action or because of a rate limit), that PKT will still be sent to the mirror tunnel.

NOTE: The `Mirror` action does not affect the forwarding behavior. It only mirrors what was received that matched the OpenFlow rule.

3. The PKT that is sent to the mirror tunnel does not have its DSCP rewritten to `EF` if there is an OpenFlow rule such as:

```
{match SRC.IP == abc,  
action = (DSCP = EF, OutPort = COPY Tunnel)}
```

The inbound DSCP value of the PKT is what appears as the PKT's DSCP on the mirror tunnel.
4. OpenFlow port MOD requests is not supported on mirror tunnel ports.
5. Mirror tunnel port cannot be used as a match field (`IN_PORT`).
6. When a mirror tunnel interface is deleted by the administrator (via SNMP) but there are OpenFlow rules that are using those tunnels, the switch will not automatically remove flows associated with the tunnel ports even though mirroring will be stopped.
The controller has to delete those flows explicitly.
7. Cannot combine the `outport mirror` action with the `Strip VLAN`, `Modify VLAN`, `Modify MAC` actions.
8. Cannot support the `outport mirror` action on an OpenFlow 1.0 instance.
9. OpenFlow groups cannot support `output mirror` as an action.

Service Tunnel restrictions with other features

1. Multicast routing cannot be enabled on a device when Service Tunnels are configured and vice-versa.
2. Distributed trunking cannot be configured on a device when Service Tunnels are configured and vice-versa.
3. MESH cannot be configured on a device when Service Tunnels are configured and vice-versa.
4. MAC-Mirror cannot be configured on a device when Service Tunnels are configured and vice-versa.
5. QinQ cannot be configured on a device when Service Tunnels are configured and vice-versa.

CLI commands

show command

Syntax

```
show interfaces tunnel [<Tunnel-ID-List> | brief | type {intercept | tap [<Interface-Index> | statistics
[<Interface-Index>]]}]
Description: Show tunnel configuration and status information.
Tunnel-ID-List      Summary of network traffic handled by the tunnels.
brief              Lists all tunnels created and their status.
type              Specifies the service tunnel type.
intercept         Shows all intercept service tunnels.
tap              Shows all tap service tunnels.
Interface-Index   Status for specific intercept or tap service tunnel.
statistics        Statistics for all intercept or tap service tunnels.
```

Example: intercept

The `show interface tunnel type intercept` command displays all the intercept tunnel information.

```
HP-E8206zl# show interface tunnel type intercept
Status - Service Tunnel Information Brief
```

```
Max. Supported Tunnels : 16
Total Tunnels          : 1

Interface Index       : 1000000001
Name                  : ServiceTunnel-01
Key                   : 9991001
Local IP Address      : 1.1.1.1
Remote IP Address     : 1.1.1.2
Interface State       : Up

Interface Index       : 1000000002
Name                  : ServiceTunnel-02
Key                   : 9991002
Local IP Address      : 1.1.1.1
Remote IP Address     : 1.1.1.2
Interface State       : Up
```

Example: intercept <Interface-Index>

The `show interface tunnel type intercept <Interface-Index>` command displays the specific intercept tunnel information.

```
HP-E8206zl(config)# show interface tunnel type intercept 1000000001
Service Tunnel Configuration
Interface Index       : 1000000001
Name                  : ServiceTunnel-01
Key                   : 9991001
Local IP Address      : 1.1.1.1
Remote IP Address     : 1.1.1.2
```

```
DSCP Value      : 0
TTL             : 64
MTU            : 1280
```

Status

```
Interface State      : Up
Interface Down Reason :
Destination Address Route :
Next Hop IP         :
Next Hop Interface   :
Next Hop IP Link Status :
Source Address      :
Egress Port        :
```

Example: tap

The show interface tunnel type tap command displays all the tap tunnel information.

```
HP-E8206zl# show interface tunnel type tap
Status - Service Tunnel Information Brief
```

```
Max. Supported Tunnels : 4
Total Tunnels          : 1
Interface Index        : 1000000001
Name                   : ServiceTunnel-01
Key                    : 9991001
Local IP Address       : 1.1.1.1
Remote IP Address      : 1.1.1.2
Interface State        : Up
Interface Index        : 1000000002
Name                   : ServiceTunnel-02
Key                    : 9991002
Local IP Address       : 1.1.1.1
Remote IP Address      : 1.1.1.2
Interface State        : Up
```

Example: tap <Interface-Index>

The show interface tunnel type tap <Interface-Index> command displays the specific intercept tunnel information.

```
HP-E8206zl(config)# show interface tunnel type intercept 1000000001
Service Tunnel Configuration
Interface Index      : 1000000001
Name                 : ServiceTunnel-01
Key                  : 9991001
Local IP Address     : 1.1.1.1
Remote IP Address    : 1.1.1.2
DSCP Value           : 0
TTL                  : 64
MTU                  : 1280
```

Status

```
Interface State      : Up
Interface Down Reason :
Destination Address Route :
Next Hop IP         :
Next Hop Interface   :
Next Hop IP Link Status :
Source Address      :
Egress Port        :
```

Example: intercept statistics

The show interface tunnel type intercept statistics displays all the intercept tunnel statistics. The intercept tunnels show the RX and TX packet counters.

```
HP-E8206zl# show interface tunnel type intercept statistics
```

```
Service Tunnel Information
```

```
Aggregate Statistics
```

```
Fragmented Packets Dropped (Rx)      :  
Packets to Non-Existence Tunnel     :  
Unknown Source MAC Packets Dropped (Rx) :  
MTU Violation Drop                  :
```

```
Service Tunnel Statistics
```

```
Interface Index      : 1000000001  
Name                 : ServiceTunnel-01  
Rx Packets           : 0  
Tx Packets           : 0  
Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0  
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0  
Rx Heartbeat         : 0  
Tx Heartbeat         : 0  
Last Recv Heartbeat Timestamp       : 01/01/90 00:00:00
```

```
Interface Index      : 1000000002  
Name                 : ServiceTunnel-02  
Rx Packets           : 0  
Tx Packets           : 0  
Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0  
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0  
Rx Heartbeat         : 0  
Tx Heartbeat         : 0  
Last Recv Heartbeat Timestamp       : 01/01/90 00:00:00
```

Example: intercept statistics <Interface-Index>

The show interface tunnel type intercept statistics <Interface-Index> command displays statistics for the specified tunnel interface.

```
HP-E8206zl# show interface tunnel type intercept statistics 1000000001
```

```
Service Tunnel Statistics
```

```
Interface Index      : 1000000001  
Name: ServiceTunnel-01  
Rx Packets           : 0  
Tx Packets           : 0  
Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0  
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0  
Rx Heartbeat         : 0  
Tx Heartbeat         : 0  
Last Recv Heartbeat Timestamp       : 01/01/90 00:00:00
```

