Hewlett Packard Enterprise

HPE Synergy 40Gb F8 Switch Module

IP Configuration

Abstract

This document is intended for the person who configures HPE Synergy 40Gb F8 Switch Modules.

20150731a
March 2017
Edition: 1

Contents

Figures

Tables

Introduction

The **HPE IP** (Internet Protocol) is a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite. It has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

This chapter describes the purpose and scope of the document, conventions and acronyms used in this document.

Purpose and Scope

This document describes the basic and advanced configuration tasks of **HPE IP**. CLI (Command Line Interface) commands and SNMP (Simple Network Management Protocol) interfaces are used for the configuration. System administrators and users who configure and maintain **HPE IP** use this document

This document describes the configuration of specific features, in a step by step manner using sample values. Refer to the *HPE Synergy 40Gb F8 Switch Module Command Line Interface (CLI) Guide* for a detailed explanation of the configuration parameters and the related values, if any.

Acronyms

Table1: Acronyms Used in this Document

Acronym	Explanation
ARP	Address Resolution Protocol
BOOTP	BOOTstrap Protocol
CIDR	Classless Inter Domain Routing
ICM	Interconnect Module
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
InARP	Inverse ARP
Id	Identifier
IP	Internet Protocol
IRDP	ICMP Router Discovery Protocol
OSPF	Open Shortest Path First Protocol
PPP	Point-to-Point Protocol
RARP	Reverse Address Resolution Protocol
RFC	Request For Comments

Acronym	Explanation
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VAR	Value Added Reseller
VC	Virtual Circuit
MRP	Multicast Routing Protocol
RRD	Route Redistribution
RTM	Route Table Manager

References

HPE Synergy 40Gb F8 Switch Module Command Line Interface (CLI) GuideDocument Conventions

Table 2 lists the terms and typographical conventions used in this document.

Table 2: Conventions Used in this Document

Convention	Usage	Example
Arial Bold 10	CLI (Command Line Interface) Commands	**switch# configure terminal**
Arial 10 Italics	User Inputs to Command	**switch(switch(config)# ip vrf** *vrf1*

`Courier New 10 Regular, blue color`	CLI Command output	**switch# show ip vrf vrf3**
		`VcId VRF-Name Interfaces`
		`---- -------- ----------`
		`1 vrf3 Gi0/7, Gi0/8`

.	Notes. These topics convey additional information on an associated topic.	

	Output of the configured value	**switch# show ip vrf vrf3**
		`VcId VRF-Name Interfaces`
		`---- -------- ----------`
		`1 vrf3 Gi0/7, Gi0/8`

Protocol Description

The **HPE IP** software is a portable implementation of the industry standard IP forwarding protocol. It implements all the components required for IP

forwarding. The various components of **HPE IP** include ARP, RARP, RTM, ICMP, IRDP, IGMP, InARP, BOOTP, TFTP, TRACE ROUTE, PING and UDP.

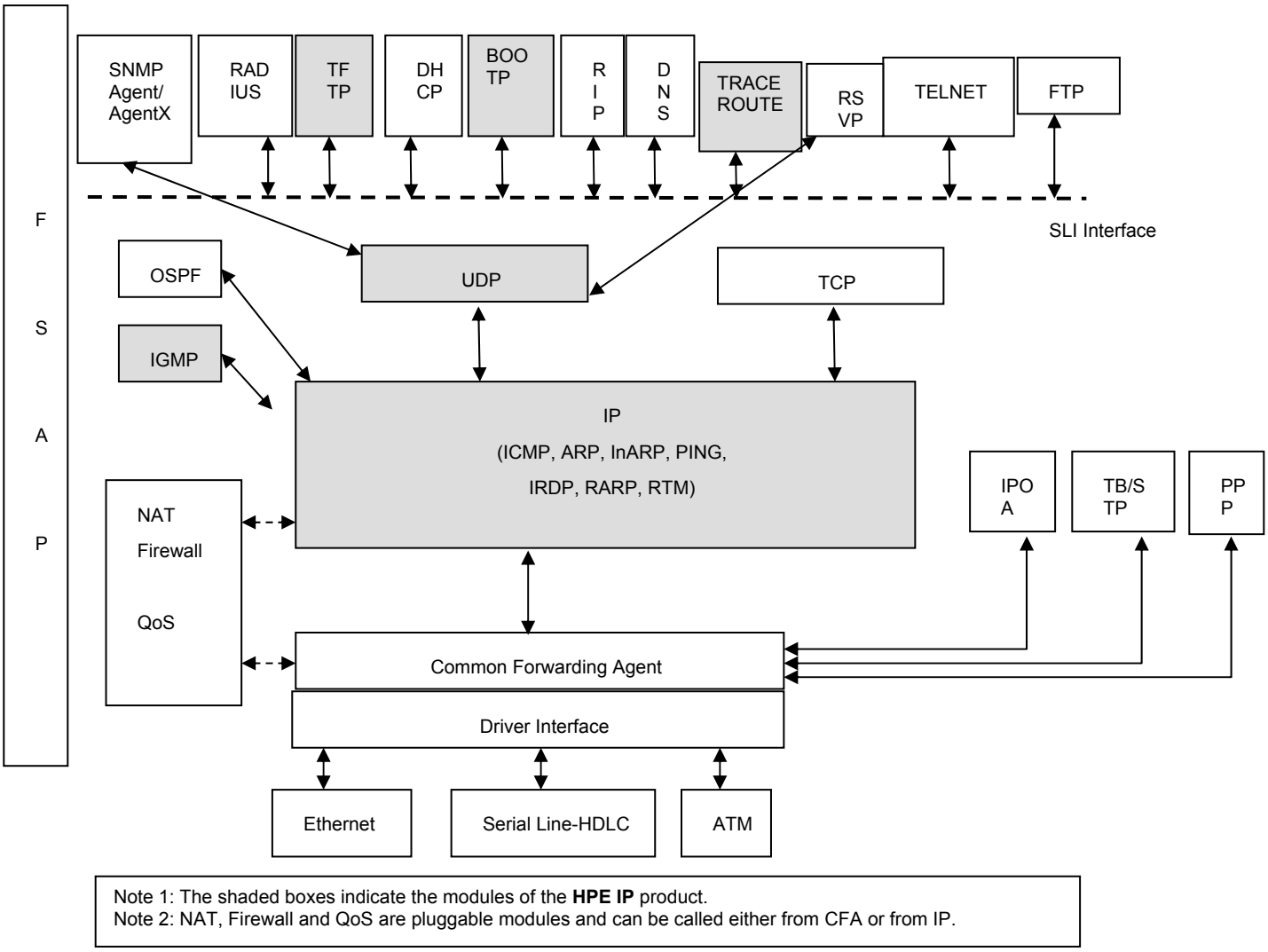

Figure 1: Product position in IP stack

Topologies

This chapter provides sample deployment scenarios used for the configuration steps given in this document. Figure 2 depicts the sample topology used for configuring and testing the basic features of **HPE IP**.

