ESMv6: IPoE Dual Stack Hosts

In This Chapter

This section describes IPoE dual stack hosts for ESMv6 configurations.

Topics in this section include:

Applicability

This section describes ESMv6: IPoE dual stack hosts and is applicable to 7750 SR series (SR-7, SR-12, SR-c4 and SR-c12) as well as 7450 ESS series in mixed mode and was tested on SR-OS 8.0R4.

This section focuses on IPoE IPv6. IPv4 configuration is shown for completeness and is described in more detail in IPv4 DHCP Hosts on page 2031.

Pre-requisites

Configuring IPoE dual stack hosts for ESMv6 are dependent on the following.

- IOM3-XP or IMM required for subscriber and network interfaces
- Chassis-mode C or higher
- Routed CO (IES/VPRN service) with Enhanced Subscriber Management (ESM)
- VLAN per subscriber (1:1 vlan)
- Routed Gateway (RG) in the home

Summary

In this section, the configuration, operation and troubleshooting of IPoE dual stack hosts in a routed home gateway environment is explained. Focus is on the Enhanced Subscriber Management for IPv6 (ESMv6) part where DHCPv6 is used for IPv6 address assignment. In the BNG, authentication, authorization and IPv6 prefix configuration for an IPoE IPv6 host can be done by a local user database or RADIUS.

Overview

IPoE Dual Stack Hosts

An IPoE dual stack subscriber may support both IPv4 and IPv6 simultaneously. The dual stack hosts share a common subscriber identification policy and have a common SLA- and Subscriber-profile.

IPoE IPv4 and IPv6 hosts operate independently as they are set up through different protocols, DHCPv4 and DHCPv6 respectively. Table 28 and Table 29 show the valid combinations of authentication, authorization and address assignment in the BNG for both address families.

Table 28: Valid Combinations for RADIUS Authenticated Hosts

	Authentication and authorization (Subscriber ID and strings)	IP address assignment (prefix, prefix length, gateway, DNS, etc.)
IPv6 host	RADIUS	RADIUS
IPv4 host	Static host	Static host
	RADIUS	RADIUS or DHCPv4

Table 29: Valid Combinations for LUDB Authenticated Hosts

	Authentication and authorization (Subscriber ID and strings)	IP address assignment (prefix, prefix length, gateway, DNS)
IPv6 host	LUDB	LUDB
IPv4 host	Static host	Static host
	Python/DHCPv4	DHCPv4
	SAP defaults	DHCPv4
	LUDB	LUDB or local DHCPv4 server

For an IPoE dual stack subscriber, up to three different types of subscriber hosts can be instantiated.

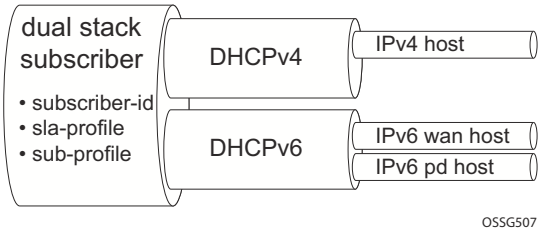

Figure 357: IPoE Dual Stack Subscriber Hosts

IPoE dual stack subscriber hosts are initially supported in a vlan/subscriber (1:1) routed CO model and with a Routed Gateway (RG). The IPv6 IPoE hosts must support DHCPv6.

Dual Stack IPoE Routed Gateway Service

In the dual stack IPoE Routed Gateway service, the RG in the home network obtains an IPv4 address through the DHCPv4 protocol and an IPv6 Prefix Delegation (PD) prefix and/or wan-host IPv6 address through the DHCPv6 protocol. The Broadband Network Gateway (BNG) authenticates and authorizes both sessions independently.

In the home network, the dual stack RG performs Network Address Translation (NAT) for IPv4, using the assigned IPv4 address as outside address. A global unique IPv6 prefix per subscriber is delegated by the BNG to the RG for use in the home network. The RG can use Stateless Address Auto Configuration (SLAAC) or DHCPv6 to allocate IPv6 addresses from this so called Prefix Delegation (PD) prefix to the devices in the home network. The wan-host IPv6 address is used by the RG on the wan side (network facing). In case of an unnumbered RG, no wan-host address is obtained.

