FSOS

IPv6 Security Configuration Guide

Contents

Figures

1 Configuring IPv6 over IPv4 Tunnel

1.1 Overview

Tunneling is an encapsulation technology, which uses one network protocol to encapsulate packets of another network protocol and transfer them over a virtual point-to-point connection. The virtual connection is called a tunnel. Tunneling refers to the whole process from data encapsulation to data transfer to data de-encapsulation.

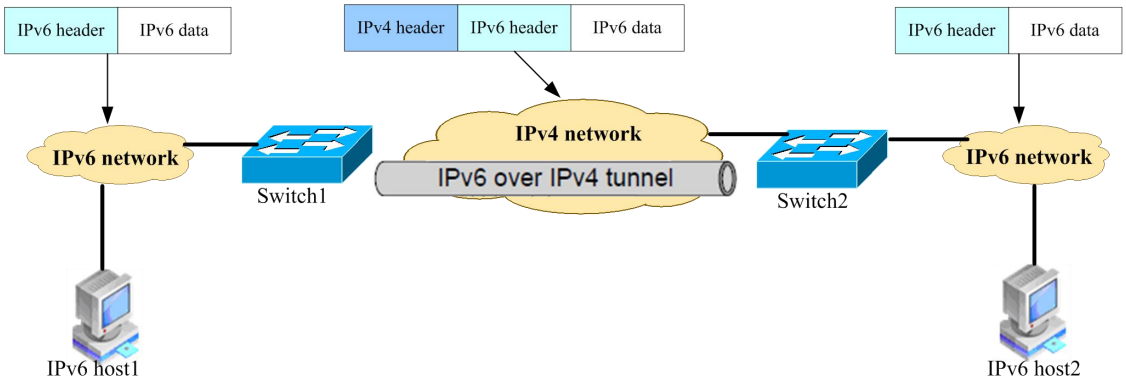

Figure 1-1 IPv6 over IPv4 Tunnel

Overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure (a core network or the Internet. By using overlay tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. Overlay tunnels can be configured between border routers or between a border router and a host; however, both tunnel endpoints must support both the IPv4 and IPv6 protocol stacks.

The IPv6 over IPv4 tunnel processes packets in the following ways:

1. A host in the IPv6 network sends an IPv6 packet to Switch1 at the tunnel source.

2. After determining according to the routing table that the packet needs to be forwarded through the tunnel, Switch1 encapsulates the IPv6 packet with an IPv4 header and forwards it through the physical interface of the tunnel.
3. Upon receiving the packet, Switch2 de-encapsulates the packet.
4. Switch2 forwards the packet according to the destination address in the de-encapsulated IPv6 packet. If the destination address is the device itself, Switch2 forwards the IPv6 packet to the upper-layer protocol for processing.

IPv6 over IPv4 tunnels are divided into manually configured tunnels and automatic tunnels, depending on how the IPv4 address of the tunnel destination is acquired.

- Manually configured tunnel: The destination address of the tunnel cannot be automatically acquired through the destination IPv6 address of an IPv6 packet at the tunnel source, and must be manually configured.
- Automatic tunnel: The destination address of the tunnel is an IPv6 address with an IPv4 address embedded, and the IPv4 address can be automatically acquired through the destination IPv6 address of an IPv6 packet at the tunnel source.

Normally, system supports the following types of overlay tunneling mechanisms:

1. Manual
2. 6to4
3. Intra-site Automatic Tunnel Addressing Protocol (ISATAP)

1.1.2 Manual Tunnel

A manually configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 backbone. The primary use is for stable connections that require regular secure communication between two edge routers or between an end system and an edge router, or for connection to remote IPv6 networks.

An IPv6 address is manually configured on a tunnel interface, and manually configured IPv4 addresses are assigned to the tunnel source and the tunnel destination. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks. Manually configured tunnels can be configured between border routers or between a border router and a host.

1.1.3 6to4 Tunnel

- ordinary 6to4 tunnel

An automatic 6to4 tunnel allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks. The key difference between automatic 6to4 tunnels and manually configured tunnels is that the tunnel is not point-to-point; it is point-to-multipoint. In automatic 6to4 tunnels, routers are not configured in pairs because they treat the IPv4 infrastructure as a virtual nonbroadcast multiaccess (NBMA) link. The IPv4 address embedded in the IPv6 address is used to find the other end of the automatic tunnel.

An automatic 6to4 tunnel may be configured on a border router in an isolated IPv6 network, which creates a tunnel on a per-packet basis to a border router in another IPv6 network over an IPv4 infrastructure. The tunnel destination is determined by the IPv4 address of the border router extracted from the IPv6 address that starts with the prefix 2002::/16, where the format is 2002:border-router-IPv4-address::/48. Following the embedded IPv4 address are 16 bits that can be used to number networks within the site. The border router at each end of a 6to4 tunnel must support both the IPv4 and IPv6 protocol stacks. 6to4 tunnels are configured between border routers or between a border router and a host.