Example: tap statistics

The show interface tunnel type intercept statistics command displays all the tap service statistics. The tap tunnels show the TX packet counters only.

```
HP-E8206zl# show interface tunnel type tap statistics
```

```
Service Tunnel Information
```

```
Aggregate Statistics
```

MTU Violation Drop :

Service Tunnel Statistics

```
Interface Index      : 1000000001
Name                 : ServiceTunnel-01
Tx Packets           : 0
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0
```

```
Interface Index      : 1000000002
Name                 : ServiceTunnel-02
Tx Packets           : 0
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0
```

Example: tap statistics <Interface-Index>

The `show interface tunnel type tap statistics <Interface-Index>` command displays the specific tap tunnel statistics configured on the switch.

```
HP-E8206z1# show interface tunnel type tap statistics 1000000001
```

Service Tunnel Statistics

```
Interface Index      : 1000000001
Name                 : ServiceTunnel-01
Tx Packets           : 0
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0
```

show interface tunnel command

Example: show interface

The `show interface tunnel` command displays the tunnel information with supported fields. Unsupported fields are indicated with n/a. For the tunnel configuration, the possible Mode values are intercept or tap.

```
HP-E8206z1# show interface tunnel
```

```
Tunnel Configuration      :
Tunnel                    : 1000000001
Tunnel Name               : ServiceTunnel-01
Tunnel Status             : Enabled
Source Address            : 1.1.1.1
Destination Address       : 1.1.1.2
Mode                      : Service Tunnel - intercept
TOS                       :
TTL                       :
IPv6                     : n/a
MTU                      :

Current Tunnel Status     :

Tunnel State              : Up
Destination Address Route:
Next Hop IP               :
Next Hop Interface        :
Next Hop IP Link Status   :
Source Address            :
```

Example: show interface brief

The `show interface tunnel brief` command displays the tunnel information with supported fields.

```
HP-E8206zl# show interface tunnel brief
```

```
Tunnel          : 1000000001
Mode            : Service Tunnel - Tap
Source Address  : 1.1.1.1
Destination Address : 1.1.1.2
Configured Tunnel Status : Enabled
Current Tunnel State : Up
```

Example: show interface <Tunnel-ID-List>

The `show interface tunnel <Tunnel-ID-List>` command displays the tunnel information with supported fields. Unsupported fields are indicated with `n/a`.

```
HP-E8206zl# show interface tunnel 1000000001
```

```
Tunnel Configuration      :

Tunnel                   : 10
Tunnel Name              :
Tunnel Status            : Enabled
Source Address           : 1.1.1.1
Destination Address      : 1.1.1.2
Mode                     : Service Tunnel - Tap
TOS                      :
TTL                      :
IPv6                     : n/a
MTU                      :

Current Tunnel Status    :

Tunnel State             : Up
Destination Address Route: 0.0.0.0/0
Next Hop IP              : 120.92.48.129
Next Hop Interface       : vlan-1
Next Hop IP Link Status  : Up
Source Address           : 1.1.1.1
Egress Port              : A1
```

Example: display interface brief

The `display interface brief` command displays the tunnel information with supported fields. Unsupported fields are indicated with `n/a`.

```
HP-E8206zl# display interface brief
```

The brief information of interface(s) under route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) - spoofing

| Interface | Link | Protocol | Main IP | Description |
|------------|------|----------|---------|------------------|
| 1000000001 | Down | Enabled | 1.1.1.1 | ServiceTunnel-01 |

The brief information of interface(s) under bridge mode:

Link: ADM - administratively down; Stby - standby

Speed or Duplex: (a)/A - auto; H - half; F - full

Type: A - access; T - trunk; H - hybrid

| Interface | Link | Speed | Duplex | Type | PVID | Description |
|-----------|------|-------|--------|------|------|-------------|
| A1 | UP | auto | A | n/a | 1 | |

Example: display interface brief down

The `display interface brief down` command displays the tunnel information with supported fields. Unsupported fields are indicated with n/a.

```
HP-E8206zl# display interface brief down
```

The brief information of interface(s) under route mode:

Link: ADM - administratively down; Stby - standby

| Interface | Link Cause |
|-----------|------------|
|-----------|------------|

| | |
|------------|----------|
| 1000000001 | Down n/a |
|------------|----------|

The brief information of interface(s) under bridge mode:

Link: ADM - administratively down; Stby - standby

| Interface | Link Cause |
|-----------|------------|
|-----------|------------|

| | |
|----|--------------------|
| A1 | Down Not connected |
|----|--------------------|

Example: display interface <Tunnel-ID-List>

The `display interface tunnel <Tunnel-ID-List>` command displays the tunnel information with supported fields. Unsupported fields are indicated with n/a.

```
HP-E8206zl# display interface tunnel
```

```
1000000001 current state: DOWN
```

```
Line protocol current state: n/a
```

```
Description: ServiceTunnel-74 Interface
```

```
The Maximum Transmit Unit is 0
```

```
Internet Address is 2.113.132.228/30 primary
```

```
Encapsulation is TUNNEL, Service-loopback-group ID n/a
```

```
Tunnel source 10.10.10.1, destination 10.10.10.2
```

```
Tunnel bandwidth n/a
```

```
Tunnel protocol/transport GRE/IP
```

```
Last clearing of counters:n/a
```

```
  Last 300 seconds input:n/a
```

```
  Last 300 seconds output:n/a
```

```
  0 packets input, 0 bytes
```

```
  0 input error
```

```
  0 packets output, 0 bytes
```

```
  0 output error
```

Clear command

The `clear` command deletes the service tunnels and clears the statistics on the switch.

Syntax

```
HP-E8206zl# clear interfaces tunnel type {intercept | tap} {all | <Interface-Index> | statistics [all | <Interface-Index>]}
```

type Specify the Service Tunnel type

intercept Delete the Service Tunnel or reset the statistics for all the sessions

all Delete all Service Tunnels of type intercept

Interface-Index Delete a specific Service Tunnel of type intercept

statistics Reset the statistics of the Service Tunnel of type intercept

Example: clear intercept all

```
HP-E8206zl# clear interfaces tunnel type intercept all
```

```
This command will delete all the Service Tunnels of type intercept. Make sure the tunnels are not in use by any application. Continue (y/n)?
```

Example: clear intercept <Interface-Index>

```
HP-E8206zl# clear interfaces tunnel type intercept 1000000001
```

```
This command will delete the specified Service Tunnel of type intercept. Make sure the tunnel is not in use by any application. Continue (y/n)?
```

Example: clear interfaces tunnel type tap all

```
HP-E8206z1# clear interfaces tunnel type tap all
This command will delete all the Service Tunnels of type tap. Make sure the tunnels are not in use by any application. Continue (y/n)?
```

Example: clear tap <Interface-Index>

```
HP-E8206z1# clear interfaces tunnel type tap 1000000001
This command will delete the specified Service Tunnel of type tap. Make sure the tunnel is not in use by any application. Continue (y/n)?
```

Show monitor

The `show` command lists any mirror sessions that are free for mirroring as well as tap tunnel configuration.