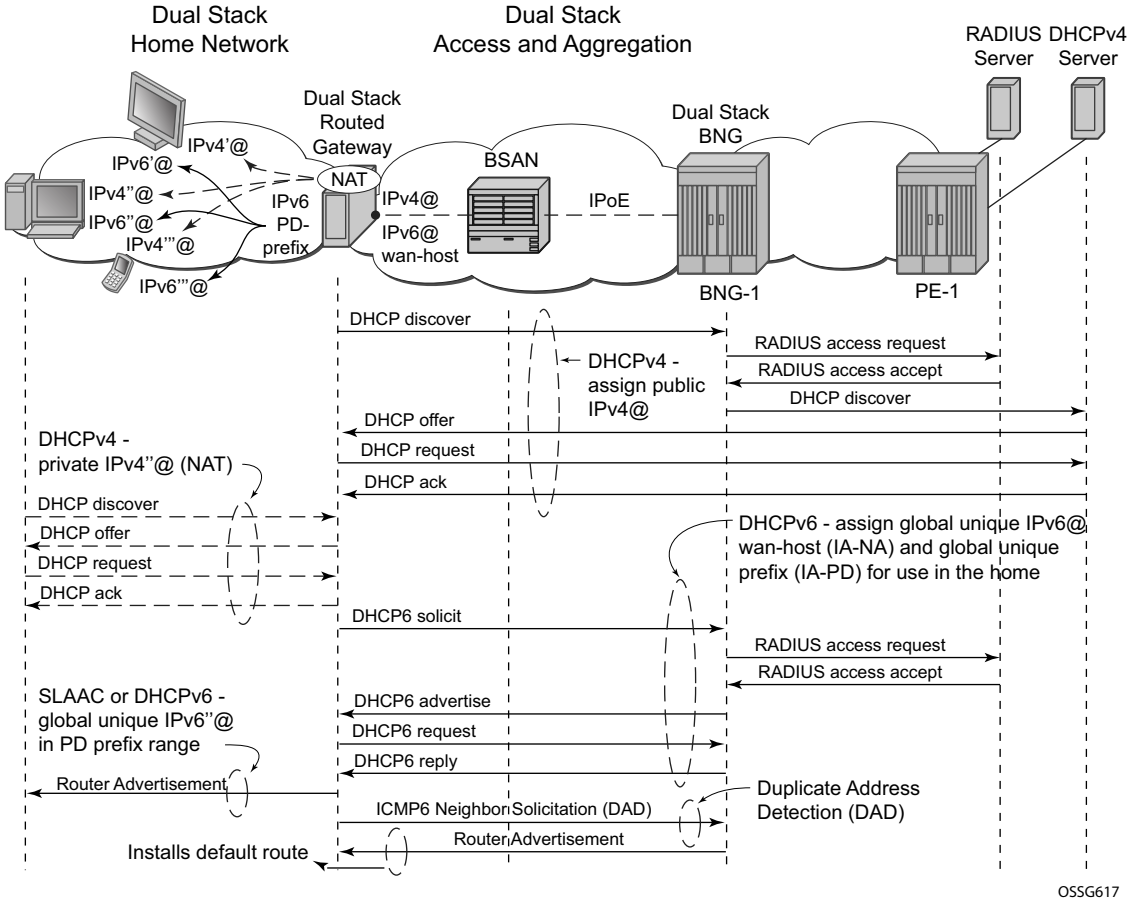

Figure 358: Dual Stack IPoE Routed Gateway Service

Recap of the DHCPv6 Protocol

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is defined in RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. The protocol enables DHCPv6 servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes.

DHCPv6 uses the Identity Association (IA) option to assign IPv6 addresses or prefixes. Two different IA types will be used in this section:

- Identity Association for Non-temporary Address (IA-NA) defined in RFC 3315.
  Used for wan-host IPv6 address assignment.

```
Option : IA_NA (3), Length : 40
  IAID : 1
  Time1: 1800 seconds
  Time2: 2880 seconds
  Option : IAADDR (5), Length : 24
    Address : 2001:DB8:B001:101::1
    Preferred Lifetime : 3600 seconds
    Valid Lifetime     : 86400 seconds
```

- Identity Association for Prefix Delegation (IA-PD), defined in RFC3633.
  Used for prefix delegation assignment (for an explanation on prefix delegation, see Prefix Delegation on page 2273)

```
Option : IA_PD (25), Length : 41
       IAID : 1
       Time1: 1800 seconds
       Time2: 2880 seconds
       Option : IAPREFIX (26), Length : 25
         Prefix : 2001:DB8:A001:100::/56
         Preferred Lifetime : 3600 seconds
         Valid Lifetime     : 86400 seconds
```

The DHCPv6 lease process is outlined in Figure 359 and Figure 360.

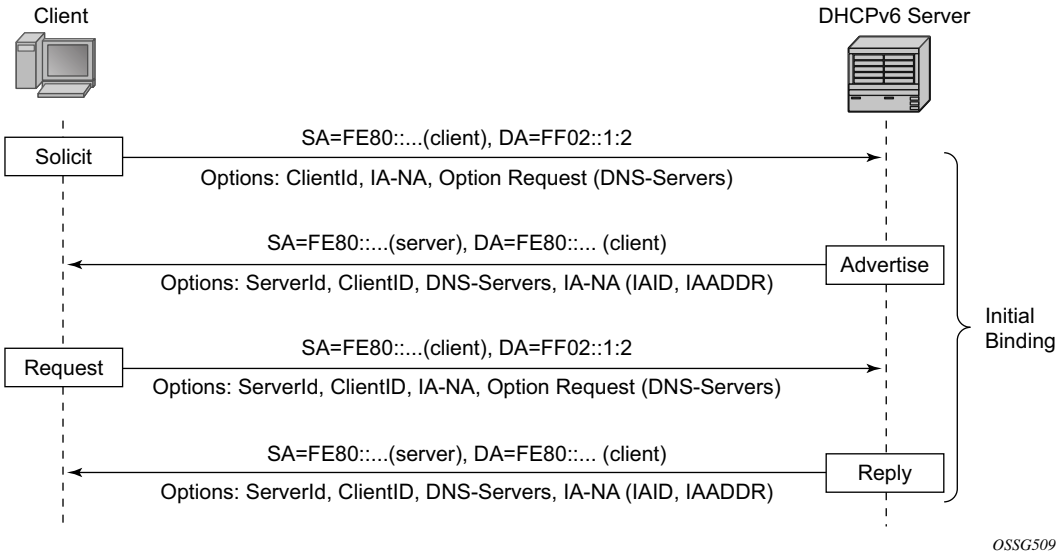

Figure 359: DHCPv6 Lease Process (Part A)

A DHCPv6 client, sends a SOLICIT message to locate servers to the All DHCPv6 Relay Agents and Servers link-scoped multicast address (FF02::1:2), using its link-local address as source address. The DHCPv6 client includes in the SOLICIT message its ClientID, Identity Associations (IA) to request IPv6 address or prefix allocation and optionally an Option Request option.