- 6to4 relay

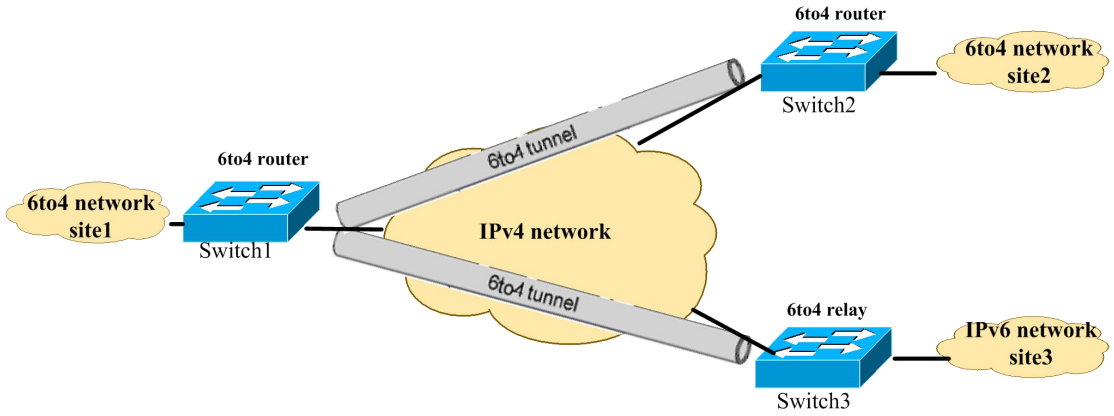

Figure 1-2 6to4 tunnel

A 6to4 tunnel is only used to connect 6to4 networks, whose IP prefix must be 2002::/16. However, IPv6 network addresses with the prefix such as 2001::/16 may also be used in IPv6 networks. To connect a 6to4 network to an IPv6 network, a 6to4 router must be used as a gateway to forward packets to the IPv6 network. Such a router is called 6to4 relay router.

As shown in the above figure, a static route must be configured on the border router (Switch1) in the 6to4 network and the next-hop address must be the 6to4 address of the 6to4 relay router (Switch3). In this way, all packets destined for the IPv6 network will be forwarded to the 6to4 relay router, and then to the IPv6 network. Thus, interworking between the 6to4 network (with the address prefix starting with 2002) and the IPv6 network is realized.

1.1.4 ISATAP Tunnel

ISATAP is an automatic overlay tunneling mechanism that uses the underlying IPv4 network as a NBMA link layer for IPv6. ISATAP is designed for transporting IPv6 packets within a site where a native IPv6 infrastructure is not yet available; for example, when sparse IPv6 hosts are deployed for testing. ISATAP tunnels allow individual IPv4 or IPv6 dual-stack hosts within a site to communicate with other such hosts on the same virtual link, basically creating an IPv6 network using the IPv4 infrastructure.

When an ISATAP tunnel is used, the destination address of an IPv6 packet and the IPv6 address of a tunnel interface both adopt special ISATAP addresses. ISATAP uses a well-defined IPv6 address format composed of any unicast IPv6 prefix (/64), which can be link local, or global (including 6to4 prefixes), enabling IPv6 routing locally or on the Internet. The IPv4 address is encoded in the last 32 bits of the IPv6 address, enabling automatic IPv6-in-IPv4 tunneling. The ISATAP address format is prefix(64bit):0:5EFE: IPv4-address.

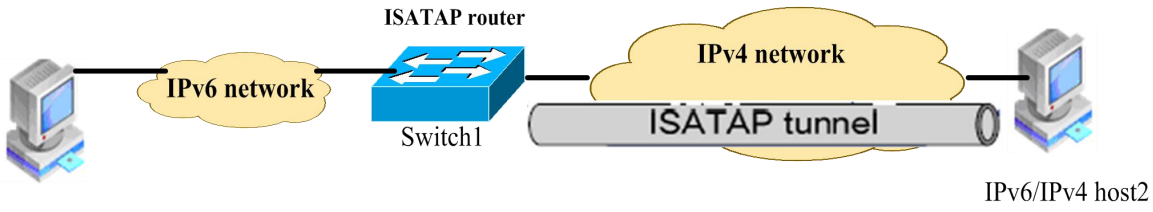

Figure 1-3 ISATAP tunnel

The ISATAP router provides standard router advertisement network configuration support for the ISATAP site. This feature allows clients to automatically configure themselves as they would do if they were connected to an Ethernet. It can also be configured to provide connectivity out of the site.

Although the ISATAP tunneling mechanism is similar to other automatic tunneling mechanisms, such as IPv6 6to4 tunneling, ISATAP is designed for transporting IPv6 packets within a site, not between sites.

1.2 Configure Manual Tunnel

1.2.1 Topology

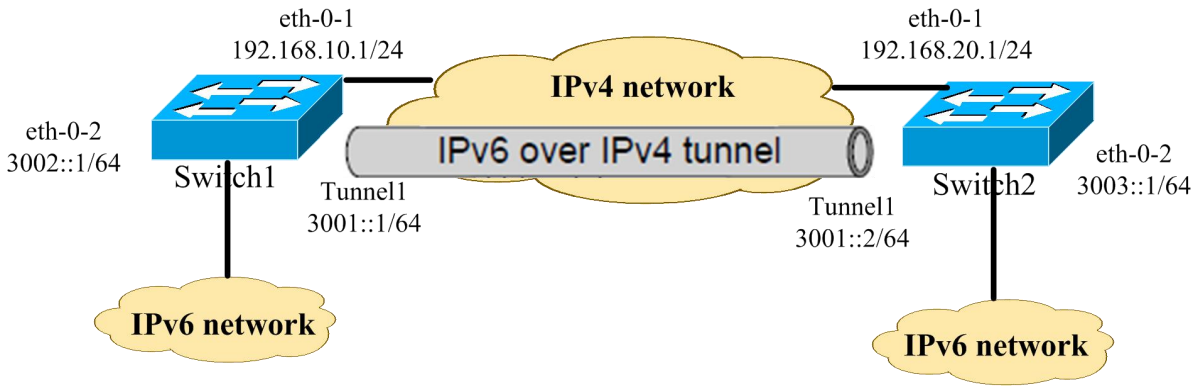

Figure 1-4 configure manual tunnel

As shown in the above Figure, two IPv6 networks are connected over an IPv4 network. Configure an IPv6 manual tunnel between Switch1 and Switch2 to make the two IPv6 networks reachable to each other.