Topology for Testing HPE IP

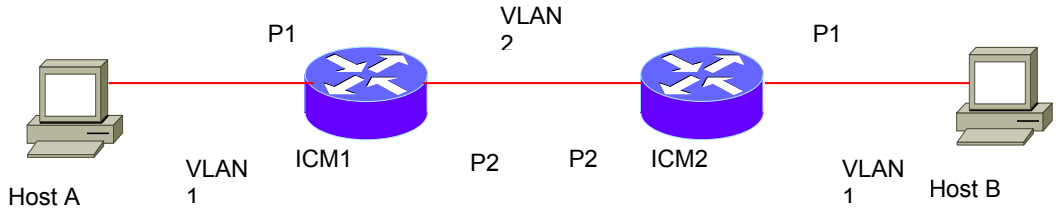

Figure 2: Topology for HPE IP

* P1 and P2 represent the port numbers of the ICM switches

The Table 3 lists the IPv4 addresses of all the interfaces in the switches and the hosts.

Table 3: IPv4 Addresses of Interfaces in the Switches and Hosts – HPE IP

Switch / Host	Interface of ICM Switches	IPv4 Address / Mask
ICM1 (ICM switch)	VLAN 1	40.0.0.1 / 255.0.0.0
	VLAN 2	50.0.0.1 / 255.0.0.0
ICM1 (ICM switch)	VLAN 2	50.0.0.10 / 255.0.0.0
	VLAN 1	60.0.0.1 / 255.0.0.0
Host A (host device connected ICM1)		40.10 / 255.0.0.0
Host B (host device connected ICM2)		60.10 / 255.0.0.0

Topology for Testing Route Redistribution in IP

Figure 3 depicts the sample topology used for configuring route redistribution in IP.

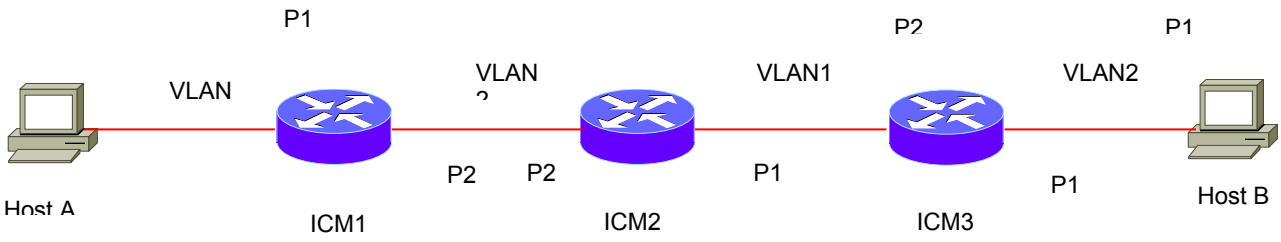

Figure 3: Topology for Redistribution

Table 4 lists the IPv4 addresses of all the interfaces in the switches and the hosts

Table 4: IPv4 Addresses of Interfaces in the Switches and Hosts – Route Redistribution

Switch / Host	Interface of ICM Switches	IPv4 Address / Mask
ICM1 (ICM switch)	VLAN 1	40.0.0.1 / 255.0.0.0
	VLAN 2	50.0.0.1 / 255.0.0.0

ICM2 (ICM switch)	VLAN 2	50.0.0.10 / 255.0.0.0
	VLAN 1	60.0.0.1 / 255.0.0.0
ICM3 (ICM switch)	VLAN 1	60.0.0.10 / 255.0.0.0
	VLAN 2	70.0.0.1 / 255.0.0.0
Host A (host device connected ICM)		40.0.0.10 / 255.0.0.0
Host B (host device connected ICM)		70.0.0.10 / 255.0.0.0

Topology for Testing BFD Over Static IP

Figure 4 depicts the sample topology used for configuring and testing BFD

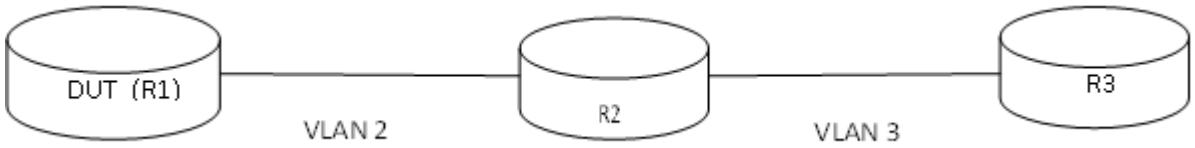

Figure 4: BFD Configuration and Testing Topology

Figure 4 depicts the components used in the topology. The description is as follows,

- R1, R2 and R3 represent routers in which ICM is installed.
- VLAN2 and VLAN3 represent the VLAN interfaces of the ICM routers.
- Each ICM switch has a router ID.(Table 5 lists the IPv4 and IPv6 addresses of the interfaces and hosts provided in the Figure 4

Table 5: IPv4 and IPv6 Addresses of Interfaces in the Routers and Hosts

Router / Host	Interface	Slot	IPv4 Address / Mask	IPv6 Address / Prefix Length
R1	Vlan2	0/2	20.0.0.1 / 255.0.0.0	fec0::2222:0:1 / 96, 2222::1/96
R2	Vlan2	0/2	20.0.0.2 / 255.0.0.0	fec0::2222:0:2 / 96, 2222::2/96
	Vlan3	0/3	30.0.0.2 / 255.0.0.0	fec0::3333:0:2 / 96, 3333::2/96
R3	Vlan3	0/2	30.0.0.3 / 255.0.0.0	fec0::3333:0:3 / 96, 3333::3/96

General Configurations

The **HPE IP** is configurable and managed by CLI and SNMP interfaces. This chapter describes the preliminary configurations of **HPE IP.**

Default Configurations

Table 6 lists the default configurations of **HPE IP**.