Syntax

```
HP-8206z1(config)# show monitor
There are no Remote Mirroring endpoints currently assigned.
```

Network Monitoring

| Sessions | Status | Type | Sources | Mirror-Policy |
|----------|-------------|------------------------------|---------|---------------|
| 1 | active | port | 1 | No |
| 2 | not defined | | | |
| 3 | Reserved by | VXLAN | | |
| 4 | Reserved by | Service Insertion Tap Tunnel | | |

Debug command

The `debug` command enables Service tunnel event debug messages. To view the debug messages, execute the command `show debug buffer` or `show debug logging`.

Syntax

```
debug tunnel {intercept [heartbeat] | tap}
```

Example: debug tunnel intercept

```
HP-E8206z1# debug tunnel intercept heartbeat
Description: Enable heartbeat debug logging for Service Tunnel of type intercept
```

Example: debug tunnel tap

```
HP-E8206z1# debug tunnel tap
```

Show Tech Service Tunnel command

The `show tech tunnel` command displays output for the `intercept` or `tap` tunnel type and is used by technical support.

Syntax

```
HP-5406z1# show tech tunnel {intercept | tap}
```

Example: show tech tunnel intercept

```
HP-5406z1# show tech tunnel intercept
```

show interfaces tunnel type intercept

Status - Service Tunnel Information Brief

Max. Supported Tunnels : 16
Total Tunnels : 2

Interface Index : 100663627
Name : ServiceTunnel-02
Key : 212
Local Address : 10.0.0.1
Remote Address : 57.50.50.50
Interface State : Down

Interface Index : 100663626
Name : ServiceTunnel-01
Key : 212
Local Address : 41.30.30.30
Remote Address : 57.50.50.50
Interface State : Down

show interfaces tunnel type intercept statistics

Service Tunnel Information

Aggregate Statistics

Fragmented Packets Dropped (Rx) : 0
Packets to Non-Existent Tunnel : 0
Unknown Source MAC Packets Dropped (Rx) : 0
MTU Violation Drop : 0

Service Tunnel Statistics

Interface Index : 100663627
Name : ServiceTunnel-02
Rx Packets : 0
Tx Packets : 0
Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0
Rx Heartbeat : 0
Tx Heartbeat : 0
Last Received Heartbeat Timestamp : 01/01/90 00:00:00

Interface Index : 100663626
Name : ServiceTunnel-01
Rx Packets : 0
Tx Packets : 0
Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0
Rx Heartbeat : 0
Tx Heartbeat : 0
Last Received Heartbeat Timestamp : 01/01/90 00:00:00

ifmShowIPv4ServiceTunnels
Max. Supported Tunnels : 16
Total Tunnels : 2

show arp

IP ARP table

| IP Address | MAC Address | Type | Port |
|------------|-------------|------|------|
|------------|-------------|------|------|

show ip route

IP Route Entries

| Destination | Gateway | VLAN Type | Sub-Type | Metric | Dist. |
|-------------|---------|-----------|----------|--------|-------|
|-------------|---------|-----------|----------|--------|-------|


```

127.0.0.0/8      reject      static      0      0
127.0.0.1/32    lo0         connected   1      0

```

show ip

Internet (IP) Service

IP Routing : Disabled

```

Default Gateway :
Default TTL      : 64
Arp Age         : 20
Domain Suffix   :
DNS server      :

```

| VLAN | IP Config | IP Address | Subnet Mask | Proxy ARP | |
|--------------|------------|-------------|---------------|-----------|-------|
| | | | | Std | Local |
| -----+----- | | | | | |
| DEFAULT_VLAN | DHCP/Bootp | | | | |
| VLAN5 | Manual | 10.0.0.1 | 255.255.255.0 | No | No |
| VLAN6 | Manual | 41.30.30.30 | 255.255.255.0 | No | No |

show mac-address

Status and Counters - Port Address Table

```

MAC Address  Port  VLAN
-----

```

```

tgTunnelShowTech
SI Tunnel Show Tech

```

Tunnel Glue Uport Table

| Index | noRoleIndex | UifIndex | IPort | Status |
|-------|-------------|-----------|-------|-----------|
| 0 | 150995326 | 134218110 | 53 | Allocated |

OpenFlow Status : Disabled

Tunnel Glue Tunnel Entry Table

| Tunnel | Interface | Status |
|--------|-----------|-------------|
| 0 | 100663626 | Established |
| 1 | 100663627 | Established |

Tunnel Information for Tunnel : 0

PvGre Tunnel Entries at Tunnel Glue

```

ifIndex      : 100663626
TGstatus     : ESTABLISHED
FDstatus     : ESTABLISHED
TCAMstatus   : ESTABLISHED
UPORTstatus  : ESTABLISHED
Before       : 16
After        : 1
Uport        : 0
HwLogPort    : 209
gatewayIf    : 0
outLPortIf   : 0
GRE_key      : 212
encapType    : 4
vlan_id      : 1
gatewayMacAddr: 000000-000000
srcMacAddr   : 2C59E5-0F20C0
TTL          : 64
MTU          : 1468
TOS          : 0
Bandwidth    : 1024
Tunnel Status : Down No Route
Current Rx Counter Rate(HIT) : 0 Packets per second
Current Tx Counter Rate(FRAME) : 0 Packets per second