Any on-link DHCPv6 server responds with a unicasted ADVERTISE message using the link local addresses. The server includes in the ADVERTISE message the ClientID, its ServerID, IPv6 addresses and/or prefixes in Identity Associations (IA) and options containing the requested configuration parameters.

The DHCPv6 client selects an ADVERTISE message and sends a REQUEST message to the All DHCPv6 Relay Agents and Servers link-scoped multicast address. It includes its ClientID, the ServerID of the corresponding DHCPv6 server, Identity Associations (IA) to request IPv6 address or prefix allocation and optionally an Option Request option.

Upon receipt of a valid REQUEST message, the DHCPv6 server with corresponding ServerID, sends a unicast REPLY message using the link local addresses. The REPLY contains the ClientID and ServerID, IPv6 addresses and/or prefixes in Identity Associations (IA) and options containing the requested configuration options.

The DHCPv6 client should perform Duplicate Address Detection (DAD) on the addresses in any IA it received in the REPLY before using that address for traffic.

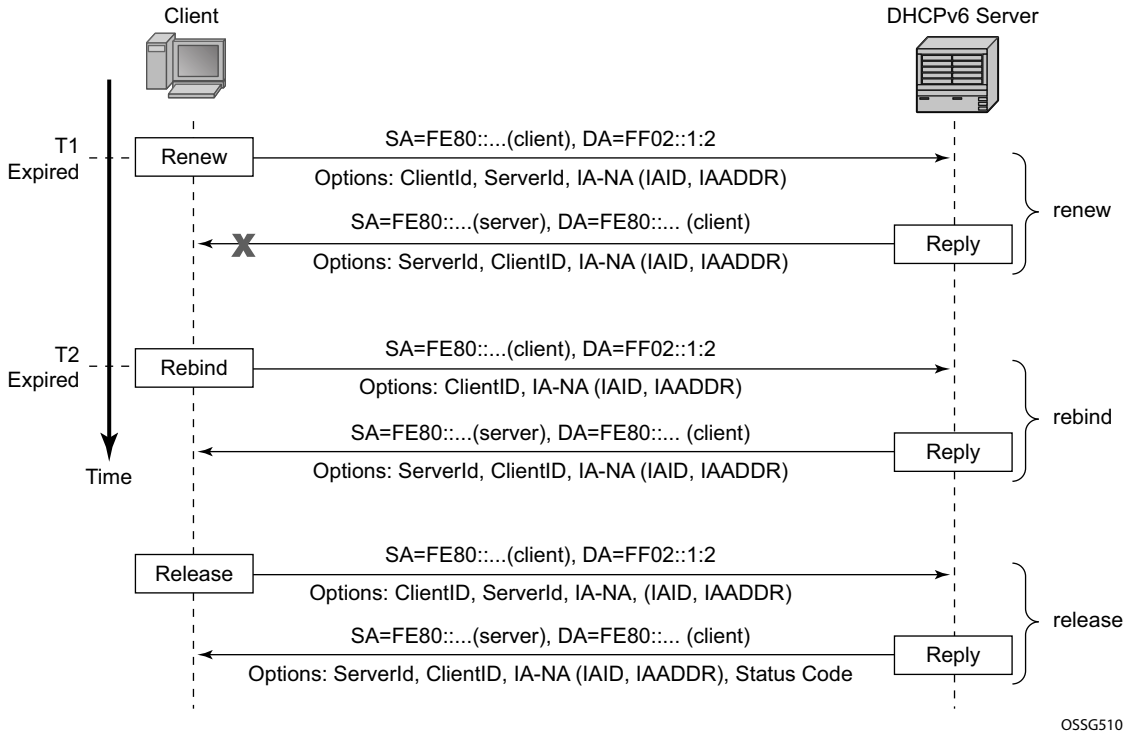

Figure 360: DHCPv6 Lease Process (Part B)

Upon expiration of the renew timer T1 associated with the Identity Association option, the DHCPv6 client sends a RENEW to the All DHCPv6 Relay Agents and Servers link-scoped multicast address to request an extension of the lifetime of an address. It includes its ClientID, the ServerID of the DHCPv6 server that originally provided the address and Identity Associations (IA) containing the IPv6 address or prefix for which an extension of the lifetime is requested.

Upon expiration of the rebind timer T2 associated with the Identity Association option (no response received to the RENEW), the DHCPv6 client sends a REBIND to the All DHCPv6 Relay Agents and Servers link-scoped multicast address to request an extension of the lifetime of an address. It includes its ClientID and Identity Associations (IA) containing the IPv6 address or prefix for which n extension of the lifetime is requested.