Table 6: Default Configurations

Parameter	Default Configuration

Parameter	Default Configuration
ICMP Redirect messages	Enabled
ICMP unreachable messages	Enabled
ICMP Redirect messages	Enabled
ICMP Redirect messages	Enabled
IP rarp client request interval	100
IP rarp client request retries	4
Path MTU discovery	Disabled
Aggregate Routes	50
Multi paths	2
Load sharing	Disabled
Directed broadcast	Disabled
Proxy-ARP	Disabled
Proxy ARP subnet check	Enabled
Ping packet-size	40
Ping packet-count	3
Ping time-out	1 sec
IP vrf	Default
IP Routing	Enabled
IP Time–to–Live	64 sec
ARP Time out	7200 (300)
ARP Max retries	3
IPv4 enable	Enable

Basic CLI Command Modes

Table 7 lists the command modes, access and exit methods of the modes and the prompt displayed in the modes.

Table 7: CLI Command Modes

Command Mode	Access Method	Prompt	Exit method
User EXEC	This is the initial mode to start a session.	**switch>**	The logout method is used.
Privileged EXEC	The User EXEC mode command **enable** is used to enter the Privileged EXEC mode.	**switch#**	The command **disable** is used to return to User EXEC mode from the Privileged EXEC mode.
Global Configuration	The Privileged EXEC mode command **configure terminal** is used to enter the Global Configuration mode	**switch(switch(config)#**	The command **exit / end** is used to exit to the Privileged EXEC mode.
Interface Configuration	The Global Configuration mode command **interface**	**switch(config-if)#**	The command **exit** is used to exit to the

	<interface-type><interface-id> is used to enter the Interface configuration mode.		Global Configuration mode. The command **end** is used to exit to the Privileged EXEC mode.
Router Configuration	The protocol specific Global Configuration mode router command (such as **router rip**) is used to enter into the Router Configuration mode.	**switch(config-router)#**	The command **exit** is used to exit to the Global Configuration mode. The command **end** is used to exit to the Privileged EXEC mode.
VLAN (Virtual LAN) Configuration	The Global Configuration mode command **vlan <vlan no>** is used to enter the VLAN Configuration mode	**switch(config-vlan)#**	The command **exit** is used to exit to the Global Configuration mode. The command **end** is used to exit to the Privileged EXEC mode.

Configuring ICM1 in Topology for HPE IP

Execute the following commands to configure ICM1 in Figure 2.

switch#configure terminal;

switch(config)#interface vlan *1***;**

switch(config-if)#shutdown;

switch(config-if)#ip address *40.0.0.1 255.0.0.0;*

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan 1;

switch(config-vlan)#ports TwentyGigE 0/1/1 untagged TwentyGigE 0/1/1;

switch(config-vlan)#exit;

switch(config)#interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *1***;**

switch(config-if)#no shutdown;

switch(config-if)#exit

switch(config)#interface vlan *2***;**

switch(config-if)#shutdown;

switch(config-if)#ip address *50.0.0.1 255.0.0.0***;**

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *2;*

switch(config-vlan)#ports TwentyGigE 0/1/1 ;

switch(config-vlan)#exit;

switch(config)interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *2*;

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#ip route *60.0.0.0 255.0.0.0 50.0.0.10;*

switch(config)#exit;

switch#show ip interface;

switch#show ip route;

Configuring ICM2 in Topology for HPE IP

Execute the following commands to configure ICM2 in Topology for HPE IP.

switch#configure terminal;

switch(config)#interface vlan *1*;

switch(config-if)#shutdown;

switch(config-if)#ip address *60.0.0.1 255.0.0.0;*

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *1*;

switch(config-vlan)#ports TwentyGigE 0/1/1 untagged TwentyGigE 0/1/1*;*

switch(config-vlan)#exit;

switch(config)#interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *1*;

switch(config-if)#no shutdown;

switch(config-if)#exit

switch(config)#interface vlan *2*;

switch(config-if)#shutdown;

switch(config-if)#ip address *50.0.0.10 255.0.0.0;*

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *2;*

switch(config-vlan)#ports TwentyGigE 0/1/1 ;

switch(config-vlan)#exit;

switch(config)interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *2*;

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#ip route *40.0.0.0 255.0.0.0 50.0.0.1;*

switch(config)#exit;

switch#show ip interface;

switch#show ip route;

Configuring ICM1 in Topology for Redistribution

Execute the following commands to configure ICM1 in Topology for Redistribution.

switch#configure terminal;

switch(config)#interface vlan *1*;

switch(config-if)#shutdown;

switch(config-if)#ip address *40.0.0.1 255.0.0.0*;

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *1*;

switch(config-vlan)#ports TwentyGigE 0/1/1 untagged TwentyGigE 0/1/1;

switch(config-vlan)#exit;

switch(config)#interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *1*;

switch(config-if)#no shutdown;

switch(config-if)#exit

switch(config)#interface vlan *2;*

switch(config-if)#shutdown;

switch(config-if)#ip address *50.0.0.1 255.0.0.0;*

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *2*;

switch(config-vlan)#ports TwentyGigE 0/1/1 ;

switch(config-vlan)#exit;

switch(config)interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *2*;

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#exit;

switch#show ip interface;

switch#show ip route;

Configuring ICM2 in Topology for Redistribution

Execute the following commands to configure ICM2 in Topology for Redistribution.

switch#configure terminal;

switch(config)#interface vlan *1*;

switch(config-if)#shutdown;

switch(config-if)#ip address *60.0.0.1 255.0.0.0*;

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *1*;

switch(config-vlan)#ports TwentyGigE 0/1/1*;*

switch(config-vlan)#exit;

switch(config)#interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *1*;

switch(config-if)#no shutdown;

switch(config-if)#exit

switch(config)#interface vlan *2*;

switch(config-if)#shutdown;

switch(config-if)#ip address *50.0.0.10 255.0.0.0;*

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *2*;

switch(config-vlan)#ports TwentyGigE 0/1/1 ;

switch(config-vlan)#exit;

switch(config)interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *2*;

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#exit;

switch#show ip interface;

switch#show ip route;

Configuring ICM3 in Topology for Redistribution

Execute the following commands to configure ICM3 in Topology for Redistribution.

switch#configure terminal;

switch(config)#interface vlan *1*;

switch(config-if)#shutdown;

switch(config-if)#ip address *60.0.0.10 255.0.0.0;*

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *1*;

switch(config-vlan)#ports TwentyGigE 0/1/1;

switch(config-vlan)#exit;

switch(config)#interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *1*;

switch(config-if)#no shutdown;

switch(config-if)#exit

switch(config)#interface vlan *2*;

switch(config-if)#shutdown;

switch(config-if)#ip address *70.0.0.1 255.0.0.0*;

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#vlan *2*;

switch(config-vlan)#ports TwentyGigE 0/1/1 untagged TwentyGigE 0/1/1;

switch(config-vlan)#exit;

switch(config)interface TwentyGigE 0/1/1;

switch(config-if)#switchport pvid *2*;

switch(config-if)#no shutdown;

switch(config-if)#exit;

switch(config)#exit;

switch#show ip interface;

switch#show ip route;

Configuring HPE IP

HPE IP supports dynamic registration of Higher Layer protocols, subnets, static routes and CIDR. It implements routing table using TRIE and maintains a common routing table using RTM to support route redistribution. This chapter describes the configuration of the following **HPE IP** features using CLI and SNMP interfaces.