1.2.2 Configuration

Switch1

1) Enable IPv6

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 enable	Enable IPv6

2) Configure IPv4 address and route to make packets reachable in the IPv4 network

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-1 as routed port
Switch(config-if)# ip address 192.168.10.1/24	Configure IPv4 address for eth-0-1
Switch(config)# ip route 192.168.20.0/24 192.168.10.2	Configure route to reach tunnel destination
Switch(config)# arp 192.168.10.2 0.0.2222	Configure ARP to get the Next-hop MAC address

3) Configure IPv6 address

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-2	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-2 as routed port

Switch(config-if)# ipv6 address 3002::1/64	Configure IPv6 address for eth-0-2

4) Configure tunnel information

Switch# configure terminal	Enter into global configuration
Switch(config)# interface tunnel1	Create tunnel interface
Switch(config-if)# tunnel source eth-0-1	Set tunnel source
Switch(config-if)# tunnel destination 192.168.20.1	Set tunnel destination
Switch(config-if)# tunnel mode ipv6ip	Configure tunnel mode as manual
Switch(config-if)# ipv6 address 3001::1/64	Configure IPv6 address for tunnel

5) Configure tunnel decap

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# tunnel enable	Enable tunnel decapsulation on eth-0-1

6) Configure a static route to tunnel destination

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 route 3003::/16 tunnel1	Configure a static route with tunnel interface as next-hop

Switch2

1) Enable IPv6

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 enable	Enable IPv6

2) Configure IPv4 address and route to make packets reachable in the IPv4 network

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-1 as routed port
Switch(config-if)# ip address 192.168.20.1/24	Configure IPv4 address for eth-0-1
Switch(config)# ip route 192.168.10.0/24 192.168.20.2	Configure route to reach tunnel destination
Switch(config)# arp 192.168.20.2 0.0.1111	Configure ARP to get the Next-hop MAC address

3) Configure IPv6 address

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-2	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-2 as routed port
Switch(config-if)# ipv6 address 3003::1/64	Configure IPv6 address for eth-0-2

4) Configure tunnel information

Switch# configure terminal	Enter into global configuration

Switch(config)# interface tunnel1	Create tunnel interface
Switch(config-if)# tunnel source eth-0-1	Set tunnel source
Switch(config-if)# tunnel destination 192.168.20.1	Set tunnel destination
Switch(config-if)# tunnel mode ipv6ip	Configure tunnel mode as manual
Switch(config-if)# ipv6 address 3001::2/64	Configure IPv6 address for tunnel

5) Configure tunnel decap

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# tunnel enable	Enable tunnel decapsulation on eth-0-1

6) Configure a static route to tunnel destination

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 route 3002::/16 tunnel1	Configure a static route with tunnel interface as next-hop

1.2.3 Validation

Switch1

Switch1# show interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP, Status Valid
  Tunnel source 192.168.10.1(eth-0-1), destination 192.168.20.1
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

Switch1# show ipv6 interface tunnel1

```
  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::c0a8:a01
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is disabled
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
```

```
  Hosts use stateless autoconfig for addresses.
```

Switch2

Switch1# show interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP, Status Valid
  Tunnel source 192.168.20.1(eth-0-1), destination 192.168.10.1
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

Switch1# show ipv6 interface tunnel1

```
  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::c0a8:1401
  Global unicast address(es):
    3001::2, subnet is 3001::/64
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is disabled
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
  Hosts use stateless autoconfig for addresses.
```


Notice:

1. Must enable IPv6/IPv4 dual stack before tunnel configuration.
2. Make sure tunnel destination is reachable in the IPv4 network.
3. There must exist a IPv6 address in the tunnel interface, otherwise routes with tunnel interface as nexthop will be invalid.