If a DHCPv6 client no longer uses one or more of the assigned addresses or prefixes, it sends a RELEASE message to the server that assigned the address or prefix. The server acknowledges with a REPLY message and includes a status code (for example, success).

If the DHCPv6 server sends a Server Unicast Option, then the DHCPv6 client should unicast the REQUEST, RENEW, RELEASE and DECLINE messages to the server using the IPv6 address specified in the option. The 7750 SR DHCPv6 proxy-server does not include the Server Unicast Option.

The DHCPv6 client should perform Duplicate Address Detection (DAD) on each of the addresses assigned through DHCPv6, before using that address for traffic. The DHCPv6 client uses Neighbor Solicitation for this purpose as described in RFC 4862, *IPv6 Stateless Address AutoConfiguration*.

Unlike DHCPv4, DHCPv6 does not provide a default route. In IPv6, default routers are learned via Router Advertisements (see Enable Router Advertisements on page 2282).

Prefix Delegation

Prefix Delegation (PD) is a mechanism for automated delegation of IPv6 prefixes using DHCPv6. A delegating router delegates a long-lived IPv6 prefix to a requesting router. The delegating router does not require knowledge about the topology of the links in the network to which the prefixes will be assigned.

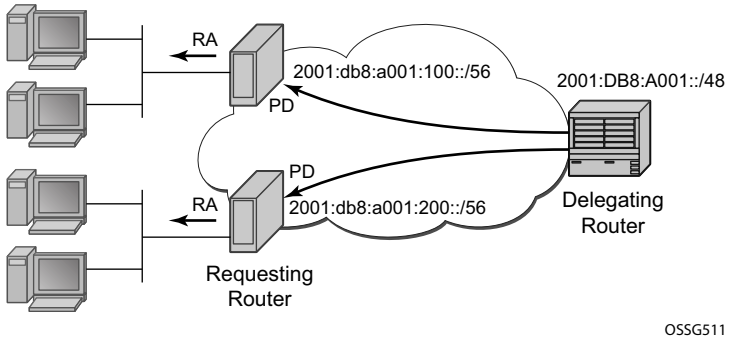

Figure 361: Prefix Delegation

In the context of ESM IPv6, the BNG is acting as delegating router (DHCPv6 server) and the Routed Gateway in the home as requesting router (DHCPv6 client). The DHCPv6 option Identity Association for Prefix Delegation (IA-PD) (Figure 361) is used to assign the IPv6 prefix.

Note that the mechanism through which a requesting router (routed gateway) assigns IPv6 addresses on its interfaces (home network) is arbitrary and can be based upon SLAAC (as shown in Figure 361) or DHCPv6.

Configuration

ESMv6 for IPoE is applicable in a Routed CO environment. The two scenarios below show a minimal configuration to enable dual stack subscribers in a VPRN service context.

Notes:

- ESM IPv6 specific parts are highlighted.
- There are no subscriber QoS policies defined (out of scope for this section)

Scenario 1

RADIUS authentication and authorization (later referenced as RADIUS).

```
A:BNG-1# configure subscriber-mgmt
A:BNG-1>config>subscr-mgmt# info
----------------------------------------------
        authentication-policy "radius-1" create
            description "Radius authentication policy"
            password <encrypted password>
            radius-authentication-server
                router "Base"
                server 1 address 172.16.1.1 secret <encrypted secret>
            exit
        exit
        sla-profile "sla-profile-1" create
        exit
        sub-profile "sub-profile-1" create
        exit
        sub-ident-policy "sub-ident-1" create
            sub-profile-map
                use-direct-map-as-default
            exit
            sla-profile-map
                use-direct-map-as-default
            exit
        exit
----------------------------------------------
A:BNG-1>config>subscr-mgmt# exit all


A:BNG-1# configure service vprn 1
A:BNG-1>config>service>vprn# info
----------------------------------------------
            vrf-import "import-1"
            route-distinguisher 64496:1
            auto-bind ldp
            vrf-target export target:64496:1
            subscriber-interface "sub-int-1" create
                address 10.1.255.254/16
                dhcp
```

```
                    gi-address 10.1.255.254
                exit
                group-interface "group-int-1" create
                    description "radius authentication and authorization"
                    ipv6
                        router-advertisements
                            managed-configuration
                            no shutdown
                        exit
                        dhcp6
                            proxy-server
                                no shutdown
                            exit
                        exit
                    exit
                    dhcp
                        server 172.16.0.1
                        trusted
                        lease-populate 10
                        no shutdown
                    exit
                    authentication-policy "radius-1"
                    sap 1/1/2:1 create
                        sub-sla-mgmt
                            sub-ident-policy "sub-ident-1"
                            multi-sub-sap 10
                            no shutdown
                        exit
                    exit
                exit
                ipv6
                    delegated-prefix-len 56
                    subscriber-prefixes
                        prefix 2001:DB8:A001::/48 pd
                        prefix 2001:DB8:B001:100::/56 wan-host
                    exit
                exit
            exit
            service-name "dual-stack"
            no shutdown
-------------------------------------------
A:BNG-1>config>service>vprn#
```