- IPv4 Address
- IPv4 Routing

- Virtual Routing and Forwarding
- Static IPv4 Routes
- Static ARP Entries
- Route redistribution Policy for Routing Protocols
- Sending IPv4 Ping
- Enabling/Disabling ICMP Messages
- Path MTU Discovery
- IPv4 Trace Route
- Proxy ARP

The sub sections on SNMP configurations have references to tables for the index values used in setting up of the variables.

Configuring IPv4 Address

You can assign IP addresses to network interfaces to enable those interfaces and allow communication with the hosts on those interfaces. IP address can be a primary or secondary address. An interface can have one primary IP address and multiple secondary addresses. The secondary IP address can be created only if the primary IP address is already created for the interface. The interface must be shut down before configuring IPv4 address. Figure 2 depicts the topology setup used for this configuration.

CLI Configuration

To configure IPv4 address through CLI,

1. Enter the Interface Configuration mode.

   switch#configure terminal

   switch(config)# interface vlan *1*
2. Configure IP address in vlan1 interface

   switch(config-if)# ip address *40.0.0.1 255.0.0.0*
3. Execute the following show command to view the successful IP address configuration.

   switch#show ip interface

   ```
   vlan1 is up, line protocol is up
   Internet Address is 40.0.0.1/8
   Broadcast Address  40.255.255.255
   ```
4. Configure Secondary IP address in vlan1 interface and execute the show command to view the same.

   switch(config-if)# ip address *70.0.0.1 255.0.0.0* **secondary**

   switch(config-if)#end

   switch#show ip interface

   ```
   vlan1 is up, line protocol is up
   Internet Address is 40.0.0.1/8
   Broadcast Address  40.255.255.255
   ```

```
   Secondary Address  70.0.0.1/8
```

To delete the IP address, use the no form of the command.

switch(config-if)#no ip address *40.0.0.1 255.0.0.0*

switch(config-if)#end

switch#show ip interface

```
vlan1 is up, line protocol is up
Internet Address is 0.0.0.0/0
Broadcast Address  255.255.255.255
```

ConfiguringIPv4 Routing

Enabling IPv4 routing allows you to configure Connection profiles (or similar profiles in an external authentication server) that define destinations across WAN interfaces and add routes to the routing table. Figure 2 depicts the topology setup used for this configuration.

CLI Configuration

Enable IP routing through CLI

1. Enter the Global Configuration mode.

   switch#configure terminal

2. Enable IP routing

   switch(config)# ip routing

3. Execute the following show command to view the IP routing information.

   switch# show ip information

```
VRF  Name:     default
Global IP Configuration:
------------------------
 IP routing is enabled
 Default TTL is 64
 ICMP redirects are always sent
 ICMP unreachables are always sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 50
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is disabled
```

To disable IP routing, use the no form of the command and view the output using the show command.

switch(config)# no ip routing

switch# show ip information

```
VRF  Name:     default
Global IP Configuration:
------------------------
 IP routing is disabled
 Default TTL is 64
 ICMP redirects are always sent
 ICMP unreachables are always sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 50
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is disabled
```

VRF instance should be created before executing this command. For enabling ip routing in a particular VRF instance the VRF name should be given along with the command. If the VRF name is not given in the command IP routing, configuration is done for the default VRF instance that exists without creating explicitly.

Configuring Virtual Routing and Forwarding Support

Virtual Routing and Forwarding (VRF) support allows a single ICM switch to act as a collection of multiple logical virtual routers. Each virtual router has a routing table and a set of IP (Internet Protocol) interfaces logically separated from other virtual router. The IP addresses of the local interfaces or the destination networks can be repeated across the virtual routers (overlapping IP address in the virtual routers).

Incoming packets are associated with the virtual router using VLAN ID (Identifier) or physical interface. VLAN ID is used, if IP interfaces are mapped on top of VLANs. Physical interface is used, if IP interfaces are directly mapped on physical interfaces. This section describes how to configure VRF using CLI configuration and SNMP configuration. Figure 2 depicts the topology setup used for this configuration.

Default VRF instance cannot be deleted. VRF instance can be deleted only after removing the association with the relevant IP interfaces. IP interface when unmapped from a non-default VRF instance is mapped to default-VRF instance.

CLI Configuration

To configure VRF using CLI,

1. Enter the Global Configuration mode.

   switch#configure terminal

2. Create the VRF instance.

   switch(config)# ip vrf *vrf1*

3. Display the virtual context table entries.

   switch# show ip vrf

```
Virtual Context Table
---------------------
VcId  VRF-Name                          Interfaces
----  -------                           ----------
0     default                           vlan1
1     vrf1
```

4. Execute the ip vrf forwarding command to associate the IP interface to the VRF instance.

   switch(config)# interface vlan *3*

   switch(config-if)# ip vrf forwarding *vrf1*

   switch# show ip vrf

```
Virtual Context Table
---------------------
VcId  VRF-Name                          Interfaces
----  -------                           ----------
0     default                           vlan1,
1     vrf1                              vlan3
```

To disassociate the IP interface from a non-default VRF instance, use the no form of the command.

switch(config)# interface vlan *3*

switch(config-if)#no ip vrf forwarding *vrf 1*

To delete the VRF instance, use the no form of the no ip vrf command.

switch(config)# no ip vrf *vrf1*

Configuring Static IPv4 Routes

Static routing explicitly defines the next hop from a router to a particular destination. The **HPE IP** router provides a facility to define a static route to a destination. The destination is defined by a network prefix. This section describes how to configure Static IPv4 routes using CLI configuration and SNMP configuration. Figure 2 depicts the topology setup used for this configuration.