1.3 Configure 6to4 Tunnel

1.3.1 Topology

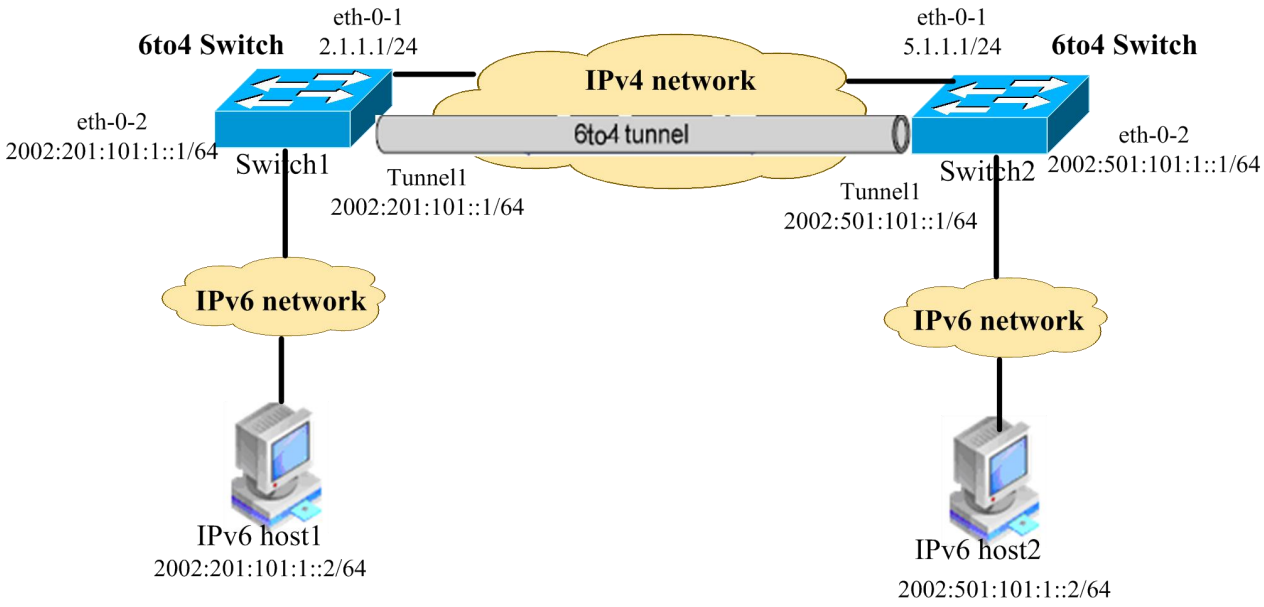

Figure 1-5 configure 6to4 tunnel

As shown in the above Figure, two 6to4 networks are connected to an IPv4 network through two 6to4 routers (Switch1 and Switch2) respectively. Configure a 6to4 tunnel to make Host1 and Host2 reachable to each other.

To enable communication between 6to4 networks, you need to configure 6to4 addresses for 6to4 routers and hosts in the 6to4 networks.

- The IPv4 address of eth-0-1 on Switch1 is 2.1.1.1/24, and the corresponding 6to4 prefix is 2002:0201:0101::/48 after it is translated to an IPv6 address. Assign interface tunnel 1 to subnet 2002:0201:0101::/64 and eth-0-2 to subnet 2002:0201:0101:1::/64.
- The IPv4 address of eth-0-1 on Switch2 is 5.1.1.1/24, and the corresponding 6to4 prefix is 2002:0501:0101::/48 after it is translated to an IPv6 address. Assign interface tunnel 1 to subnet 2002:0501:0101::/64 and eth-0-2 to subnet 2002:0501:0101:1::/64.

1.3.2 Configuration

Switch1

1) Enable IPv6

Switch# configure terminal	Enter into global configuration

Switch(config)# ipv6 enable	Enable IPv6

2) Configure IPv4 address and route to make packets reachable in the IPv4 network

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-1 as routed port
Switch(config-if)# ip address 2.1.1.1/24	Configure IPv4 address for eth-0-1
Switch(config)# ip route 5.1.1.0/24 2.1.1.2	Configure route to reach tunnel destination
Switch(config)# 2.1.1.2 0.0.2222	Configure ARP to get the Next-hop MAC address

3) Configure IPv6 address

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-2	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-2 as routed port
Switch(config-if)# ipv6 address 2002:201:101:1::1/64	Configure IPv6 address for eth-0-2

4) Configure tunnel information

Switch# configure terminal	Enter into global configuration
Switch(config)# interface tunnel1	Create tunnel interface
Switch(config-if)# tunnel source eth-0-1	Set tunnel source
Switch(config-if)# tunnel mode ipv6ip 6to4	Configure tunnel mode as 6to4
Switch(config-if)# ipv6 address 2002:201:101::1/64	Configure IPv6 address for tunnel

5) Configure tunnel decap

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# tunnel enable	Enable tunnel decapsulation on eth-0-1

6) Configure a static route to tunnel destination

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 route 2002::/16 tunnel1	Configure a static route with tunnel interface as next-hop

Switch2

1) Enable IPv6

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 enable	Enable IPv6

2) Configure IPv4 address and route to make packets reachable in the IPv4 network

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration

Switch(config-if)# no switchport	Configure the eth-0-1 as routed port
Switch(config-if)# ip address 5.1.1.1/24	Configure IPv4 address for eth-0-1
Switch(config)# ip route 2.1.1.0/24 5.1.1.2	Configure route to reach tunnel destination
Switch(config)# arp 5.1.1.2 0.0.1111	Configure ARP to get the Next-hop MAC address

3) Configure IPv6 address

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-2	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-2 as routed port
Switch(config-if)# ipv6 address 2002:501:101:1::1/64	Configure IPv6 address for eth-0-2

4) Configure tunnel information

Switch# configure terminal	Enter into global configuration
Switch(config)# interface tunnel1	Create tunnel interface
Switch(config-if)# tunnel source eth-0-1	Set tunnel source
Switch(config-if)# tunnel mode ipv6ip 6to4	Configure tunnel mode as 6to4
Switch(config-if)# ipv6 address 2002:501:101::1/64	Configure IPv6 address for tunnel

5) Configure tunnel decap

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# tunnel enable	Enable tunnel decapsulation on eth-0-1