Scenario 2

Local User Database for authentication and authorization (later referenced as LUDB).

```
*A:BNG-1# configure subscriber-mgmt
*A:BNG-1>config>subscr-mgmt# info
----------------------------------------------
        sla-profile "sla-profile-1" create
        exit
        sub-profile "sub-profile-1" create
            radius-accounting-policy "aaa-policy"
        exit
        sub-ident-policy "sub-ident-1" create
            sub-profile-map
                use-direct-map-as-default
            exit
            sla-profile-map
                use-direct-map-as-default
            exit
            strings-from-option 254
        exit
        local-user-db "ludb-1" create
            dhcp
                match-list mac
                host "host-1" create
                    host-identification
                        mac 00:0a:bc:00:00:01
                    exit
                    address gi-address
                    identification-strings 254 create
                        subscriber-id "sub-1"
                        sla-profile-string "sla-profile-1"
                        sub-profile-string "sub-profile-1"
                    exit
                    options
                        subnet-mask 255.255.0.0
                        default-router 10.1.255.254
                    exit
                    ipv6-address 2001:DB8:B001:101::1
                    ipv6-prefix 2001:DB8:A001:100::/56
                    no shutdown
                exit
            exit
            no shutdown
        exit
----------------------------------------------
*A:BNG-1>config>subscr-mgmt# exit all


A:BNG-1# configure service vprn 1
A:BNG-1>config>service>vprn# info
----------------------------------------------
            dhcp
                local-dhcp-server "dhcp-s1" create
                    user-db "ludb-1"
                    use-gi-address
                    pool "pool-1" create
```

```
            subnet 10.1.0.0/16 create
                options
                    subnet-mask 255.255.0.0
                    default-router 10.1.255.254
                exit
                address-range 10.1.0.1 10.1.0.255
            exit
        exit
        no shutdown
    exit
exit
vrf-import "import-1"
route-distinguisher 64496:1
auto-bind ldp
vrf-target export target:64496:1
interface "dhcp-s1"  create
    address 192.0.2.1/32
    local-dhcp-server "dhcp-s1"
    loopback
exit
subscriber-interface "sub-int-1" create
    address 10.1.255.254/16
    dhcp
        gi-address 10.1.255.254
    exit
    group-interface "group-int-2" create
        description "Local user database authentication and authorization"
        ipv6
            router-advertisements
                managed-configuration
                no shutdown
            exit
            dhcp6
                user-db "ludb-1"
                proxy-server
                    no shutdown
                exit
            exit
        exit
        dhcp
            server 192.0.2.1
            trusted
            lease-populate 10
            no shutdown
        exit
        sap 1/1/2:2 create
            sub-sla-mgmt
                sub-ident-policy "sub-ident-1"
                multi-sub-sap 10
                no shutdown
            exit
        exit
    exit
    ipv6
        delegated-prefix-len 56
        subscriber-prefixes
            prefix 2001:DB8:A001::/48 pd
            prefix 2001:DB8:B001:100::/56 wan-host
        exit
```

```
                exit
            exit
            service-name "dual-stack"
            no shutdown
-----------------------------------------------
A:BNG-1>config>service>vprn#
```

Configuring IPv6 Subscriber Prefixes

Applies to both scenarios RADIUS and LUDB.

IPv6 subscriber prefixes must be defined at the **subscriber-interface** <*sub-int-name*> **ipv6 subscriber-prefixes** context. Three types of prefixes can be configured:

- **wan-host** — Prefix from which the IPv6 addresses are assigned that are to be used on the Routed Gateway WAN interface (network facing).
- **pd** — Prefix from which the IPv6 Prefix Delegation prefixes are assigned that are to be used by the Routed Gateway for allocation in the home network (LAN interfaces).
- **pd wan-host** (both) — Prefix from which both IPv6 addresses (wan-host) and IPv6 Prefix Delegation prefixes (pd) can be assigned. This requires that the delegated prefix length is set to 64 bits.

A subscriber prefix length must be between /32 and /63.

Subscriber prefixes are subnetted in fixed length subnets that are assigned to subscriber hosts:

- /64 for **wan-host** subscriber prefixes

  A /128 IPv6 address is assigned to the subscriber host. Broadband Forum standards requires a /64 prefix per subscriber even when used for WAN interfaces and thus the full /64 subnet gets associated with the subscriber host [ref. WT-177 - IPv6 in the context of TR-101]. Two subscriber hosts cannot get an IPv6 address from the same /64 subnet.
- /delegated-prefix-len (/48..64) for **pd** subscriber prefixes

  The delegated prefix length is configured in the **subscriber-interface** <*sub-int-name*> **ipv6** context. The recommended value by Broadband Forum standards is /56 (default = /64) [ref. WT-177 - IPv6 in the context of TR-101]. The configured length applies to all **pd** subscriber prefixes on a subscriber-interface.

Table 30 provides an overview of the subscriber-prefix parameters that apply:

Table 30: Applicable Subscriber-Prefix Parameters

Subscriber prefix type	Subscriber prefix length	DHCPv6 option	Must be subnetted as
wan-host	/32..63	IA-NA	/64 (assigned as /128)
pd	/32..63 (*)	IA-PD	/delegated-prefix-len

(*) must be smaller than configured delegated prefix length

Enable DHCPv6 Proxy Server

Applies to RADIUS and LUDB scenarios.