```

```
Weighed 5 minute average Rx Counter Rate(HIT) : 0 Packets per second
Weighed 5 minute average Tx Counter Rate(FRAME): 0 Packets per second
localIpAddr      : 41.30.30.30
remoteIpAddr     : 57.50.50.50
gatewayIP        : 0.0.0.0
```

```
-----
| Tunnel IOCTL info |
-----
```

```
Rx Counter(HIT)      : 0
Tx Counter(FRAME)    : 0
```

```
-----
Tunnel Information for Tunnel : 1
-----
```

```
PvGre Tunnel Entries at Tunnel Glue
```

```
ifIndex      : 100663627
TGstatus     : ESTABLISHED
FDstatus     : ESTABLISHED
TCAMstatus   : ESTABLISHED
UPORTstatus  : ESTABLISHED
Before       : 0
After        : 16
Uport        : 0
HwLogPort    : 209
gatewayIf    : 0
outLPortIf   : 0
GRE_key      : 212
encapType    : 4
vlan_id      : 1
gatewayMacAddr: 000000-000000
srcMacAddr   : 2C59E5-0F20C0
TTL          : 64
MTU          : 1468
TOS          : 0
Bandwidth    : 1024
Tunnel Status : Down No Route
Current Rx Counter Rate(HIT): 0 Packets per second
Current Tx Counter Rate(FRAME): 0 Packets per second
Weighed 5 minute average Rx Counter Rate(HIT): 0 Packets per second
Weighed 5 minute average Tx Counter Rate(FRAME): 0 Packets per second
localIpAddr  : 10.0.0.1
remoteIpAddr : 57.50.50.50
gatewayIP    : 0.0.0.0
```

```
-----
| Tunnel IOCTL info |
-----
```

```
Rx Counter(HIT)      : 0
Tx Counter(FRAME)    : 0
```

```
-----
| Tunnel IOCTL info |
-----
```

```
Global Counter(FRAG)      : 0
Global Counter(DENY)      : 0
Global Counter(Uport Hit) : 0
Global Counter(SA MAC drop) : 0
Global Counter(MTU violation): 0
```

```
PvGre Tunnel Entries at Tunnel Glue
```

```
-----
TGindex : 0
Uport   : 0
EncapType : 4
Vlan ID : 1
```

```
-----
TGindex : 1
Uport   : 0
EncapType : 4
Vlan ID : 1
```

```
tunnelIndexDump
ifIndex      tunnel idx      ttl      MTU      lp      status      frame
count      tos
-----
0x0600014a   0x1c10         0x0040   0x05c5   00d1    (E)         0x00000000 0x00
0x0600014b   0x1c11         0x0040   0x05c5   00d1    (E)         0x00000000 0x00
```

IPATunnelshow

Tunnel Table

=====

Number of Configured Tunnels: 0
 Number of si Tunnels: 2
 Number of Remote Mirror Tunnels: 0

| IfIndex | Type | Prot | Flags | Vrf | Rte | Arp | localIpAddr/remoteIpAddr |
|-----------|------|------|--------|-----|-----|-----|--------------------------|
| 100663626 | 5 | 47 | 0x000a | 0 | 0 | -1 | 41.30.30.30/57.50.50.50 |
| 100663627 | 5 | 47 | 0x000a | 0 | 0 | -1 | 10.0.0.1/57.50.50.50 |

ipamShowTnlProbe 2

Sentinel Tunnels:

IP : 120.92.32.129
 VLAN : 1
 unresolved: 0

IP : 120.92.32.129
 VLAN : 1
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

IP : 0.0.0.0
 VLAN : 0
 unresolved: 0

```

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

```

```

Slot 1
tunnelRead
slot a:

```

```

-----
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| L |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| O | I |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| G | F |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   | I | L |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   | E |   | C |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| P | N |   | O | P |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   | D | R | O |   | M |   | M |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| O | C | U |   |   | U |   | M | T | T | C |   |   |   |   |   |   |   |   |   |   |   |
|   | E | A | R |   | A |   | A |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| R | A | N |   | N |   | T |   |   |   | O |   |   |   |   |   |   |   |   |   |   |   |
|   | X | M | T |   | C |   | C |   |   |   | P |   |   |   |   |   |   |   |   |   |   |
T | P | T |   | T |   | U | L | S | S |   |   |   |   |   |   |   |   |   |   |   |   |
|600014a|0010|1c10|2c59e50f20c0|000000000000|1e1e1e29|32323239|000000d4|0000|00d
1|GREv4|00000000|00000000|000005c5|40|00|01|

|600014b|0011|1c11|2c59e50f20c0|000000000000|0100000a|32323239|000000d4|0000|00d
1|GREv4|00000000|00000000|000005c5|40|00|01|

```

=== The command has completed successfully. ===

Example: show tech tunnel tap

```

HP-5406z1# show tech tunnel tap
show interfaces tunnel type tap

```

Status - Service Tunnel Information Brief

```

Max. Supported Tunnels : 4
Total Tunnels           : 2

```

```

Interface Index      : 100663627
Name                 : ServiceTunnel-02
Key                  : 212
Local Address        : 10.0.0.1
Remote Address       : 57.50.50.50
Interface State      : Down

```

```
Interface Index      : 100663626
Name                 : ServiceTunnel-01
Key                  : 212
Local Address        : 41.30.30.30
Remote Address       : 57.50.50.50
Interface State      : Down
```

show interfaces tunnel type tap statistics

Service Tunnel Information

Aggregate Statistics

MTU Violation Drop : 0

Service Tunnel Statistics

```
Interface Index      : 100663627
Name                 : ServiceTunnel-02
Tx Packets           : 0
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0
Tx Heartbeat        : 0
```

```
Interface Index      : 100663626
Name                 : ServiceTunnel-01
Tx Packets           : 0
Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0
Tx Heartbeat        : 0
```

```
ifmShowIPv4ServiceTunnels
Max. Supported Tunnels : 16
Total Tunnels          : 2
```

show arp

IP ARP table

| IP Address | MAC Address | Type | Port |
|------------|-------------|------|------|
|------------|-------------|------|------|

show ip route

IP Route Entries

| Destination | Gateway | VLAN | Type | Sub-Type | Metric | Dist. |
|--------------|---------|-----------|------|----------|--------|-------|
| 127.0.0.0/8 | reject | static | | 0 | 0 | |
| 127.0.0.1/32 | lo0 | connected | | 1 | 0 | |

show ip

Internet (IP) Service

IP Routing : Disabled

```
Default Gateway :
Default TTL     : 64
Arp Age        : 20
Domain Suffix   :
DNS server     :
```

Proxy ARP

| VLAN | IP Config | IP Address | Subnet Mask | Std | Local |
|--------------|------------|-------------|---------------|-----|-------|
| DEFAULT_VLAN | DHCP/Bootp | | | | |
| VLAN5 | Manual | 10.0.0.1 | 255.255.255.0 | No | No |
| VLAN6 | Manual | 41.30.30.30 | 255.255.255.0 | No | No |

show mac-address

Status and Counters - Port Address Table

```
MAC Address  Port  VLAN
-----
```

tgTunnelShowTech
SI Tunnel Show Tech

Tunnel Glue Uport Table

| Index | noRoleIndex | UifIndex | IPort | Status |
|-------|-------------|-----------|-------|-----------|
| 0 | 150995326 | 134218110 | 53 | Allocated |

OpenFlow Status : Disabled

Tunnel Glue Tunnel Entry Table

| Tunnel | Interface | Status |
|--------|-----------|-------------|
| 0 | 100663626 | Established |
| 1 | 100663627 | Established |