6) Configure a static route to tunnel destination

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 route 2002::/16 tunnel1	Configure a static route with tunnel interface as next-hop

1.3.3 Validation

Switch1

Switch1# show interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP 6to4, Status Valid
  Tunnel source 2.1.1.1(eth-0-1), destination UNKNOWN
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

Switch2

Switch1# show interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP 6to4, Status Valid
  Tunnel source 5.1.1.1(eth-0-1), destination UNKNOWN
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

 Notice:

1. No destination address needs to be configured for a 6to4 tunnel
2. The automatic tunnel interfaces using the same encapsulation protocol cannot share the same source IP address
3. To encapsulate and forward IPv6 packets whose destination address does not belong to the network segment where the receiving tunnel interface resides, you need to configure a static route to reach the destination IPv6 address through this tunnel interface on the router. Because automatic tunnels do not support dynamic routing, you can configure a static route to that destination IPv6 address with this tunnel interface as the outbound interface or the peer tunnel interface address as the next hop
4. Only on4 6to4 tunnel can exist in the same node.

1.4 Configure 6to4 relay

1.4.1 Topology

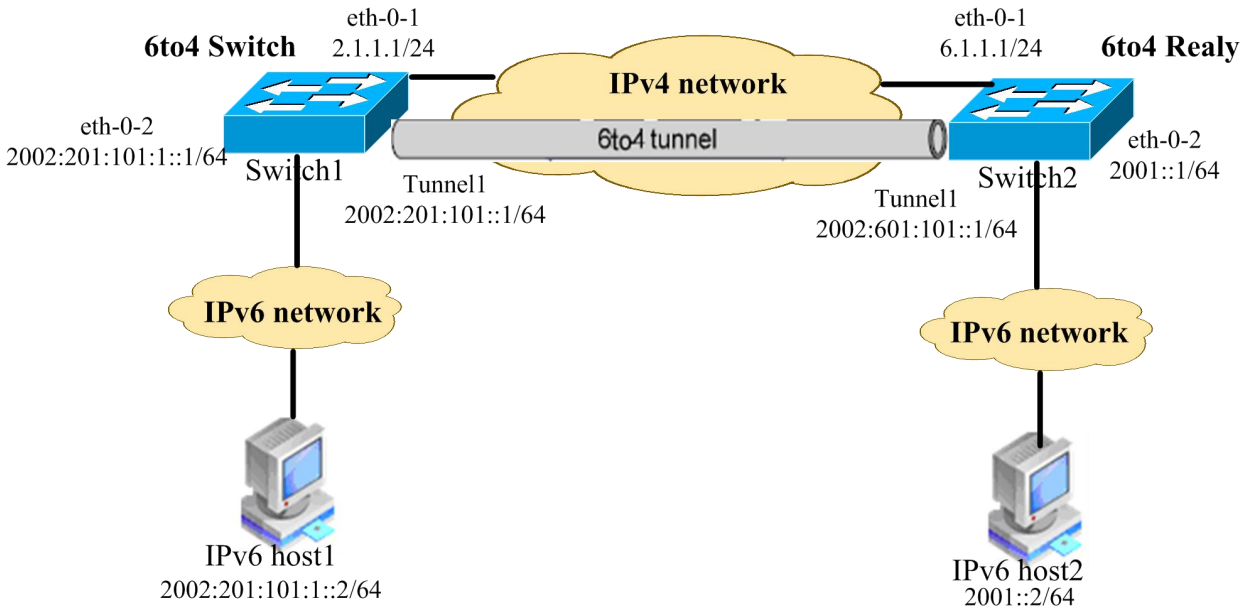

Figure 1-6 configure 6to4 relay

As shown in the above Figure, Switch1 is a 6to4 router, and 6to4 addresses are used on the connected IPv6 network. Switch2 serves as a 6to4 relay router and is connected to the IPv6 network (2001::/16). Configure a 6to4 tunnel between Router A and Router B to make Host A and Host B reachable to each other.

1.4.2 Configuration

Switch1

1) Enable IPv6

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 enable	Enable IPv6

2) Configure IPv4 address and route to make packets reachable in the IPv4 network

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-1 as routed port
Switch(config-if)# ip address 2.1.1.1/24	Configure IPv4 address for eth-0-1
Switch(config)# ip route 6.1.1.0/24 2.1.1.2	Configure route to reach tunnel destination

Switch(config)# 2.1.1.2 0.0.2222	Configure ARP to get the Next-hop MAC address

3) Configure IPv6 address

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-2	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-2 as routed port
Switch(config-if)# ipv6 address 2002:201:101:1::1/64	Configure IPv6 address for eth-0-2

4) Configure tunnel information

Switch# configure terminal	Enter into global configuration
Switch(config)# interface tunnel1	Create tunnel interface
Switch(config-if)# tunnel source eth-0-1	Set tunnel source
Switch(config-if)# tunnel mode ipv6ip 6to4	Configure tunnel mode as 6to4
Switch(config-if)# ipv6 address 2002:201:101::1/64	Configure IPv6 address for tunnel

5) Configure tunnel decap

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# tunnel enable	Enable tunnel decapsulation on eth-0-1

6) Configure a static route to tunnel destination

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 route 2001::/16 2002:601:101::1	Configure a static route to IPv6 only network
Switch(config)# ipv6 route 2002:601:101::/48 tunnel1	Configure a static route to 6to4 relay router