CLI Configuration

To add Static IPv4 routes using CLI,

In ICM1

1. Enter the Global Configuration mode

   switch#configure terminal

2. Configure the route.

switch(config)# ip route 60.0.0.0 255.0.0.0 50.0.0.10

3. Execute the following show command to view the route.

   switch# show ip route

```
Codes: C - connected, S - static, R - rip, B - bgp, O
- ospf, I - isis, E - ECMP

IA - OSPF inter area, N1 - OSPF NSSA external type 1,

N2 - OSPF NSSA external type 2, E1 - OSPF external
type 1,

E2 - OSPF external type 2 L1 - ISIS Level1, L2 - ISIS
Level2, ia - ISIS Inter Area



Vrf Name:          default

---------

  0.0.0.0/0  [1] via 15.199.200.1

C 15.199.200.0/21 is directly connected, cpu0
```

To delete a static route, use the no form of the command.

switch(config)# no ip route *60.0.0.0 255.0.0.0 50.0.0.10*

switch# show ip route

```
Vrf Name:          default

---------

C 40.0.0.0/8  is directly connected, vlan1

C 50.0.0.0/8  is directly connected, vlan2
```

VRF instance should be created and mapped to interfaces before adding VRF specific route entries.

Configuring Static ARP Entries

Address Resolution Protocol (ARP) is used to connect Layer 3 IP address to Layer 2 MAC address. It means that ARP is used to link our IP addressing to our Ethernet addressing (MAC Addressing). If you want to communicate with any device on your network, you must have the Ethernet MAC address for that device. If the device is not on your LAN, then use the default gateway (your router). In this case, your router will be the destination MAC address that your PC will communicate with. This configuration is used to add or delete a static ARP. Figure 2 depicts the topology setup used for this configuration.

CLI Configuration

The CLI configurations for static ARP entries performed through the Global Configuration mode

1. Enter the Global Configuration mode

   switch#configure terminal

2. Configure the ARP cache timeout interval.

   switch(config)# arp timeout *1000*

3. Configure the number of ARP request retry count

   switch(config)# ip arp max-retries *5*

   switch(config)# end

4. View the ARP information

   switch# show ip arp information

```
ARP Configurations:

------------------

VRF Name:  default

 Maximum number of ARP request retries is 5

 ARP cache timeout is 1000 seconds
```

5. Configure the static ARP entry:

   switch(config)# arp *40.123.31.78 00:11:22:33:47:0A* **vlan** *1*

6. View the static ARP entries

   switch#show ip arp

```
VRF Id  : 0

VRF Name: default

Address    Hardware Address   Type  Interface  Mapping

-------    ----------------   ----  ---------  -------

40.123.31.77   00:11:22:33:46:0a  ARPA  vlan1   Static

40.123.31.78   00:11:22:33:47:0a  ARPA  vlan1   Static
```

To delete a static ARP entry

switch(config)# no arp *40.123.31.77*

switch#show ip arp

```
VRF Id  : 0

VRF Name: default

Address    Hardware Address   Type  Interface  Mapping

-------    ----------------   ----  ---------  -------

40.123.31.78  00:11:22:33:47:0a  ARPA  vlan1    Static
```

VRF instance should be created and mapped to interface before adding VRF specific ARP entries

Configuring Route Redistribution Policy

Route redistribution allows different routing protocols to exchange routing information. This policy is implemented in one or more of the following cases.

- Run multiple routing protocols on a network
- Migrate from one routing protocol to another
- Use a new protocol, but need to maintain the current one.
- Use of routers from different vendors

After configuring route redistribution, the routes to all the networks are learnt using the routing protocols in each router. Figure 3 depicts the topology setup used for this configuration.

CLI Configuration

To configure Route redistribution policy using CLI, Enable dynamic routing protocols in each network and Redistribute them to each other as described in following steps.

1. Execute the show ip route command in the respective Switch to view all the connected routes. This command displays the routing information in present in the routing table.

   In ICM1,

   switch# show ip route

```
Codes: C - connected, S - static, R - rip, B - bgp, O
- ospf, I - isis, E - ECMP

IA - OSPF inter area, N1 - OSPF NSSA external type 1,

N2 - OSPF NSSA external type 2, E1 - OSPF external
type 1,

E2 - OSPF external type 2 L1 - ISIS Level1, L2 - ISIS
Level2, ia - ISIS Inter Area



Vrf Name:          default

---------

  0.0.0.0/0  [1] via 15.199.200.1

C 15.199.200.0/21 is directly connected, cpu0

Vrf Name:          default

---------

C 40.0.0.0/8  is directly connected, vlan1

C 50.0.0.0/8  is directly connected, vlan2
```

   In ICM2,

   switch# show ip route

```
Vrf Name:          default
```

```
---------
C 50.0.0.0/8  is directly connected, vlan2
C 60.0.0.0/8  is directly connected, vlan1
```

In ICM3,

switch# show ip route

```
Vrf Name:          default
---------
C 60.0.0.0/8  is directly connected, vlan1
C 70.0.0.0/8  is directly connected, vlan2
```

2. Configure the redistribute-policy for the Destination IP in ICM2, to permit or deny (by ICM2) the redistribution of that route to the destination protocol.

   switch# configure terminal

   switch(config)# redistribute-policy deny *70.0.0.0 255.0.0.0* **rip ospf**

3. Enable OSPF routing protocol in ICM1 VLAN2 interface.

Command	Purpose
switch(config)# router ospf	Enables routing process.
switch(config-router)# router-id *1.1.1.1*	Sets the router-id for the OSPF process.
switch(config-router)#network *40.0.0.1* **area** *0.0.0.0* **switch(config-router)#network** *50.0.0.1* **area** *0.0.0.0*	Defines the interfaces on which OSPF runs and the area ID for those interfaces.
switch(config-router)# ASBR Router	Specifies this router as the ASBR routers that act as gateways (redistribution) between OSPF and other routing protocols or other instances of the OSPF routing process are called ASBR.
switch(config-router)# redistribute connected	Redistributes directly connected network routes to the OSPF routing protocol.
switch(config-router)# exit	

4. Enable OSPF routing protocol in ICM2 VLAN2 interface.

Command	Purpose
switch(config)# router ospf	Enables routing process.
switch(config-router)# router-id *2.2.2.2*	Sets the router-id for the OSPF process.
switch(config-router)# network *60.0.0.1* **area** *0.0.0.0* **switch(config-router)# network** *50.0.0.10* **area** *0.0.0.0*	Defines the interfaces on which OSPF runs and the area ID for those interfaces.
switch(config-router)# ASBR Router	Specifies this router as the ASBR routers that act as gateways (redistribution) between OSPF and

	other routing protocols or other instances of the OSPF routing process are called ASBR.
switch(config-router)# redistribute connected	Redistributes directly connected network routes to the OSPF routing protocol.
switch(config-router)# redistribute rip	Redistributes routes that are learnt by the RIP process, to the OSPF protocol.
switch(config-router)# exit	