Tunnel Information for Tunnel : 0

PvGre Tunnel Entries at Tunnel Glue

```
ifIndex      : 100663626
TGstatus     : ESTABLISHED
FDstatus     : ESTABLISHED
TCAMstatus   : ESTABLISHED
UPORTstatus  : ESTABLISHED
Before       : 16
After        : 1
Uport        : 0
HwLogPort    : 209
gatewayIf    : 0
outLPortIf   : 0
GRE_key      : 212
encapType    : 4
vlan_id      : 1
gatewayMacAddr: 000000-000000
srcMacAddr   : 2C59E5-0F20C0
TTL          : 64
MTU          : 1468
TOS          : 0
Bandwidth    : 1024
Tunnel Status : Down No Route
Current Tx Counter Rate(FRAME): 0 Packets per second
Weighed 5 minute average Tx Counter Rate(FRAME): 0 Packets per second
localIpAddr  : 41.30.30.30
remoteIpAddr : 57.50.50.50
gatewayIP    : 0.0.0.0
```

```
-----
| Tunnel IOCTL info |
-----
Tx Counter(FRAME) : 0
```

Tunnel Information for Tunnel : 1

PvGre Tunnel Entries at Tunnel Glue

```

ifIndex      : 100663627
TGstatus    : ESTABLISHED
FDstatus    : ESTABLISHED
TCAMstatus  : ESTABLISHED
UPORTstatus : ESTABLISHED
Before      : 0
After       : 16
Uport       : 0
HwLogPort   : 209
gatewayIf   : 0
outLPortIf  : 0
GRE_key     : 212
encapType   : 4
vlan_id     : 1
gatewayMacAddr: 000000-000000
srcMacAddr  : 2C59E5-0F20C0
TTL         : 64
MTU         : 1468
TOS         : 0
Bandwidth   : 1024
Tunnel Status : Down No Route
Current Tx Counter Rate(FRAME): 0 Packets per second
Weighed 5 minute average Tx Counter Rate(FRAME): 0 Packets per second
localIpAddr : 10.0.0.1
remoteIpAddr : 57.50.50.50
gatewayIP   : 0.0.0.0
    
```

| Tunnel IOCTL info |

Tx Counter(FRAME) : 0

| Tunnel IOCTL info |

```

Global Counter(FRAG)      : 0
Global Counter(DENY)     : 0
Global Counter(Uport Hit) : 0
Global Counter(SA MAC drop) : 0
Global Counter(MTU violation): 0
    
```

PvGre Tunnel Entries at Tunnel Glue

```

-----
TGindex      : 0
Uport        : 0
EncapType    : 4
Vlan ID     : 1
    
```

```

-----
TGindex      : 1
Uport        : 0
EncapType    : 4
Vlan ID     : 1
    
```

tunnelIndexDump

| ifIndex | tunnel idx | ttl | MTU | lp | status | frame count | tos |
|------------|------------|--------|--------|------|--------|-------------|------|
| 0x0600014a | 0x1c10 | 0x0040 | 0x05c5 | 00d1 | (E) | 0x00000000 | 0x00 |
| 0x0600014b | 0x1c11 | 0x0040 | 0x05c5 | 00d1 | (E) | 0x00000000 | 0x00 |

IPATunnelshow

Tunnel Table
=====

```

Number of Configured Tunnels: 0
Number of si Tunnels: 2
Number of Remote Mirror Tunnels: 0
    
```

| IfIndex | Type | Prot | Flags | Vrf | Rte Rtdesc | Arp Rtdesc | localIpAddr/remoteIpAddr |
|-----------|------|------|--------|-----|------------|------------|----------------------------|
| 100663626 | 5 | 47 | 0x000a | | 0 | 0 | -1 41.30.30.30/57.50.50.50 |
| 100663627 | 5 | 47 | 0x000a | | 0 | 0 | -1 10.0.0.1/57.50.50.50 |

ipamShowTnlProbe 2

Sentinel Tunnels:

```

IP      : 120.92.32.129
VLAN    : 1
unresolved: 0

IP      : 120.92.32.129
VLAN    : 1
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

IP      : 0.0.0.0
VLAN    : 0
unresolved: 0

```


Slot 1

tunnelRead

slot a:

```

-----
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| L |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| I |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| O |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| F |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| G |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| I |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| E |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| N |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| P |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| D |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| O |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| E |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| R |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| X |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| T |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|600014a|0010|1c10|2c59e50f20c0|000000000000|1e1e1e29|32323239|000000d4|0000|00d
1|GREv4|00000000|00000000|000005c5|40|00|01|

|600014b|0011|1c11|2c59e50f20c0|000000000000|0100000a|32323239|000000d4|0000|00d
1|GREv4|00000000|00000000|000005c5|40|00|01|

```

=== The command has completed successfully. ===

Troubleshooting

This section lists the different failure scenarios associated with service tunnels along with possible failure cause and troubleshooting information.

Tunnel creation

| ID | Issue | Possible cause | Troubleshooting help |
|----|--|--|--|
| 1 | Failed error: SNMP_ERRORSTATUS_COMMITFAILED | <ul style="list-style-type: none"> Cannot create a service tap tunnel because a mirror session is not available. No more tunnels can be created. The maximum number is 4. | You must have a mirror session available to create a service tap tunnel. |
| 2 | Wrong value error: SNMP_ERRORSTATUS_WRONGVALUE | <ul style="list-style-type: none"> Tunnel DSCP values of -2 and -1 are not supported. Truncate option is not supported in SI tunnels. | <ul style="list-style-type: none"> Choose a value other than -2 and -1 for your DSCP tunnel. Do not use the truncate option for SI intercept tunnels. |
| 3 | User tries to create a service tunnel and gets the following SNMP error: SNMP_ERRORSTATUS_WRONGVALUE | <p>Incorrect endpoint address</p> <ul style="list-style-type: none"> If local endpoint IP address of the tunnel interface is not a valid switch VLAN interface IP address, a tunnel cannot be created. <p>Note that DHCP assigned local IP addresses or OOBM interface IP addresses are not considered to be valid local endpoint addresses.</p> <ul style="list-style-type: none"> If the remote endpoint IP address is a multicast address, a tunnel cannot be created. If the to-be-created tunnel's remote endpoint IP address is the same as one of switch's interface IP addresses, a tunnel cannot be created. | <p>To know what the error is do an SNMP WALK on hpSwitchErrorMsgEntry MIB object. This will display a message as to why the SET request failed.</p> <p>For example, in the case of an 'invalid local IP' case, the error message would be as follows:</p> <pre>hpSwitchEntityErrorMsg.2.1.49.27 = Cannot create Service Tunnel because the specified source IP address is not configured on any interface.</pre> <p>To know the list of configured IP addresses on a device, run the following CLI command</p> <pre>switch# show ip</pre> <p>All configured interface IP addresses get listed here. The tunnel's local IP address should be one of the IP addresses listed here.</p> <p>Relevant MIB objects:</p> <pre>ipAddressTable (RFC 4293 MIB)</pre> |
| 4 | User tries to create a service tunnel and gets the following SNMP error: SNMP_ERRORSTATUS_WRONGVALUE | <p>Incorrect encapsulation parameters</p> <ul style="list-style-type: none"> If the GRE Key of the tunnel being created is 0, a tunnel cannot be created. If the encapsulation method is set to non-GRE type, a tunnel cannot be created. | Do an SNMP walk on hpSwitchErrorMsgEntry MIB object. This will display a message as to why the SET request failed. |
| 5 | User tries to create a service tunnel and gets the following SNMP error: SNMP_ERRORSTATUS_INCONSISTENTVALUE | <p>Exclusive features</p> <p>The following switch features are mutually exclusive with service tunnels and if they are already enabled, service tunnels cannot be created.</p> <ul style="list-style-type: none"> Distributed Trunk IPv4/IPv6 multicast routing QinQ Mesh MAC Mirror | <p>Do an SNMP walk on hpSwitchErrorMsgEntry MIB object. This will display a message as to why the SET request failed.</p> <p>Run the following CLI commands to know if any of the mutually exclusive features are already enabled.</p> <pre>DT switch# show trunks Port Name Type Group Type ----- 1 xyz 100/1000T Trk1 dt-lacp 2 xyz 100/1000T Trk1 dt-trunk</pre> <p>Trunk Type dt-lacp or dt-trunk implies Distributed Trunking configuration.</p> <p>Relevant MIB objects:</p> |