Switch2

1) Enable IPv6

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 enable	Enable IPv6

2) Configure IPv4 address and route to make packets reachable in the IPv4 network

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-1 as routed port
Switch(config-if)# ip address 6.1.1.1/24	Configure IPv4 address for eth-0-1
Switch(config)# ip route 2.1.1.0/24 6.1.1.2	Configure route to reach tunnel destination
Switch(config)# arp 6.1.1.2 0.0.1111	Configure ARP to get the Next-hop MAC address

3) Configure IPv6 address

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-2	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-2 as routed port
Switch(config-if)# ipv6 address 2001::1/64	Configure IPv6 address for eth-0-2

4) Configure tunnel information

Switch# configure terminal	Enter into global configuration
Switch(config)# interface tunnel1	Create tunnel interface
Switch(config-if)# tunnel source eth-0-1	Set tunnel source
Switch(config-if)# tunnel mode ipv6ip 6to4	Configure tunnel mode as 6to4
Switch(config-if)# ipv6 address 2002:601:101::1/64	Configure IPv6 address for tunnel

5) Configure tunnel decap

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# tunnel enable	Enable tunnel decapsulation on eth-0-1

6) Configure a static route to tunnel destination

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 route 2002::/16 tunnel1	Configure a static route with tunnel interface as next-hop

1.4.3 Validation

Switch1

Switch1# show interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP 6to4, Status Valid
  Tunnel source 2.1.1.1(eth-0-1), destination UNKNOWN
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

Switch1# show ipv6 route

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
       [*] - [AD/Metric]
Timers: Uptime

S       2001::/16 [1/0]
       via 2002:601:101::1 (recursive via ::, tunnel1), 00:00:32
C       2002:201:101::/64
       via ::, tunnel1, 00:00:04
```

```
C       2002:201:101::1/128
        via ::1, tunnel1, 00:00:04
S       2002:601:101::/48 [1/0]
        via ::, tunnel1, 00:00:22
```

Switch1# show ipv6 interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::201:101
  Global unicast address(es):
    2002:201:101::1, subnet is 2002:201:101::/64
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is disabled
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
  Hosts use stateless autoconfig for addresses.
```

Switch2

Switch1# show interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP 6to4, Status Valid
  Tunnel source 6.1.1.1(eth-0-1), destination UNKNOWN
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

Notice:

1. The configuration on a 6to4 relay router is similar to that on a 6to4 router. However, to enable communication between the 6to4 network and the IPv6 network, you need to configure a route to the IPv6 network on the 6to4 router.
2. It is not allowed to change the tunnel mode from 6to4 to ISATAP when there is any 6to4 relay routes existing. You must delete this routes first.

1.5 Configure ISATAP Tunnel

1.5.1 Topology

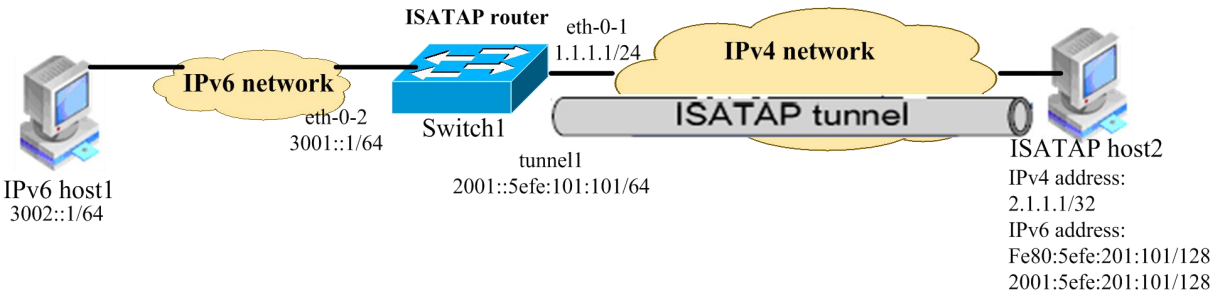

Figure 1-7 configure ISATAP tunnel

As shown in the above Figure, an IPv6 network is connected to an IPv4 network through an ISATAP router. It is required that the IPv6 host in the IPv4 network can access the IPv6 network through the ISATAP tunnel.

1.5.2 Configuration

Switch1

1) Enable IPv6

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 enable	Enable IPv6

2) Configure IPv4 address and route to make packets reachable in the IPv4 network

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-1 as routed port
Switch(config-if)# ip address 1.1.1.1/24	Configure IPv4 address for eth-0-1
Switch(config)# ip route 2.1.1.0/24 1.1.1.2	Configure route to reach tunnel destination
Switch(config)# 1.1.1.2 0.0.2222	Configure ARP to get the Next-hop MAC address

3) Configure IPv6 address

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-2	Enter into interface configuration
Switch(config-if)# no switchport	Configure the eth-0-2 as routed port
Switch(config-if)# ipv6 address 3001::1/64	Configure IPv6 address for eth-0-2

4) Configure tunnel information

Switch# configure terminal	Enter into global configuration
Switch(config)# interface tunnel1	Create tunnel interface
Switch(config-if)# tunnel source eth-0-1	Set tunnel source
Switch(config-if)# tunnel mode ipv6ip isatap	Configure tunnel mode as ISATAP
Switch(config-if)# ipv6 address 2001::/64 eui-64	Configure IPv6 address for tunnel
Switch(config-if)# no ipv6 nd ra suppress	Disable the RA suppression so that hosts can acquire information such as the address prefix from the RA message released by the ISATAP router.