5. Enable RIP routing protocol in ICM2 VLAN1 interface.

Command	Purpose
switch(config)# router rip	Enables routing process.
switch(config-router)# network *60.1* **switch(config-router)# network** *50.10*	Enables RIP on an IP network or an unnumbered interface.
switch(config-router)# redistribute connected	Enables redistribution of corresponding protocol routes into RIP.
switch(config-router)# redistribute ospf	Advertises routes learnt by OSPF in the RIP process.
switch(config-router)# exit	

6. Enable RIP routing protocol in ICM3 VLAN1 interface.

Command	Purpose
switch(config)# router rip	Enables routing process.
switch(config-router)# network *60.10*	Enables RIP on an IP network or an unnumbered interface.
switch(config-router)# redistribute connected	Enables redistribution of corresponding protocol routes into RIP.
switch(config-router)# exit	

7. Execute the following show command to view the Routing Information in ICM1 Routing Table.

   switch# show ip route

```
Vrf Name:          default
---------
C 40.0.0.0/8  is directly connected, vlan1
C 50.0.0.0/8  is directly connected, vlan2
O 60.0.0.0/8  [2] via 50.0.0.10
```

8. Configure the redistribute-policy in ICM2 for the route 70.0.0.0/8 to permit its redistribution.

   switch# configure terminal

   switch(config)# redistribute-policy permit *70.0.0.0 255.0.0.0* **rip ospf**

   switch(config)# exit

9. Execute the show ip route command in the respective Switch to view all the connected routes. This command displays the routing information in present in the routing table.

In ICM1,

switch# show ip route

```
Vrf Name:          default
---------
C 40.0.0.0/8  is directly connected, vlan1
C 50.0.0.0/8  is directly connected, vlan2
O 60.0.0.0/8  [2] via 50.0.0.10
O 70.0.0.0/8  [10] via 50.0.0.10
```

In ICM2,

switch# show ip route

```
Vrf Name:          default
---------
O 40.0.0.0/8  [2] via 50.0.0.1
C 50.0.0.0/8  is directly connected, vlan2
C 60.0.0.0/8  is directly connected, vlan1
R 70.0.0.0/8  [2] via 60.0.0.10
```

In ICM3,

switch# show ip route

```
Vrf Name:          default
---------
R 40.0.0.0/8  [4] via 60.0.0.1
R 50.0.0.0/8  [2] via 60.0.0.1
C 60.0.0.0/8  is directly connected, vlan1
C 70.0.0.0/8  is directly connected, vlan2
```

Sending IPv4 Ping

Ping is used to test whether a particular host is reachable across an IP network. The PING application is built over ICMP ECHO REQUEST and ECHO RESPONSE messages. The results of the PING operations are stored in the PING table and the administrator can view it. Ping estimates the round-trip time and packet loss rate between hosts using interval timing and response rate. Figure 2 depicts the topology setup used for this configuration.

CLI Configuration

To send an Ipv4 ping, through CLI,

1. Send ping to the destination (Host A of VLAN1 interface) from source (ICM1's VLAN interface) in the Global Configuration mode.

switch#ping *40.10*

```
Switch# ping 40.10
Reply Not Received From : 40.0.0.10, Timeout : 1 secs
Reply Not Received From : 40.0.0.10, Timeout : 1 secs
Reply Not Received From : 40.0.0.10, Timeout : 1 secs
Reply Received From :40.0.0.10, TimeTaken : 130 msecs
Reply Received From :40.0.0.10, TimeTaken : 50 msecs
Reply Received From :40.0.0.10, TimeTaken : 60 msecs
--- 40.0.0.10 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets
Loss
```

2. View the captured packets using Ethereal (the protocol analyzer).

```
[root@localhost root]# tethereal -i eth1
tethereal: Symbol `pcap_version' has different size in
shared object, consider re-linking
Capturing on eth1
  0.000000 3com_03:04:01 -> Broadcast    ARP Who has
40.0.0.10?  Tell 40.0.0.1
  0.015371 00:11:22:33:44:0a -> 3com_03:04:01 ARP
40.0.0.10 is at 00:11:22:33:44:0a
  0.038585     40.0.0.1 -> 40.0.0.10    ICMP Echo
(ping) request
  0.065545    40.0.0.10 -> 40.0.0.1     ICMP Echo
(ping) reply
  0.101199     40.0.0.1 -> 40.0.0.10    ICMP Echo
(ping) request
  0.115553    40.0.0.10 -> 40.0.0.1     ICMP Echo
(ping) reply
  0.135841     40.0.0.1 -> 40.0.0.10    ICMP Echo
(ping) request
  0.155515    40.0.0.10 -> 40.0.0.1     ICMP Echo
(ping) reply
```

3. View the ARP entries

switch# show ip *arp*

```
VRF Id  : 0
VRF Name: default
Address    Hardware Address   Type  Interface  Mapping
-------    -----------------  ----  ---------  -------
40.123.31.77 00:11:22:33:46:0a  ARPA  vlan1   Static

40.0.0.10   00:00:d1:1e:3e:ce  ARPA  vlan1   Dynamic
```

4. Clear the dynamic Arp entry

   switch(config)# clear ip *arp*

   switch# show ip *arp*

```
VRF Id  : 0
VRF Name: default
Address    Hardware Address   Type  Interface  Mapping
-------    -----------------  ----  ---------  -------
40.123.31.77   00:11:22:33:46:0a  ARPA  vlan1   Static
```

Configuring ICMP Messages

ICMP is an integral of any IP implementation. It is an error reporting and diagnostic utility used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts.

This section describes the configurations for enabling ICMP Redirect messages and Unreachable messages. Figure 2 depicts the topology setup used for this configuration.

Enabling ICMP Redirect Message

ICMP redirect messages are sent to notify the hosts on the data link that a better route is available for a particular destination. ICMP Redirect messages are generated when the destination can be reached through a gateway in the same network, and the packet was received by one other gateway in the same network. The packet is forwarded to the particular gateway and not dropped in this case.