An IPv6 IPoE subscriber host initiates a DHCPv6 session to request its configuration data (IPv6 addresses and/or IPv6 PD prefixes, DNS servers). Upon receipt of a DHCPv6 SOLICIT message, the BNG authenticates the IPv6 subscriber host and obtains its configuration information from a RADIUS server or local user database. A DHCPv6 proxy server in the BNG maintains the DHCPv6 session with the IPv6 IPoE subscriber host.

The DHCPv6 proxy server must be enabled in the **subscriber-interface** <*sub-int-name*> **group-interface** <*group-int-name*> **ipv6 dhcp6 proxy-server** context. The default is **shutdown**.

```
service
    vprn 1 customer 1 create
        subscriber-interface "sub-int-1" create
            group-interface "group-int-1" create
                ipv6
                    dhcp6
                        proxy-server
                            renew-timer 1800           # default
                            rebind-timer 2880          # default
                            valid-lifetime 86400       # default
                            preferred-lifetime 3600    # default
                            client-applications dhcp   # default
                            no shutdown
                        exit
```

When enabled, the DHCPv6 proxy server by default allows IPv6 IPoE hosts to authenticate (configured with client-applications dhcp. Additionally, you can enable support for IPv6 PPPoE hosts. See ESMv6: PPPoE Dual Stack Hosts on page 2307.

A number of timers associated with IPv6 addresses and IPv6 prefixes within DHCPv6 Identity Associations can be configured in the DHCPv6 proxy server.

RFC 4862 defines two timers associated with graceful degradation of address bindings:

- Preferred lifetime — The length of time that a valid address is preferred (the time until deprecation). When the preferred lifetime expires, the address becomes deprecated and its use should be discouraged for new sessions.
- Valid lifetime — The length of time an address remains in the valid state (the time until invalidation). The valid lifetime must be greater than or equal to the preferred lifetime. When the valid lifetime expires, the address becomes invalid.

RFC 3315 (DHCPv6) defines two timers associated with an Identity Association (IA) option that give the servers explicit control over when a client recontacts the server about a specific IA:

- T1 (renew) — The time at which the client contacts the server from which the addresses/prefix in the IA were obtained to extend the lifetimes of the addresses/prefix assigned to the IA
- T2 (rebind) — The time at which the client contacts any available server to extend the lifetimes of the addresses/prefixes assigned to the IA;

These timers are common for all DHCPv6 sessions in a group-interface and cannot be configured from RADIUS nor local user database.

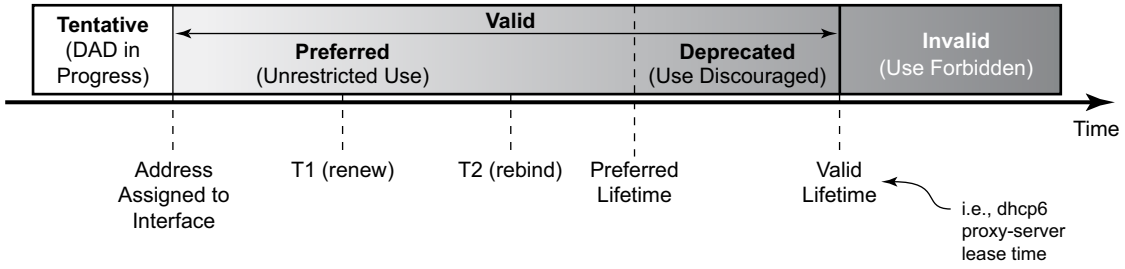

Figure 362: IPv6 Address/Prefix Timers

When violating the following rule, the default timers will be used:

$$renew - timer \leq rebind - timer \leq preferred - lifetime \leq valid - lifetime$$

Table 31: Timer Parameters

Timer	Use	Default	Range
T1	Renew timer	1800s (30 min)	0..604800s (7 days)
T2	Rebind timer	2880s (48 min)	0..1209600s (14 days)
preferred-lifetime		3600s (1hr)	300..4294967295s
valid-lifetime	DHCPv6 lease time	86400s (24 hrs)	300..4294967295s

If the DHCPv6 lease is not renewed by the client before the DHCPv6 lease timer expires, then the subscriber host is deleted from the system. In other words, beyond the valid lifetime, subscriber traffic from/to the associated IPv6 addresses is dropped.

Enable Router Advertisements

Applies to both scenarios RADIUS and LUDB.

In IPv6, default routers are automatically installed via the router discovery mechanism. Unsolicited Router Advertisements (RA) must explicitly be enabled on a group interface. The default is **shutdown**.

```
service
    vprn 1 customer 1 create
        subscriber-interface "sub-int-1" create
            group-interface "group-int-1" create
                ipv6
                    router-advertisements
                        managed-configuration
                        no shutdown
                    exit
```

Note that the managed-configuration flag is set for consistency only. It tells the hosts that addresses are available by DHCPv6. However, as described in the Security section later (see Security on page 2299), the host cannot rely on this flag because DHCPv6 must be initiated by the host before the BNG sends RAs.