| ID | Issue | Possible cause | Troubleshooting help |
|----|---|---|--|
| | | | <p>hpSwitchPortTable (hpSwitchConfig MIB)</p> <p>IP MCAST</p> <pre>switch# show running-config ip multicast-routing</pre> <p>Look for the above line which indicates that multicast routing is enabled on the device.</p> <p>Relevant MIB objects:</p> <p>ipMRouteEnable (RFC 2932 MIB)</p> <p>QinQ</p> <pre>switch# show qinq</pre> <p>QinQ configuration information: ----- Mode : svlan (or mixedvlan)</p> <p>If the qinq mode is svlan or mixedvlan, it means qinq is enabled on the device.</p> <p>Relevant MIB objects:</p> <p>hpicfProviderBridgeType (hpicfProviderBridge MIB)</p> <p>Mesh</p> <pre>switch# show mesh</pre> <p>MAC Mirror</p> <pre>switch# show mac-mirror</pre> |
| 6 | <p>User tries to create a service tunnel and gets the following SNMP error:</p> <pre>SNMP_ERRORSTATUS_RESOURCEUNAVAILABLE</pre> | <p># of tunnels limit</p> <p>There is a limit on the number of tunnels that can be configured on a device and once that limit has been reached, any further tunnel creation will be errored out.</p> | <p>Do an SNMP walk on hpSwitchErrorMsgEntry MIB object. This will display a message as to why the SET request failed.</p> <p>Run the following CLI command:</p> <pre>switch# show interface tunnel type intercept</pre> <p>Max. Supported Tunnels : 16 Total Tunnels : 16</p> <p>The 'total tunnels' field is the current number of tunnels configured on the box while 'max tunnels' is the limit.</p> <p>Relevant MIB objects:</p> <p>hpicfMaxIPv4ServiceTunnels hpicfTotalIPv4ServiceTunnels (hpicfServiceTunnels MIB)</p> |
| 7 | <p>User tries to create a service tunnel and gets the following SNMP error:</p> <pre>SNMP_ERRORSTATUS_RESOURCEUNAVAILABLE</pre> | <p>No V1 line card support</p> <p>On 5400 chassis platforms, tunnels cannot be created when the chassis has been configured to run in v1-compat-mode.</p> | <p>Do an SNMP walk on hpSwitchErrorMsgEntry MIB object. This will display a user friendly message as to why the SET request failed.</p> <p>Run the following CLI command to check if the device is running in v1-compat mode.</p> <pre>switch# show system</pre> <p>Allow V1 Modules : Yes</p> <p>This means the device is in V1 compat mode.</p> <p>Relevant MIB objects:</p> <p>hpSwitchAllowV1Modules (hpSwitchConfig MIB)</p> |

| ID | Issue | Possible cause | Troubleshooting help |
|----|--|--|--|
| 8 | User tries to create a service tunnel and gets the following SNMP error: SNMP_ERRORSTATUS_RESOURCEUNAVAILABLE | No platform support Tunnels cannot be created on 3500/6200/6600 platforms and SMB platforms. | Do an SNMP walk on hpSwitchErrorMsgEntry MIB object. This will display a message as to why the SET request failed. |
| 9 | User tries to create a service tunnel and gets the following SNMP error: SNMP_ERRORSTATUS_RESOURCEUNAVAILABLE | No hardware resource Tunnel needs free TCAM entries on all slots to be available for creation. Unavailability of these resources results in tunnel creation failure. | Do an SNMP walk on hpSwitchErrorMsgEntry MIB object. This displays a message as to why the SET request failed. Run the following CLI command and check if TCAM resources are available. switch# show qos resources Look at the 'Rules available' and 'Meters available' column for all slots (or port groups). For the first service tunnel to be created - 'Rules available' must be >= 26 and 'Meters available' must be >= 2. For subsequent service tunnels to be created - 'Rules available' must be >= 6 |

Tunnel operational status

| D | Issue | Possible cause | Troubleshooting help |
|---|---|--|---|
| 1 | Tunnel's operstatus is reported as DOWN in the CLI or Event logs or via OpenFlow. | Network connectivity issue <ul style="list-style-type: none"> The tunnel endpoint is on a directly connected subnet but down (not responding to ARP requests). The tunnel endpoint is not on a directly connected subnet and there is no IP route on the switch to reach the tunnel endpoint IP address. The tunnel endpoint is not on a directly connected subnet, there is an IP route on the switch to reach the endpoint IP address but the corresponding nexthop is down (not responding to ARP requests). The uplink interface on the switch via which the endpoint or gateway is reachable is down. | Run the following CLI command to check for tunnel endpoint IP resolution status. switch# show interface tunnel type intercept Status Interface State : Down Down Reason : No route to destination Destination Address Route : Next Hop IP : Next Hop Interface : Next Hop IP Link Status : Source Address : Egress port : Look for the 'State' field being 'Down' and also the 'Down Reason' and 'Next Hop' related fields below this field. If there is no route to the destination, the Nexthop fields would be empty. Check the IP route table, gateway availability and uplink interface status to troubleshoot further. |
| 2 | Tunnel's operstatus is reported as DOWN in the CLI or Event logs or OpenFlow. | ASIC component failure Loopback port going down can result in tunnels momentarily going down (software picks a new loopback port as soon as the current loopback port goes down). Note that a loopback port goes down only when a line card that | Look for the following message in the event logs: Service Tunnel decapsulation interface flap - Packets may have been dropped. When the last line card goes down, the tunnel will be reported as down until a new line card comes up again. |

| D | Issue | Possible cause | Troubleshooting help |
|---|-------|--|---|
| | | <p>houses the loopback port goes down. There is one loopback port on every linecard and so if one linecard goes down, another linecard's loopback port will start handling tunnel packets.</p> <p>During the transition, tunneled packets can be dropped.</p> <p>On stackable platforms, each port group represents the equivalent of one linecard and has one loopback port. If a port group is down, a loopback port from another port group will handle tunneled packets.</p> | <p>Run the following CLI command to know if the tunnel is down due to resource unavailability.</p> <pre>switch# show interface tunnel type intercept Status Interface State : Down Down Reason : Out of resources</pre> <p>Look for the "Down Reason" field in the output that indicates there are no ASIC resources.</p> |

