Nexthop Forwarding Support

- Revision History, on page 1
- Feature Description, on page 1
- How It Works, on page 1
- Configuring Next Hop Forwarding Support, on page 6
- VLAN Segmentation Using Next Hop Forwarding, on page 10
- Monitoring and Troubleshooting, on page 14

Revision History

Table 1: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

The next hop forwarding is the process of forwarding the packets to an adjacent router or device. The next hop router is the next closest or optimal IP for a packet in the destination path.

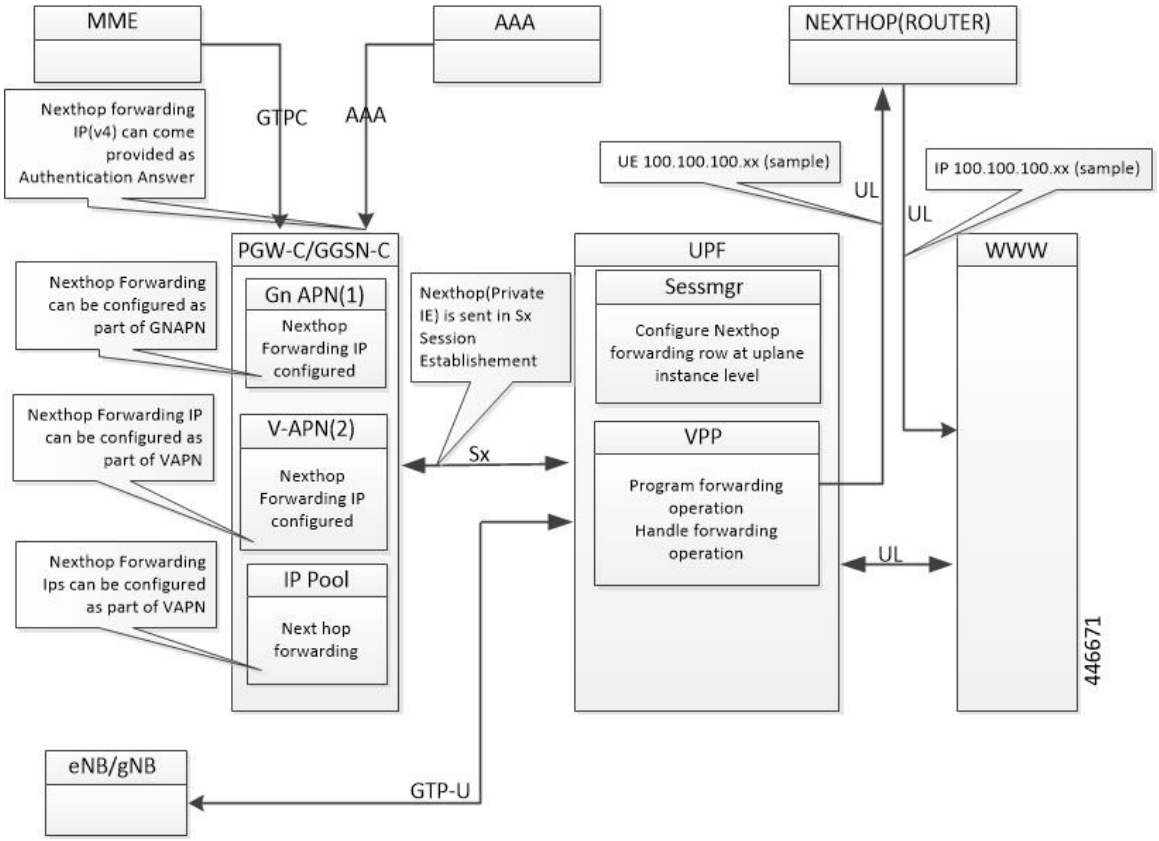
In the uplink direction, the UE and the GI IP can be in a different subnet. The routing path in UPF is defined to allow the uplink packet to be forwarded accordingly.

How It Works

Architecture

The following illustration provides an overview of Next hop forwarding feature.

Figure 1: Next hop forwarding



You can configure Next hop IP address at the SMF under DNN profile or IPAM profile. During PDU Establishment, the SMF relays the IPv4/IPv6 address over the N4 interface in the NEXT HOP IP private IE in a PFCP Session Establishment Request.

You can also configure the Next hop IP address at the UPF through Charging-Action.

Note When Next hop address is provided by both SMF and UPF Charging-Action, the UPF Charging-Action Nexthop address takes precedence.