Additional parameters that can be configured with respect to the router advertisements (defaults are shown):

```
service
    vprn 1 customer 1 create
        subscriber-interface "sub-int-1" create
            group-interface "group-int-1" create
                ipv6
                    router-advertisements
                        shutdown
                        current-hop-limit 64
                        no managed-configuration
                        max-advertisement 1800
                        min-advertisement 900
                        no mtu
                        no other-stateful-configuration
                        prefix-options
                            no autonomous
                            preferred-lifetime 3600
                            valid-lifetime 86400
                        exit
                        reachable-time 0
                        retransmit-time 0
                        router-lifetime 4500
                    exit
```

Table 32: Router Advertisements Parameters

Parameter	Description (RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*)	Value Range (default)
current-hop-limit	The default value that should be placed in the Hop Count field of the IP header for outgoing IP packets. A value of zero means unspecified (by this router); the RG picks its own value.	0..255 (64)
managed-configuration	Managed address configuration flag. When set, it indicates that addresses are available through DHCPv6	(no)
max-advertisement	Unsolicited Router Advertisements are not strictly periodic: the interval between subsequent transmissions is randomized to reduce the probability of synchronization with the advertisements from other routers on the same link. Whenever a multicast advertisement is sent from an interface, the timer is reset to a uniformly distributed random value between the interface's configured MinRtrAdvInterval and MaxRtrAdvInterval.	900..1800 s (1800)
min-advertisement		900..1350 s (900)
mtu	Routers can advertise an MTU for hosts to use on the link.	1280..9212 bytes (no)
other-stateful-configuration (not applicable for IPoE)	Other configuration flag. When set, it indicates that other configuration information is available through DHCPv6. (DNS). Can be ignored if managed address configuration flag is enabled	(no)
prefix-options: autonomous (not applicable for IPoE)	Autonomous address-configuration flag. When set indicates that this prefix can be used for stateless address autoconfiguration (SLAAC)	(no)
prefix-options: preferred-lifetime (not applicable for IPoE)	The length of time in seconds that addresses generated from the prefix via stateless address autoconfiguration (SLAAC) remain preferred	0..4294967295 (3600)
prefix-options: valid-lifetime (not applicable for IPoE)	The length of time in seconds that the prefix is valid for the purpose of on-link determination. (also used by SLAAC)	0..4294967295 (86400)

Table 32: Router Advertisements Parameters (Continued)

Parameter	Description (RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*)	Value Range (default)
reachable-time	The time that a node assumes a neighbor is reachable after having received a reachability confirmation. Used by the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router); the RG picks its own value.	0..3600000 ms (0)
retransmit-time	The time between retransmitted Neighbor Solicitation messages. Used by address resolution and the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router); the RG picks its own value.	0..1800000 ms (0)
router-lifetime	The lifetime associated with the default router in units of seconds.	2700..9000 s (4500)

RADIUS Authentication and Authorization

Applies to scenario 1 RADIUS only.

The RADIUS authentication and authorization configuration for IPoE IPv6 subscriber host is no different from an IPv4 subscriber host:

```
subscriber-mgmt
    authentication-policy "radius-1" create
        description "Radius authentication policy"
        password <hashed password> hash2
        radius-authentication-server
            router "Base"
            server 1 address 172.16.1.1 secret <hashed secret> hash2
        exit
    exit

    vprn 1 customer 1 create
        subscriber-interface "sub-int-1" create
            group-interface "group-int-1" create
                authentication-policy "radius-1"
```

Additional RADIUS AVPs that are applicable for IPoE IPv6 subscriber hosts are listed in Table 33.

Table 33: RADIUS AVPs

RADIUS AVP	Type	Purpose
Alc-IPv6-Address [26-6527-99]	ipv6addr	maps to IA_NA of DHCPv6 (RG WAN interface address)
Alc-Ipv6-Primary-Dns [26-6527-105]	ipv6addr	maps to DNS Recursive Name Server option (RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*) in DHCPv6
Alc-Ipv6-Secondary-Dns [26-6527-106]	ipv6addr	maps to DNS Recursive Name Server option (RFC 3646) in DHCPv6
Delegated-IPv6-Prefix [123]	ipv6prefix	maps to IA_PD for prefix delegation (RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*) in DHCPv6

A sample FreeRADIUS users record to authenticate a dual stack IPoE subscriber:

```
00:0a:bc:00:00:01   Auth-Type := Local, Cleartext-Password := "password"
                    Alc-Subsc-ID-Str = "sub-1",
                    Alc-Subsc-Prof-Str = "sub-profile-1",
                    Alc-SLA-Prof-Str = "sla-profile-1",
                    Alc-IPv6-Address = 2001:db8:b001:101::1,
                    Delegated-IPv6-Prefix = 2001:db8:a001:100::/56,
                    Alc-Ipv6-Primary-DNS = 2001:db8:dddd:1::1,
                    Alc-Ipv6-Secondary-DNS = 2001:db8:dddd:2::1
```

Note the FreeRADIUS Server 2.0.0 and greater has full support for both IPv6 attributes and IPv6 network packets.

The IPv6 address/prefix related timers can be configured in the **dhcp6 proxy-server** context (see Enable DHCPv6 Proxy Server on page 2280).

Local User Database Authentication and Authorization

Applies to scenario 2 LUDB only.