Encapsulation path - traffic steering to tunnel (via OpenFlow)

| ID | Issue | Possible cause | Troubleshooting help |
|----|--|---|---|
| 1 | FlowMod failure when trying to program an OpenFlow rule that is diverting packets to a tunnel interface. | <p>Invalid tunnel ifindex</p> <p>The tunnel ifindex in an OF FlowMod must match a configured tunnel interface's ifIndex.</p> <p>Otherwise, the FlowMod will fail.</p> | <p>Run the following CLI command and check if the ifindex in the OpenFlow Flow Mod rule is valid.</p> <pre>switch\$ show interface tunnel type intercept Interface Index : 1000000001</pre> <p>Relevant MIB objects:</p> <pre>tunnelInetConfigIfIndex (rfc4087 MIB)</pre> <p>From an OF response perspective, the flow mod request will be rejected with error type="BAD_ACTION", code="BAD_OUT_PORT"</p> |
| 2 | FlowMod failure when trying to program an OpenFlow rule that is diverting packets to a tunnel interface. | <p>OpenFlow 1.0 instance</p> <p>OpenFlow Forwarding to a tunnel interface is only supported on 1.3 instances.</p> <p>If the instance is a 1.0, the FlowMod will fail.</p> | NA |

| ID | Issue | Possible cause | Troubleshooting help |
|----|--|--|--|
| 3 | FlowMod failure when trying to program an OpenFlow rule that is diverting packets to a tunnel interface. | <p>Tunnel 'outport action' limitations</p> <p>There are some restrictions with using Tunnels as outports as listed here:</p> <ul style="list-style-type: none"> • For Intercept tunnels only: Cannot add tunnel interface as one of the ports in a multi-port output action. • For Intercept tunnels only: Cannot club a flow-rule's output action of sending packets to a tunnel with "Normal" or "SendToController" actions. • Cannot club a flow-rule's output action of sending packets to a tunnel with OpenFlow Strip-VLAN action as the inner encapsulated packets will always be VLAN tagged. • Tunnel interface cannot be part of a FLOOD action. | The flow mod request will be rejected with error type="BAD_ACTION", code="BAD_OUT_PORT". |
| 4 | FlowMod failure when trying to program an OpenFlow rule that is diverting packets to a tunnel interface. | <p>Limitations with OpenFlow tables and tunnels</p> <p>The outport action for tunnel interfaces is only supported on the Policy Engine (TCAM) tables and not on the other tables including the OpenFlow software tables.</p> | The flow mod request is rejected with error type="BAD_REQUEST", code="BAD_TABLE_ID". |
| 5 | FlowMod failure when programming OpenFlow rules with in_port as tunnel IfIndex. | <p>Match criteria limitations with tunnels</p> <p>Tunnel Interfaces cannot be used as a match field (IN_PORT) in OpenFlow rules.</p> | The flow mod request is rejected with error type="BAD_ACTION", code="BAD_ARGUMENT". |
| 6 | DNS/IP packets not sent out to the tunnel. | <p>Higher precedence rule</p> <p>Another higher precedence OpenFlow rule matched instead of the DNS/IP match rule.</p> | <p>Check if there are overlapping rules with higher precedence compared to tunnel rules.</p> <p>If so, check the packet counts of the higher precedence overlapping rules to see if they are incrementing.</p> |
| 7 | DNS/IP packets not sent out to the tunnel. | <p>Packet encapsulation failure</p> <p>If the tunnel is UP and packets are matching an OpenFlow rule that is directing traffic to the tunnel but packets are not being sent to the</p> | <p>Run the following CLI command to know if there are MTU violations causing packets to not be tunneled.</p> <pre>switch\$ show interface tunnel type intercept statistics</pre> |

| ID | Issue | Possible cause | Troubleshooting help |
|----|--|---|---|
| | | <p>controller, it could be for one of the following reasons</p> <ul style="list-style-type: none"> • MTU violation during encapsulation can cause packets to be dropped. • Uplink interface drops (link congestion). • Network congestion in the upstream network. | <p>Service Tunnel Statistics MTU Violation Drop : 10</p> <p>Relevant MIB objects: hpicfServiceTunnelStatsMTUViolationDrop (hpicfServiceTunnels MIB)</p> <p>If there are no MTU violation related drops, run the following command to know if there are uplink interface TX drops.</p> <p>To do that, first determine the uplink interface that this tunnel uses by running the “show interface tunnel type intercept” command and identify the ‘Egress port’.</p> <pre>switch\$ show interface <port></pre> <p>Look for TX drop counters on this interface.</p> |
| 8 | DNS/IP packets not sent out to the tunnel. | <p>Stale tunnels</p> <p>When a tunnel is deleted but an OpenFlow rule that is diverting packets to that tunnel interface is still not removed, packets to the stale tunnels are dropped.</p> | <p>Run the following CLI command and check if the ifindex in the tunnel used is valid.</p> <pre>switch\$ show interface tunnel type intercept</pre> <p>Interface Index : 1000000001</p> <p>Relevant MIB objects: tunnelInetConfigIfIndex (rfc4087 MIB)</p> <p>Also in this case, the tunnel rule hit count increases as packets match the tunnel rule.</p> |

Decapsulation path

The Decapsulation path applies to Intercept tunnels only. It does not apply to Tap tunnels.

| ID | Issue | Possible cause | Troubleshooting help |
|----|--|--|---|
| 1 | Tunneled packets received from the remote endpoint not decapsulated at the switch. | <p>GRE Key incompatibility</p> <p>If the GRE KEY in the encapsulated packet does not match one of the configured tunnels’ GRE KEY values, encapsulated packets can be dropped.</p> | <p>Run the following CLI command to know if there are drops due to GRE KEY incompatibilities.</p> <pre>switch\$ show interface tunnel type intercept statistics</pre> <p>Service Tunnel Statistics Packets to Non-Existent Tunnels: 200</p> <p>If this counter is incrementing, it means there is GRE KEY incompatibility in traffic inbounds on one or more tunnels.</p> <p>Relevant MIB objects hpicfServiceTunnelStatsRxInvalidKey (hpicfServiceTunnels MIB)</p> |
| 2 | Encapsulated packets received from the remote endpoint not decapsulated at the switch. | <p>IP fragmentation</p> <p>If the GRE KEY matched that of a configured tunnel but the packet was a fragmented frame (‘More Fragments Bit’ set), the switch</p> | <p>Run the following CLI command to know if there are drops due to fragmentation.</p> <pre>switch\$ show interface tunnel type intercept statistics</pre> <p>Service Tunnel Statistics</p> |