Configuration Priority

S. No.	Configuration	Priority
1.	UPF (Charging Action)	1
2.	DNN profile	2
3.	IP Pool	3

Configuration Use Cases

Case	IP Type	DNN	IP Pool	UPF (Charging Action)	Nexthop IP Selection
Next hop supplied only in DNN	IPv4	209.165.201.18	Not configured	Not configured	Next hop Address is selected from DNN: IPv4: 209.165.201.18 IPv6: 8001::10
	IPv6	8001::10	Not configured		
Next hop supplied only in IP pool	IPv4	Not configured	209.165.201.19	Not configured	Next hop Address is selected from IP Pool: IPv4: 209.165.201.19 IPv6: 8001::10
	IPv6	Not configured	8001::10		
IPv4 and IPv6 configured in DNN and IP pool	IPv4	209.165.201.18	209.165.201.19	Not configured	Next hop Address is selected from DNN: IPv4: 209.165.201.18 IPv6: 9001::3
	IPv6	9001::3	8001::10		
IPv6 configured in DNN and IPv4 in IP pool	IPv4	Not configured	209.165.201.19	Not configured	Next hop IPv4 is selected from IP pool: 209.165.201.19 Next hop IPv6 selected from DNN : 8001::10
	IPv6	8001::10	Not configured		
IPv6 configured in DNN, IPv4 in IP pool, and IPv4 in UPF Charging Action	IPv4	209.165.201.18	209.165.201.19	209.165.201.20	Next hop Address is selected from UPF (CA): 209.165.201.20
	IPv6	8001::10	Not configured	Not configured	
IPv6 configured in DNN, IPv4 in IP pool, and IPv6 in UPF Charging Action	IPv4	209.165.201.18	209.165.201.19	Not configured	Next hop Address is selected from UPF(CA) : 9001::10
	IPv6	8001::10	Not configured	9001::10	

Interface

The following Private IEs are introduced in Sx/N4 Session Establishment message.

238	PFCP_IE_NEXTHOP	PFCP_IE_NEXTHOP								Sx/N4 Session Establishment Request	Private IE: UPF: nexthop forwarding support-IPv4 /IPv6 address
		BITS									
		Octets	7	6	5	4	3	2	1		
		1 to 2	Type = 238 (decimal)								
		3 to 4	Length = n								
		5 to 10	PFCP_IE_NEXTHOP_ID								
		11-14	PFCP_IE_NEXTHOP_IP								

239	PFCP_IE_NEXTHOP_ID	PFCP_IE_NEXTHOP_ID								1. Inside Create FAR IE of Sx Session Establishment Request	Private IE : UPF: nexthop forwarding support-IPv4 /IPv6 address
		BITS								2. Inside PFCP_IE_NEXTHOP IE of Sx/N4 Session Establishment Request	
		Octets	7	6	5	4	3	2	1	PFCP_IE_NEXTHOP of Sx/N4 Session Establishment Request	
		1 to 2	Type = 239 (decimal)								
		3 to 4	Length = 5								
		5 to 10									

<table>
<tr><td rowspan="9">240</td><td rowspan="9">PFCP_IE_NEXTHOP_IP</td><td colspan="10">PFCP_IE_NEXTHOP_IP</td><td rowspan="9">PFCP_IE_NEXTHOP of Sx/N4 Session Establishment Request</td><td rowspan="9">Private IE : UPF: nexthop forwarding support- IPv4/ IPv6 address</td></tr>
<tr><td></td><td colspan="9">Bits</td></tr>
<tr><td></td><td>Octets</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td></td></tr>
<tr><td></td><td>1 to 2</td><td colspan="7">Type = 240 (decimal)</td><td></td></tr>
<tr><td></td><td>3 to 4</td><td colspan="7">Length = n</td><td></td></tr>
<tr><td></td><td>5</td><td colspan="5">spare</td><td>V4</td><td>V6</td><td></td></tr>
<tr><td></td><td>m to m+3</td><td colspan="7">IPv4 Address</td><td></td></tr>
<tr><td></td><td>p to p+15</td><td colspan="7">IPv6 Address</td><td></td></tr>
</table>