CLI Configuration

To enable ICMP redirect messages through CLI,

1. Enter the Global Configuration mode.

   switch#configure terminal

2. Enable the IP redirects.

   switch(config)# ip redirects

3. Execute the show command to view IP information.

   switch#show ip information

```
VRF  Name:     default


Global IP Configuration:
------------------------
 IP routing is enabled
 Default TTL is 64
 ICMP redirects are always sent
```

```
 ICMP unreachables are always sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 50
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is disabled
```

To disable the ICMP redirects, execute the no form of the ip redirect command. Use the show command to view the output.

switch(config)# no ip redirects

switch#show ip information

```
VRF  Name:     default

Global IP Configuration:
------------------------
 IP routing is enabled
 Default TTL is 64
 ICMP redirects are never sent
 ICMP unreachables are always sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 50
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is disabled
```

VRF instance should be created and mapped to interface before executing VRF specific ICMP redirect command.

Enabling ICMP Unreachable Message

ICMP Destination Unreachable messages are generated when any one of the following are not reachable - the destination network, protocol, application. Figure 2 depicts the topology setup used for this configuration.

CLI Configuration

To enable ICMP unreachable messages through CLI,

1. Enter the Global Configuration mode.

   switch#configure terminal

2. Enable the IP redirects.

   switch(config)# ip unreachables

3. Execute the show command to view IP information.

switch#show ip information

```
VRF  Name:     default

Global IP Configuration:
------------------------
 IP routing is enabled
 Default TTL is 64
 ICMP redirects are always sent
 ICMP unreachables are always sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 50
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is disabled
```

To disable the ICMP unreachable messages, execute the no form of the ip redirect command. Use the show command to view the output

switch(config)# no ip unreachables

switch#show ip information

```
VRF  Name:     default

Global IP Configuration:
------------------------
 IP routing is enabled
 Default TTL is 64
 ICMP redirects are never sent
 ICMP unreachables are never sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 50
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is disabled
```

Configuring Path MTU Discovery

Path MTU discovery is the process of determining the maximum size of packet that can be sent across the network between two hosts without the

packet being broken into multiple fragments during transmission. HPE IP detects the decrease in Path MTU as soon as possible and notifies the packetization layers about the change. Figure 2 depicts the topology setup used for this configuration.

CLI Configuration

To configure Path MTU Discovery using CLI,

1. Enter the Global Configuration mode.

   switch#configure terminal

2. Enable path mtu discover.

   switch(config)# ip path mtu discover

3. Execute the following show command to view the status of path mtu discover.

   switch# show ip information

```
      VRF  Name:     default


Global IP Configuration:
------------------------
 IP routing is enabled
 Default TTL is 64
 ICMP redirects are always sent
 ICMP unreachables are never sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 50
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is enabled
```

4. Set MTU for usage in PMTU Discovery.

   switch(config)# ip path mtu *60.0.0.1 0 1000*

   switch# show ip pmtu

```
  Ip Path MTU Table
    -----------------
Vrf Name        Destination  TOS    PMTU
--------        -----------  ---    ----
default         60.0.0.1     0      1000
```

To disable Path MTU discover,

1. Execute the no forma of the command and use the show command to view the output of the same.

switch(config)#no ip path mtu discover

switch# show ip information

```
      VRF  Name:     default


Global IP Configuration:
------------------------
 IP routing is enabled
 Default TTL is 64
 ICMP redirects are always sent
 ICMP unreachables are never sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 50
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is disabled
```

2. Remove MTU for usage in PMTU Discovery

switch(config)#no ip path mtu *60.0.0.1 0*

switch# show ip pmtu

```
  Ip Path MTU Table
    -----------------
Vrf Name        Destination  TOS    PMTU
--------        -----------  ---    ----
```

To remove the path mtu for a particular network the no form of the ip path mtu command is used.

Configuring IPv4 Trace Route

Trace route is an application built using UDP probes and ICMP (Time Exceeded and Port Unreachable) error messages to trace the route to the destination. It can help you to know,

- Why connections to a given server are poor
- Where exactly the problem is
- How systems are connected to each other

Traceroute works by increasing the time-to-live (TTL) value of each successive batch of packets sent. TTL is a limit on the period of time or number of iterations or transmissions that a unit of data (e.g. a packet) can experience before it should be discarded. Figure 2 depicts the topology setup used for this configuration.

Configuring Proxy-ARP

Proxy ARP is a technique by which a device, which is physically located on one network, appears to be logically part of a different physical network connected to the same router/firewall. It allows you to hide a device with a public IP address on a private network behind a router, and still have the device appear to be on the public network. The Proxy ARP is aware of the location of the traffic's destination, and offers its own MAC address in reply. Figure 2 depicts the topology setup used for this configuration.

CLI Configuration

To configure Proxy-ARP using CLI,

1. Enter the interface mode.

   switch# configure terminal

   switch(config)# interface vlan *2*

2. Enable Proxy ARP on the interface.

   switch(config-if)#ip proxy-arp

3. Execute the following show command to view status of Proxy ARP.

   switch#show ip proxy-arp

```
PROXY ARP Status
----------------
vlan1       : Disabled
vlan2       : Enabled
```

4. Execute the following set of command to set and view the status of a particular VRF.

   switch# configure terminal

   switch(config)# ip vrf *vrf2*

   switch(config)# interface vlan *4*

   switch(config-if)# ip vrf forwarding *vrf2*

   switch(config-if)# ip proxy-arp

   switch(config-if)# exit

   switch(config)# exit

   switch# show ip proxy-arp vrf *vrf2*

```
PROXY ARP Status
----------------
vlan4       : Enabled
----------------------
```

To disable Proxy ARP, execute the no form of the ip proxy-arp command and use the show command to view the output of the same.

switch(config-if)# no ip proxy-arp

switch#show ip proxy-arp

```
PROXY ARP Status
----------------
vlan1       : Disabled
vlan2       : Disabled
```

Configuring BFD over Static IP path

Refer to Figure 4 for the topology.

For feature overview please refer BFD ConfigUM section 4.2

CLI Configurations

ICM can be configured with BFD over both single-hop and multi-hop static IP path.

The following configurations are related to Figure 4.