5) Configure tunnel decap

Switch# configure terminal	Enter into global configuration
Switch(config)# interface eth-0-1	Enter into interface configuration
Switch(config-if)# tunnel enable	Enable tunnel decapsulation on eth-0-1

6) Configure a static route to tunnel destination

Switch# configure terminal	Enter into global configuration
Switch(config)# ipv6 route 2001::/16 tunnel1	Configure a static route to the ISATAP host

ISATAP host

The specific configuration on the ISATAP host is related to its operating system. The following example shows the configuration of the host running the Windows XP.

Install IPv6.

C:\>ipv6 install

On a Windows XP-based host, the ISATAP interface is usually interface 2. Configure the IPv4 address of the ISATAP router on interface 2 to complete the configuration on the host. Before that, display information on the ISATAP interface:

```
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  does not use Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 0.0.0.0
  router link-layer address: 0.0.0.0
    preferred link-local fe80::5efe:2.1.1.1, life infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 25000ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

A link-local address (fe80::5efe:2.1.1.2) in the ISATAP format was automatically generated for the ISATAP interface. Configure the IPv4 address of the ISATAP router on the ISATAP interface.

C:\>ipv6 rlu 2 1.1.1.1

After carrying out the above command, look at the information on the ISATAP interface.

C:\>ipv6 if 2

```
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  does not use Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 2.1.1.1
  router link-layer address: 1.1.1.1
               preferred global 2001::5efe:2.1.1.1, life 29d23h59m46s/6d23h59m46s (public)
    preferred link-local fe80::5efe:2.1.1.1, life infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 25000ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

1.5.3 Validation

Switch1

Switch# show interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP ISATAP, Status Valid
  Tunnel source 1.1.1.1(eth-0-1), destination UNKNOWN
  Tunnel DSCP inherit,  Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

Switch# show ipv6 interface tunnel1

```
Interface tunnel1
  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::101:101
  Global unicast address(es):
    2001::101:101, subnet is 2001::/64 [EUI]
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is enabled
  ND reachable time is 30000 milliseconds
```

```
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND next router advertisement due in 359 secs.
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
  Hosts use stateless autoconfig for addresses.
```

Notice:

1. No destination address needs to be configured for a ISATAP tunnel
2. The automatic tunnel interfaces using the same encapsulation protocol cannot share the same source IP address
3. To encapsulate and forward IPv6 packets whose destination address does not belong to the network segment where the receiving tunnel interface resides, you need to configure a static route to reach the destination IPv6 address through this tunnel interface on the router. Because automatic tunnels do not support dynamic routing, you can configure a static route to that destination IPv6 address with this tunnel interface as the outbound interface or the peer tunnel interface address as the next hop

2 Configuring NDP

2.1 Overview

Nodes (hosts and routers) use Neighbor Discovery to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. Hosts also use Neighbor Discovery to find neighboring routers that are willing to forward packets on their behalf. Finally, nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses. When a router or the path to a router fails, a host actively searches for functioning alternates.

2.2 Topology

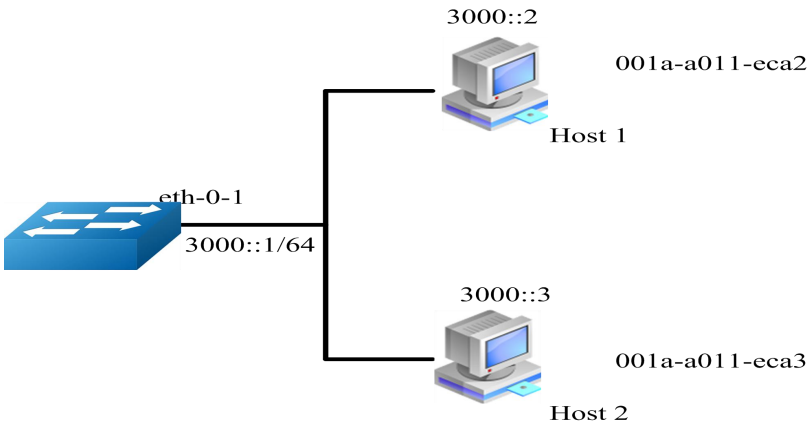

Figure 2-1 NDP Topology

2.3 Configuring NDP

In this configuration example, interface eth-0-1 assigned with ipv6 address 3000::1/64, on subnet 3000::/64, there are two hosts, and their IP addresses are 3000::2, 3000::3, MAC address are 001a-a011-eca2, 001a-a011-eca3. Neighbor entry of host 3000::2 is added manually, the entry of host 3000::3 is added dynamically.

The reachable time of neighbor entries for interface eth-0-1 configure to 10 minutes, NS interval on interface eth-0-1 configure to 2 seconds.

Switch# configure terminal	Enter configuration commands, one per line. End with CNTL/Z
Switch (config)# interface eth-0-1	Enter the interface mode
Switch (config-if)# no switchport	Configure the port to layer 3 port.
Switch (config-if)# no shutdown	no shutdown the selected interface
Switch (config-if)# ipv6 address 3000::1/64	Add IPv6 address
Switch (config-if)# ipv6 nd reachable-time 600	Set neighbor reachable time
Switch (config-if)# ipv6 nd ns-interval 2000	Set NS packet interval
Switch (config-if)# exit	Exit to global configuration mode
Switch (config)# ipv6 neighbor 3000::2 001a.a011.eca2	Add static Neighbor cache entry
Switch(config)# end	Exit to exec mode.