The following is a sample output of SX_SESSION_ESTABLISHMENT_REQUEST in which the SMF relays the Next hop IP to the UPF.

```
CREATE FAR:
  Type: 3
  Value:
   FAR ID:
     Type: 108
     Value: 0x80000002
   APPLY ACTION:
     Type: 44
     Value:
       DROP: 0
       FORW: 1
       BUFF: 0
       NOCP: 0
       DUPL: 0
   FORWARDING PARAMETERS:
     Type: 4
     Value:
       DESTINATION INTERFACE:
         Type: 42
         Value: CORE (1)
       PDN INSTANCE:
          Type: 22
          Value: intershat
          INNER PACKET MARKING:
            Type: 220
            TOS/TRAFFIC CLASS: 0xB8 0xFC
    NextHop ID:
       Value: 0x0001

CREATE TRAFFIC ENDPOINT:
    Type: 127  Length: 20
    Value:
    Traffic Endpoint ID:
        Type: 131  Length: 1
        Value: 0x0004
        Hex: 0083 0001 04
```

```
        Local F-TEID:
            Type: 21  Length: 1
            Value:
                CH: 1
                IPv4: 0
                IPv6: 0
                CHID: 0
            Hex: 0015 0001 04
        Bearer Info:
            Type: 225  Length: 6
            QCI: 5
            ARP: 84
            Charging ID: 5592407
            Hex: 00E1 0006 0554 0055 5557
    Hex: 007F 0014 0083 0001 0400 1500 0104 00E1
                 0006 0554 0055 5557
NEXT HOP IP:
    Type: 237  Length: 14
    Value:
    NextHop ID:
        Type: 238  Length: 1
        Value: 0x0001
        Hex: 00EE 0001 01
    IP ADDR:
        Type: 239  Length: 5
        Value:
            IPv4: 1
            IPv6: 0
            IPv4: 209.165.202.150
            IPv6:
            Hex: 00EF 0005 020F 0F0F 0F
    Hex: 00ED 000E 00EE 0001 0100 EF00 0502 0F0F
         0F0F
```

Limitations

The following are the known limitations of this feature:

- Configuring next hop forwarding through AAA is not supported.
- Next hop address sent on RADIUS and Diameter (Redirect information from PCF) interfaces is not qualified.
- When you configure next hop forwarding in DNN profile and IPAM, the next hop is only seen in Sx Establishment, and not in Create FAR IE of Sx Session Modification Request.

Configuring Next Hop Forwarding Support

Configuring Next Hop Forwarding Through Charging Action

At the UPF, use the following CLI commands to configure Next hop forwarding through Charging Action.

```
configure
  active-charging service service_name
    charging-action charging_action_name
      nexthop-forwarding-address ipv4_address/ipv6_address
```

NOTES:

- **charging-action** *charging_action_name*: Specifies the name of a charging action. *charging_action_name* must be an alphanumeric string of 1–63 characters and can contain punctuation characters. Each charging action must have a unique name.
- **nexthop-forwarding-address** *ipv4_address/ipv6_address*: Configures the next hop forwarding address.

Configuring Next Hop Forwarding Through DNN Profile

At the SMF, use the following CLI commands to configure Next hop forwarding through the DNN profile.

```
configure
  profile dnn intershat
       nexthop-forwarding-address { ipv4 ipv4_address| ipv6  ipv6_address }
       end
```

NOTES:

- **nexthop-forwarding-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **}**: Configures the Next hop forwarding address.
  - *ipv4_address*: Configures IPv4 address.
  - *ipv6_address*: Configures IPv6 address (supports colon-separated hexadecimal notation).

Configuring Next Hop Forwarding at IP Pool Through IPAM Profile for IPv4 Addresses

At the SMF, use the following CLI command to configure Next hop forwarding at the IP pool through the IPAM profile for IPv4 addresses.

```
configure
  ipam
    instance instance_id
      address-pool pool_name
        ipv4
        address-ranges
          address-range start_ipv4_address end_ipv4_address
nexthop-forwarding-address nexthop_forwarding_address
          prefix-range prefix_value length  prefix_length
nexthop-forwarding-address nexthop_forwarding_address
          split-size per-cache number_of_addresses
          split-size per-dp number_of_addresses
          commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv4**: Enter the IPv4 mode of the pool.
- **address-ranges**: Specify the starting address of the IPv4 address range. Enter the IPv4 address range and prefix range addresses with the next hop forwarding address.
  - **address-range** *start_ipv4_address end_ipv4_address* **nexthop-forwarding-address** *nexthop_forwarding_address*: Specify the starting and the ending addresses of the IPv4 address range with the next hop forwarding address.
  - **prefix-range** *prefix_value* **length** *prefix_length*: Specify the prefix value and the length within the IPv4 address.
  - **nexthop-forwarding-address** *nexthop_forwarding_address*: Specify the next hop forwarding address.
- **split-size per-cache** *number_of_addresses*: Specify the number of IPv4 addresses per chunk for IPAM cache allocation. Specify in the power of 2. The IPAM server consumes this configuration. *number_of_addresses* must be an integer in the range of 2-262144.
- **split-size-per-dp** *number_of_addresses*: Specify the number of IPv4 addresses per chunk for data plane allocation. Specify in the power of 2. The IPAM cache consumes this configuration.

  number_of_addresses must be an integer in the range of 2-262144.

Configuring Next Hop Forwarding at IP Pool Through IPAM Profile for IPv6 Addresses

To configure the IPv6 address with the next hop configuration for IPv6 pools and address ranges, use the following sample configuration:

```
configure
   ipam
     instance instance_id
        address-pool pool_name
           ipv6
           address-ranges
              address-range start_ipv6_address end_ipv6_address
nexthop-forwarding-address nexthop_forwarding_address
              prefix-range prefix_value length prefix_length
nexthop-forwarding-address nexthop_forwarding_address
                split-size per-cache number_of_addresses
                split-size per-dp number_of_addresses
                exit
                prefix-range prefix_value length prefix_length
nexthop-forwarding-address nexthop_forwarding_address
              commit
```

NOTES:

- **address-pool** *pool_name*: Specify the name of the address pool. *pool_name* must be a string.
- **ipv6**: Enter the IPv6 mode of the pool.

- **address-ranges**: Specify the IPv6 address ranges and prefix range addresses with the next hop forwarding address.

Note IANA IPv6 configuration is used by BNG.

  - **address-range** *start_ipv6_address end_ipv6_address* : Specify the starting and the ending addresses of the IPv6 address range.
  - **nexthop-forwarding-address** *nexthop_forwarding_address*: Specify the next hop forwarding address.
  - **prefix-range** *prefix_value* **length** *prefix_length*: Specify the prefix value and length within the IPv6 address.
  - **nexthop-forwarding-address** *nexthop_forwarding_address*: Specify the next hop forwarding address.

- **prefix-ranges** : Specify the prefix ranges of an IPv6 address.

Note SMF supports only IAPD IPv6 configuration.

  - **split-size per-cache** *number_of_addresses*: Specify the number of IPv6 addresses per chunk for IPAM cache allocation.
  - **split-size-per-dp** *number_of_addresses*: Specify the number of IPv6 addresses per chunk for the data plane allocation.
  - **prefix-range** *prefix_value* **length** *prefix_length* **nexthop-forwarding-address** *nexthop_forwardng_address*: Specify the prefix value and the length within the IPv6 address with the next hop forwarding address.

Configuration Example

The following is an example configuration to configure next hop forwarding at IP pool through IPAM profile for IPv4 addresses:

```
config
   ipam
      instance 1
         address-pool p1
                  ipv4
                     split-size per-cache 1024
                     split-size per-dp 256
                     end
```

Following is an example configuration to configure next hop forwarding at IP pool through IPAM profile for IPv6 addresses:

```
ipam
 instance 1
  address-pool ISE-Pool1
   vrf-name ISP
   tags
```

```
 dnn cisco_vlan400.com
exit
ipv6
 address-ranges
   address-range 1000::1 1000::ffff nexthop-forwarding-address :9001::3
   prefix-range 2607:fc20:1010:: length 98 nexthop-forwarding-address :9001::3
 prefix-ranges
    split-size
        per-cache 32768
        per-dp    32768
    exit
    prefix-range 2607:fc20:1010:: length 44 nexthop-forwarding-address :9001::3
exit
exit
```

VLAN Segmentation Using Next Hop Forwarding

Table 2: Feature History

Feature Name	Release Information	Description
VLAN Segmentation of Traffic Using Next Hop Forwarding	2024.01	UPF allows VLAN segmentation using Next Hop Forwarding. UPF sends packets to the VLAN from where the next hop IP is most reachable instead of sending packets to the destination IP. **Default Setting**: Disabled-Configuration required to enable

Feature Description

UPF supports segmenting the enterprise traffic using Virtual LAN (VLAN). VLANs enable a single physical LAN segment to be further segmented into smaller virtual networks so that the groups of ports are isolated from one another, as if they were on physically different segments. In VLAN segmentation, the UEs belonging to different classes are assigned to different VLANs for traffic isolation.

VLAN Segmentation can be achieved using two methods:

1. Next Hop Forwarding
2. Virtual Routing and Forwarding

In the VLAN segmentation using next hop forwarding, the IP pool is mapped with the VLAN tags. This mapping takes place at the SMF. The IP pool is associated with the next hop forwarding address on the N6 interface, which is reachable through the VLAN associated with the IP pool as configured on the Control Center.

Note This feature is supported on both 1-Rack Unit and 3-Rack Unit architectures and can support up to 16 VLANs on the N6 interface.

How it Works

Achieving VLAN segmentation using next hop forwarding follows the given process:

- The SMF sends a N4 Session Establishment Request with the next hop forwarding address to the UPF.
- The UPF associates the next hop forwarding address with the session. This association allows the session management layer on the UPF to program the VPP to perform next hop forwarding of the uplink packets belonging to that session.
- The session manager on the UPF creates the uplink streams in the VPP Fastpath conduit with next hop forwarding operation with appropriate next hop IP. Therefore, the UPF does not look at the actual IP destination route to forward the packets. Rather, it relates the UE's IP address with the next hop IP and forwards the uplink packet on the VLAN from where the next hop IP is reachable.

Enabling VLAN Segmentation Using Next Hop Forwarding

To configure VLAN segmentation on UPF using next hop forwarding, use the following configuration:

```
config
  port ethernet slot/port
     no shutdown
     vlan vlan_tag_ID
     no shutdown
     bind interface interface_name context_name
     end
     context context_name
        { ip | ipv6 } address address subnetmask [ secondary ]
        end
```

NOTES:

- **port ethernet** *slot*/*port*—Ethernet port or slot that will contain the VLAN tag.
- **no shutdown**—It enables or disables the traffic over a specified VLAN.
- **vlan** *vlan_tag_ID*—Enters the VLAN configuration mode.
- **no shutdown**—Enables or disables traffic over the current VLAN.
- **bind interface** *interface_name context_name*—It binds a virtual interface and context to support VLAN service.
- **context** *context_name*—Configures the context to in which the interface is created.
- **{ ip | ipv6 } address** *address subnetmask* **[secondary]** —Maps the IP pools with the configured VLANs. The **[secondary]** keyword assigns multiple IP addresses to the interface.

Configuration Example

To enable the VLAN segmentation using next hop forwarding on UPF, use the following sample configuration:

```
config
     port ethernet 1/10
       no shutdown
```

```
       vlan 400
         no shutdown
         bind interface N6_interface1 ISP
       #exit
       vlan 401
         no shutdown
         bind interface N6_interface2 ISP
       #exit

context ISP
 interface N6_interface1
      ip address 209.165.200.225 209.165.200.254
      ip address 209.165.201.1 209.165.200.254 secondary
      ipv6 address 2001:DB8::1/32 secondary

interface N6_interface2
      ip address 209.165.202.129 209.165.200.254
      ip address 209.165.201.30 209.165.200.254 secondary
      ipv6 address 2001:DB8:1::1/32 secondary
```

Configuring Network Reachability Server on UPF

In order to forward the packets to the next hop IP, it requires the UPF to perform source-based routing and also learn the MAC address of the next hop IP by sending an ARP request to the next hop.

Configuring network reachability allows the UPF to test the network device by sending the ping packets to the destination.

To test and detect network reachability or failure on UPF for IPv4 addresses, use following configuration:

```
config
  context context_name
  nw-reachability server server_name [ remote-addr ip_addr ] [ local-addr
 ip_addr ]
```

NOTES:

- **nw-reachability server** *server_name* **[remote-addr** *ip_addr* **] [local-addr** *ip_addr* **]** —This CLI adds or deletes a reachability-detect server. The **[local-addr** *ip_addr* specifies the source IP from which the packets are sent and the **[remote-addr** *ip_addr* specifies the destination IP to send the ping packets for detecting network failure or reachability.

Note UPF supports a maximum of 2000 IPv4 pools and 256 IPv6 pools per VPN network reachability configurations per context.

To test and detect network reachability or failure on UPF for IPv6 addresses, use the following configuration:

```
config
  context context_name
    ip access-list acl_name
    { deny | permit } [ log ] any
    exit
  nw-reachability server server_name [ remote-addr ip_addr ] [ local-addr
 ip_addr ]
  end if_name
```