1. Execute the following commands at R1
   - **Adding a static route at R1 to reach R3 via R2**

     switch# configure terminal

     switch(config)# ip route *30.0.0.0 255.0.0.0 20.0.0.2*

     switch(config)# ipv6 route *3333::3 96 2222::2*

     switch(config)# exit

     switch#

     Configuring BFD Session:

     switch# configure terminal

     switch(config)# bfd session *1*

     switch(config-bfdsess)# bfd ipv4 *20.0.0.2* **vlan** *2*

     switch(config-bfdsess)# bfd enable

     switch(config-bfdsess)# end

     switch# configure terminal

     switch(config)# bfd session *2*

     switch(config-bfdsess)# bfd ipv6 *2222::2* **vlan** *2*

     switch(config-bfdsess)# bfd enable

     switch(config-bfdsess)# end
2. Execute the following commands at R2:
   - **Configuring BFD session:**

     switch# configure terminal

     switch(config)# bfd session *1*

     switch(config-bfdsess)# bfd ipv4 *20.0.0.1* **vlan** *2*

     switch(config-bfdsess)# bfd enable

     switch(config-bfdsess)# end

switch# configure terminal

switch(config)# bfd session *2*

switch(config-bfdsess)# bfd ipv6 *2222::1* **vlan** *2*

switch(config-bfdsess)# bfd enable

switch(config-bfdsess)# end

3. Execute the following commands at R3
   - **Adding a static route at R3 to reach R1 via R2:**

     switch# configure terminal

     switch(config)# ip route *20.0.0.0 255.0.0.0 30.0.0.2*

     switch(config)# ipv6 route *2222::1 96 3333::2*

     switch(config)# exit

     switch#
4. Verify the BFD session state by executing the following show command.

   switch# show bfd session details

```
Switch default
Session Index:1
Session Status : enabled, Session Admin Status : start
Version:1,  desired tx interval:1s , required rx
interval:1s
Multiplier:3, diag:0, My discr:1, your discr:1, state
UP, D/C/M/A:0/0/0/0
Role: Active, Sess Mode: CC, Exp: 0
Oper Mode:Asynchronous Without Echo Function
Sess Type: Single hop
Timer Negotiation:Enabled
Local negotiated async tx interval:1s , Negotiated
Detect Multiplier:3
Dest UDP port: 0, Src UDP port: 0
Remote Heard Flag: True
Authentication : disabled, Authentication Type:None
Authentication Key:None
Authentication Key ID:None
Offload:Disabled, Card Number:0, Slot Number:0
Src Ip Addr:20.0.0.1, Dest Ip Addr:20.0.0.2
Admin Ctrl Required:Disabled,Admin Ctrl Err
Reason:None


Switch default
Session Index:2
```

```
Session Status : enabled, Session Admin Status : start
Version:1,  desired tx interval:1s , required rx
interval:1s
Multiplier:3, diag:0, My discr:2, your discr:2, state
UP, D/C/M/A:0/0/0/0
Role: Active, Sess Mode: CC, Exp: 0
Oper Mode:Asynchronous Without Echo Function
Sess Type: Single hop
Timer Negotiation:Enabled
Local negotiated async tx interval:1s , Negotiated
Detect Multiplier:3
Dest UDP port: 0, Src UDP port: 0
Remote Heard Flag: True
Authentication : disabled, Authentication Type:None
Authentication Key:None
Authentication Key ID:None
Offload:Disabled, Card Number:0, Slot Number:0
Src IPv6 Addr:2222::1, Dest IPv6 Addr:2222::2
Admin Ctrl Required:Disabled,Admin Ctrl Err
Reason:None
```

5. Shutdown interface gi 0/2 at R2

   switch# configure terminal

   switch(config)# int TwentyGigE 0/1/2

   switch(config)# shutdown

   switch(config)# exit

6. Verify the BFD session state by executing the following show command.

   switch# show bfd session details

```
Switch default
Session Index:1
Session Status : enabled, Session Admin Status : start
Version:1,  desired tx interval:1s , required rx
interval:1s
Multiplier:3, diag:0, My discr:1, your discr:1, state
DOWN, D/C/M/A:0/0/0/0
Role: Active, Sess Mode: CC, Exp: 0
Oper Mode:Asynchronous Without Echo Function
Sess Type: Single hop
Timer Negotiation:Enabled
Local negotiated async tx interval:1s , Negotiated
Detect Multiplier:3
```

Dest UDP port: 0, Src UDP port: 0

Remote Heard Flag: True

Authentication : disabled, Authentication Type:None

Authentication Key:None

Authentication Key ID:None

Offload:Disabled, Card Number:0, Slot Number:0

Src Ip Addr:20.0.0.1, Dest Ip Addr:20.0.0.2

Admin Ctrl Required:Disabled,Admin Ctrl Err Reason:None

Switch default

Session Index:2

Session Status : enabled, Session Admin Status : start

Version:1, desired tx interval:1s , required rx interval:1s

Multiplier:3, diag:0, My discr:2, your discr:2, state DOWN, D/C/M/A:0/0/0/0

Role: Active, Sess Mode: CC, Exp: 0

Oper Mode:Asynchronous Without Echo Function

Sess Type: Single hop

Timer Negotiation:Enabled

Local negotiated async tx interval:1s , Negotiated Detect Multiplier:3

Dest UDP port: 0, Src UDP port: 0

Remote Heard Flag: True

Authentication : disabled, Authentication Type:None

Authentication Key:None

Authentication Key ID:None

Offload:Disabled, Card Number:0, Slot Number:0

Src IPv6 Addr:2222::1, Dest IPv6 Addr:2222::2

Admin Ctrl Required:Disabled,Admin Ctrl Err Reason:None

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website (**http://www.hpe.com/assistance**).
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website (**http://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 (http://www.hpe.com/support/e-updates)
    - Software Depot website (http://www.hpe.com/support/softwaredepot)
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page (http://www.hpe.com/support/AccessToSupportMaterials).

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

Hewlett Packard Enterprise Information Library (**http://www.hpe.com/info/enterprise/docs**)

Hewlett Packard Enterprise Support Center (**http://www.hpe.com/support/hpesc**)

Contact Hewlett Packard Enterprise Worldwide (**http://www.hpe.com/assistance**)

Subscription Service/Support Alerts (**http://www.hpe.com/support/e-updates**)

Software Depot (**http://www.hpe.com/support/softwaredepot**)

Customer Self Repair (**http://www.hpe.com/support/selfrepair**)

Insight Remote Support (**http://www.hpe.com/info/insightremotesupport/docs**)

Serviceguard Solutions for HP-UX (**http://www.hpe.com/info/hpux-serviceguard-docs**)

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix (**http://www.hpe.com/storage/spock**)

Storage white papers and analyst reports (**http://www.hpe.com/storage/whitepapers**)

Remote support

Remote support is available with supported devices as part of your warranty 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 Insight Remote Support website (**http://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 (**mailto: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.