2.4 Validation commands

Switch # show ipv6 neighbors

```
IPv6 address                              Age       Link-Layer Addr State Interface
3000::2                                   -         001a-a011-eca2  REACH eth-0-1
3000::3                                   6         001a-a011-eca3  REACH eth-0-1
fe80::6d8:e8ff:fe4c:e700                  6         001a-a011-eca3  STALE eth-0-1
```

3 Configuring DHCPv6 Relay

3.1 Overview

DHCPv6 relay is any host that forwards DHCPv6 packets between clients and servers. Relay are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay forwarding is distinct from the normal forwarding of an IPv6 router, where IPv6 datagram are switched between networks somewhat transparently. By contrast, relay receive DHCPv6 messages and then generate a new DHCPv6 message to send out on another interface. The relay sets the link address (used by server to identify the subnet that client is belong to) , and, if configured, adds the remote-id option in the packet and forwards it to the DHCPv6 server..

3.2 Topology

This figure is the networking topology for testing DHCPv6 relay functions. We need two Linux boxes and one Switch to construct the test bed.

- Computer A is used as DHCPv6 server.
- Computer B is used as DHCPv6 client.
- Switch is used as DHCPv6 relay .

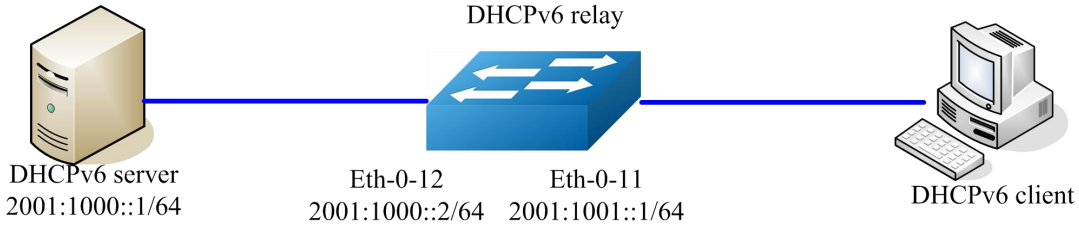

Figure 3-1 DHCPv6 Relay Topology

3.3 Configuration

Enable DHCPv6 Relay global service

Switch(config)# service dhcpv6 enable	Enable dhcpv6 services
Switch(config)# dhcpv6 relay	Enable dhcpv6 relay feature
Switch(config)# dhcpv6 relay remote-id option	Enable dhcpv6 remote-id option
Switch(config)# dhcpv6 relay pd route	Enable dhcpv6 prefix-delegation learning

Configure DHCP server groups

Switch(config)# dhcpv6-server 1 2001:1000::1	Create a dhcpv6-server group

Configure interface eth-0-12

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-12	Enter the Interface Configure mode
Switch(config-if)# no switchport	Change the port to L3 port
Switch(config-if)# ipv6 address 2001:1000::2/64	Set ipv6 address
Switch(config-if)# no shutdown	Make sure the port is enabled
Switch(config-if)# exit	Exit the Interface Configure mode

Configure interface eth-0-11

Switch(config)# interface eth-0-11	Enter the Interface Configure mode
Switch(config-if)# no switchport	Change the port to L3 port
Switch(config-if)# ipv6 address 2001:1001::1/64	Set ipv6 address
Switch(config-if)# no shutdown	Make sure the port is up
Switch(config-if)# dhcpv6-server 1	Specify the dhcpv6 server group
Switch(config-if)# exit	Exit the Interface Configure mode

3.4 Validation

Check the interface configuration

Switch# show running-config interface eth-0-12

```
!
interface eth-0-12
 no switchport
 ipv6 address 2001:1000::1/64
!
```

Switch# show running-config interface eth-0-11

```
!
interface eth-0-11
 no switchport
 ipv6 address 2001:1001::1/64
 dhcpv6-server 1
!
```

Check the dhcpv6 service status

Switch# show services

```
Networking services configuration:
Service Name          Status
============================================================
dhcp                    disable
dhcpv6                  enable
```

Check the dhcpv6 server group configuration

Switch# show dhcpv6-server

```
DHCPv6 server group information:
============================================================
group 1 ipv6 address list:
    [1] 2001:1000::1
```

Check the dhcpv6 relay statistics

Switch# show dhcpv6 relay statistics

```
DHCPv6 relay packet statistics:
============================================================
Client relayed packets :  8
Server relayed packets :  8

Client error packets   :  0
Server error packets   :  0
Missing agent options:    0
Missing circuit IDs:      0
```

Check the prefix-delegation client information learning by DHCPv6 relay

Switch# show dhcpv6 relay pd client

```
DHCPv6 prefix-delegation client information:
============================================================
Interface  : eth-0-11
Client DUID  : 000100011804ff38c2428f04970
Client IPv6 address  : fe80::beac:d8ff:fedf:c600
    IA ID  : d8dfc60
        IA Prefix :  2002:2:9:eebe::/64
            prefered/max lifetime : 280/300
            expired time :  2001-1-1 09:10:58
============================================================
```