```
interface if_name
  ipv6 address ipv6_address ipv6_mask
    bfd interval interval_value min_rx rx_value multiplier multiplier_value
    exit
  port ethernet slot/port
    no shutdown
    vlan vlan_tag_ID
    no shutdown
    bind interface interface_name context_name
    end
```

NOTES:

- **ip access-list** *acl_name*: **ip access-list** specifies the type of subscriber traffic and the direction (uplink, downlink, or both) traffic is redirected. The **ip access-list** must be specified in the context in which the subscriber authentication is performed.
- **{ deny | permit } [log] any**: Indicates the rule, when matched, drops or allows the corresponding packets. **[log]** indicates that all the packets which match the filter are to be logged.

  any indicates that all the packets will match the filter regardless of the source and/or the destination.
- **interface** *if_name*: Specifies the interface in which the to enable BFD.
- **ipv6 address** *ipv6_address ipv6_mask*: Specifies the IPv6 address for configuring the static routes.
- **bfd interval** *interval_value* **min_rx** *rx_value* **multiplier** *multiplier_value*: **bfd interval** *interval_value* specifies the transmit interval of control packets in milliseconds as an integer from 50 through 10000. **min_rx** *rx_value* specifies the minimum receive interval for control packets in milliseconds as an integer from 50 through 10000. **multiplier** *multiplier_value* specifies the value used to compute hold-down time as an integer from 3 through 50.

Configuration Example

Following is the sample configuration of network reachability to learn the MAC address of the next hop IP:

```
(config-ctx)# nw-reachability server test remote-addr 209.165.200.225 local-addr
209.165.202.129
```

OAM Support

This section describes the operations, administration, and maintenance support for this feature.

Monitoring Support

This section describes feature-level monitoring support information.

show ip arp vpp

This show command displays the correct MAC address associated with the next hop IP addresses:

```
# show ip arp vpp
Wednesday November 22 13:03:40 EST 2023
    Time        IP      Flags     Ethernet             Interface                  slot/port
3460.6250  10.1.105.254  D   00:fd:22:53:01:81  VirtualFunctionEthernet0/6/0.1105   1/10
3446.2276  10.2.105.254  D   00:fd:22:52:ff:5f  VirtualFunctionEthernet0/7/0.2105   1/11
```

show configuration context

To verify the configured ACL lists, use the following show command:

```
[ISP]Hertz-UPF-A# show configuration context  ISP
  context ISP
    ip access-list ecs-v4.acl
      permit any
    #exit
    nw-reachability server NHFWDVlan1 remote-addr 192.11.55.100 local-addr 192.11.55.51
    nw-reachability server NHFWDVlan1_ipv6 remote-addr 2001:4888:192:1155::100 local-addr
2001:4888:192:1155::51
    #exit
  interface isp-1155
      ip address 192.11.55.51 255.255.255.0
      ipv6 address 2001:4888:192:1155::51/64 secondary
      bfd interval 50 min_rx 50 multiplier 3

  port ethernet 1/10
    no shutdown
    vlan 1155
      no shutdown
      bind interface isp-1155 ISP
    #exit
```

show nw-reachability server

This show command displays the reachability status of both the next hop IPs (remote-addr). If the next hop IP is reachable, it is displayed as **Up.**

```
[ISP]upf01#  show nw-reachability server all
 Server               remote-addr             local-addr              Vrf           state
 ---------------      ---------------     --------------- ---------------- ---------------
 vlan2645             10.28.45.1              10.28.45.2              n/a             Up
 vlan2646             10.28.46.1              10.28.46.2              n/a             Up
NHFWDVlan1_ipv6  2001:4888:192:1155::100 2001:4888:192:1155::51      n/a             Up

Total Network Reachability Servers: 3 Up: 3
```

show ipv6 interface summary

This show command displays the interface summary for VLAN configuration with IPv6 configuration:

```
[ISP]Hertz-UPF-A# show ipv6 interface summary
Interface Name               Address/Mask               Port               Status
====================    ========================    ==================    ============
=========
isp                     2001:4888:192:1153::51/64      1/10 vlan 1153          UP
 [sec]
isp-1155                2001:4888:192:1155::51/64      1/10 vlan 1155          UP
 [sec]
```

Monitoring and Troubleshooting

This section provides information about CLI commands available for monitoring and troubleshooting the feature.

Show Commands and Outputs

This section provides information about show commands and their outputs in support of this feature.

show subscriber user-plane-only full all

The output of this show command is enhanced to include the following fields introduced in support of this feature.

- **Next Hop Ip Address** - Displays the configured Nexthop IP address.

Note **Next Hop Ip Address** field is displayed only if the Nexthop IP address is relayed from the SMF. This field is not displayed if Nexthop IP address is configured only at the UPF using Charging-Action.