| ID | Issue | Possible cause | Troubleshooting help |
|----|---|---|---|
| | | cannot re-assemble these frames and therefore will drop them. | Fragmented Packets Dropped (Rx) : 100 If this counter is incrementing, it means there is fragmented traffic inbound on one or more tunnels. Relevant MIB objects hpicfServiceTunnelStatsRxFragmentDrops (hpicfServiceTunnels MIB) |
| 3 | Decapsulated packets not forwarded out by the switch. | Loopback interface oversubscription Decapsulated packets (from all tunnels) hit the loopback port and are re-inserted to the ASIC for a second pass processing. This port has a 1G capacity and oversubscription on this port can cause packets to be dropped. | Look for the following message in the event logs: Packets dropped due to oversubscription on tunnel decapsulation interface. |
| 4 | Decapsulated packets not forwarded out by the switch. | Source MAC address not learned All decapsulated packets that hit the loopback port are re-inserted to the ASIC for a second pass processing. In this pass, the SRC MAC of the decapsulated frame must have already been learned on the packet's inbound VLAN. If not, such traffic will be dropped. Note that if the VLAN in the decapsulated packet is not configured on the device, packets will be dropped as well. | Run the following CLI command to know if there are drops due to SRC MAC lookup failure. HP-E8206z1# show interface tunnel type intercept statistics Service Tunnel Statistics Unknown Source MAC Packets Dropped (Rx): 200 If this counter is incrementing, it means there is traffic on the loopback interface that has failed the 'SRC MAC on the inbound VLAN' lookup. |

Other tunnel specific troubleshooting commands

| ID | Purpose | CLI command or other |
|----|---|---|
| 1 | Tunnel interface TX/RX packet counters (tunnel and heartbeat packets) | HP-E8206z1# show interface tunnel type intercept statistics 1000000001 Aggregate Statistics Fragmented Packets Dropped (Rx) : 0 Packets to Non-Existent Tunnel : 0 Unknown Source MAC Packets Dropped (Rx) : 0 MTU Violation Drop : 0 Per Tunnel Statistics Interface Index : 100663874 Name : ServiceTunnel-01 Rx Packets : 0 Tx Packets : 0 Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0 Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0 Rx Heartbeat : 0 Tx Heartbeat : 0 Last Recv Heartbeat Timestamp : 01/01/90 00:00:00 |
| 2 | Tunnel interface TX/RX packet rate | HP-E8206z1# HP-E8206z1# show interface tunnel type intercept statistics 1000000001 Aggregate Statistics Fragmented Packets Dropped (Rx) : 0 Packets to Non-Existent Tunnel : 0 |

| ID | Purpose | CLI command or other |
|----|--|---|
| | | <pre> Unknown Source MAC Packets Dropped (Rx) : 0 MTU Violation Drop : 0 Per Tunnel Statistics Interface Index : 100663874 Name : ServiceTunnel-01 Rx Packets : 0 Tx Packets : 0 Rx 5 Minute Weighted Average Rate (Pkts/sec) : 0 Tx 5 Minute Weighted Average Rate (Pkts/sec) : 0 Rx Heartbeat : 0 Tx Heartbeat : 0 Last Recv Heartbeat Timestamp : 01/01/90 00:00:00 </pre> |
| 3 | Debug logging for various tunnel related events | HP-E8206z1# debug tunnel intercept |
| 4 | Show Tech command | <pre>HP-E8206z1# show tech tunnel intercept</pre> <p>Dumps all tunnel related information including</p> <ul style="list-style-type: none"> • Statistics • ASIC encapsulation table contents • ASIC decapsulation rules • loopback port information etc • Tunnel endpoint resolution status |
| 5 | Clearing tunnel counters | HP-E8206z1# clear interfaces tunnel type intercept statistics |
| 6 | Clear/delete tunnels from CLI | HP-E8206z1# clear interfaces tunnel type intercept |
| 7 | Notifications for following events: <ul style="list-style-type: none"> • Tunnel Create • Tunnel Delete • Tunnel Up • Tunnel Down | Asynchronous notifications: <ul style="list-style-type: none"> • RMON Logs • SNMP Traps • OpenFlow PORT STATUS message |
| 8 | Capability to parse an encapsulated packet (with wireshark) | The switch encapsulates the GRE payload with protocol type set to 'Transparent Ethernet Bridging (0x6558)'. This is a standard encapsulation type that wireshark can natively understand and be able to dissect and display packet contents including payload information. |

2 Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
 - Hewlett Packard Enterprise Support Center **Get connected with updates** page:
www.hpe.com/support/e-updates
 - Software Depot website:
www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials

① **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

| Website | Link |
|--|--|
| Hewlett Packard Enterprise Information Library | www.hpe.com/info/enterprise/docs |
| Hewlett Packard Enterprise Support Center | www.hpe.com/support/hpesc |

| Website | Link |
|---|--|
| Contact Hewlett Packard Enterprise Worldwide | www.hpe.com/assistance |
| Subscription Service/Support Alerts | www.hpe.com/support/e-updates |
| Software Depot | www.hpe.com/support/softwaredepot |
| Customer Self Repair | www.hpe.com/support/selfrepair |
| Insight Remote Support | www.hpe.com/info/insightremotesupport/docs |
| Serviceguard Solutions for HP-UX | www.hpe.com/info/hpux-serviceguard-docs |
| Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix | www.hpe.com/storage/spock |
| Storage white papers and analyst reports | www.hpe.com/storage/whitepapers |

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

NOTE: There has been a change to the style of the documentation with the newest release. The "Command Table" commonly seen at the beginning of the chapters has been replaced with the ability to search for commands using the index. All commands are now listed in the index within the category "Command syntax".

Index

A

- accessing
 - updates, 34
- applicable HPE switches, 1

C

- clear interfaces tunnel, 14
- contacting Hewlett Packard Enterprise, 34
- customer self repair, 35

D

- debug tunnel intercept, 15
- documentation
 - providing feedback on, 35

H

- hardware IP tunnels, 5

I

- inspection service, 4

O

- OpenFlow and service tunnel restrictions, 8
- OpenFlow and service tunnels, 7

R

- remote support, 35

S

- service insertion, 4
- service tunnel restrictions with other features, 9
- show interface tunnel, 9
- show monitor, 15
- show tech tunnel intercept, 15
- support
 - Hewlett Packard Enterprise, 34

T

- troubleshooting, 25
- tunnel Aliveness check using OpenFlow, 6
- tunnel creation, 5
- tunnel deletion, 6

U

- updates
 - accessing, 34

W

- websites, 34
 - customer self repair, 35