The configuration example below focuses on the IPv6 host configuration. The details for local user database host matching and IPv4 host specific parameters are out of scope for this section.

```
subscriber-mgmt
    local-user-db "ludb-1" create
        dhcp
            match-list mac
            host "host-1" create
                host-identification
                    mac 00:0a:bc:00:00:01
                exit
                address gi-address                      # IPv4 host
                identification-strings 254 create
                    subscriber-id "sub-1"
                    sla-profile-string "sla-profile-1"
                    sub-profile-string "sub-profile-1"
                exit
                options
                    subnet-mask 255.255.0.0             # IPv4 host
                    default-router 10.1.255.254         # IPv4 host
                exit
                ipv6-address 2001:DB8:B001:101::1       # IPv6 host
                ipv6-prefix 2001:DB8:A001:100::/56      # IPv6 host
                no shutdown
            exit
        exit
        no shutdown
    exit
exit

    vprn 1 customer 1 create
        subscriber-interface "sub-int-1" create
            group-interface "group-int-2" create
                ipv6
                    dhcp6
                        user-db "ludb-1"
```

Next to the identification strings that are common between IPv4 and IPv6 hosts, there are two specific IPv6 host related parameters to be configured:

Table 34: Local User Database Parameters

local-user-db CLI parameter	Purpose
ipv6-address	Maps to IA_NA of DHCPv6 (RG WAN interface address)
ipv6-prefix	Maps to IA_PD for prefix delegation (RFC 3633) in DHCPv6

The IPv6 address/prefix related timers can be configured in the **dhcp6 proxy-server** context (see Enable DHCPv6 Proxy Server on page 2280).

Note that DNSv6 server information cannot be configured in the local user database scenario. The DNSv6 server information should either be manually configured on the host or a DNSv4 server should be used instead.

DHCP and DHCP6 Lease State

Applies to both scenarios RADIUS and LUDB.

The DHCP lease state is an internal database structure that keeps track of the DHCP host states. The DHCP lease state enables subscriber management functions (for example, per subscriber QoS and accounting) and security functions (for example, dynamic anti-spoof filtering) on the DHCP host.

The DHCP lease information for a specific host is extracted from the DHCPv4 ack message in case of DHCPv4 and from the DHCPv6 reply message in case of DHCPv6

Typical information stored in the DHCP lease state includes (partial table; additional data can be stored for managed SAPs, wholesale-retail).

Table 35: DHCP Lease State Information

Parameter	Comment
Service ID	Service where the DHCP host is connected.
IP Address	IPv4 or IPv6 address of the DHCP host.
Client HW Address	Ethenet MAC address of the DHCP host.
Subscriber-interface (Routed CO only)	Subscriber interface name where the DHCP host is instantiated.
Group-interface (Routed CO only)	Group interface name where the DHCP host is instantiated.
SAP	SAP where the DHCP hosts is connected.
Remaining Lifetime	The remaining time before the DHCP host is deleted from the system (updated each time a DHCP renew/rebind occurs).
Persistence Key	Lookup key for this host in the persistency file.
Sub-Ident	ESM: Subscriber ID of the DHCP host.
Sub-Profile-String	ESM: Subscriber profile string of the DHCP host.
SLA-Profile-String	ESM: SLA profile string of the DHCP host.
App-Profile-String	ESM: Application profile string of the DHCP host.
Lease ANCP-String	ESM: ANCP string for this DHCP host.
Lease Int Dest Id	ESM: Internal destination ID for this DHCP host.

Table 35: DHCP Lease State Information (Continued)

Parameter	Comment
Category-Map-Name	ESM: Volume and Time based accounting.
Dhcp6 ClientId (DUID)	DHCPv6 client unique identifier.
Dhcp6 IAID	Identity Association ID chosen by the client.
Dhcp6 IAID Type	Identity Association type: prefix (PD) or non-temporary (wan-host).
Dhcp6 Client Ip	Link local IPv6 address of the host.
Sub-Ident origin	ESM: Origin for the Subscriber ID for this host (None, DHCP, RADIUS).
Strings origin	ESM: Origin for the ESM strings for this host (None, DHCP, RADIUS).
Lease Info origin	ESM: Origin for the IP configuration for this host (None, DHCP, RADIUS).
Ip-Netmask	The IP netmask for this DHCP host.
Broadcast-Ip-Addr	The broadcast IP address for this host.
Default-Router	The default gateway for this host.
Primary-Dns	The primary DNS server for this host.
Secondary-Dns	The secondary DNS server for this host.
Primary-Nbns	The primary NetBIOS name server for this host.
Secondary-Nbns	The secondary NetBIOS name server for this host.
ServerLeaseStart	Time and date that the lease for this host started (first DHCP ack received).
ServerLastRenew	Time and date that the lease for this host was last renewed.
ServerLeaseEnd	Time and date that the lease for this host will expire.
Session-Timeout	Lease time specified by the DHCP server.
DHCP Server Addr	IP address of the DHCP server that allocated the lease for this host.

Table 35: DHCP Lease State Information (Continued)

Parameter	Comment
Circuit Id	DHCP Relay Agent information option 82 Circuit ID content.
Remote Id	DHCP Relay Agent information option 82 Remote ID content.
RADIUS User-Name	ESM: Username used in the RADIUS authentication access request.

DHCPv4 lease state population is enabled by default on a group-interface with DHCP configured as **no shutdown**. The number of DHCPv4 leases allowed on each SAP of the group-interface must be configured with the **lease-populate** option (by default a single DHCPv4 host is allowed on each SAP of the group-interface).

DCHPv6 lease state population is enabled by default on a group-interface with DHCP6 proxy-server configured as **no shutdown**. The number of DHCPv6 leases (hosts) cannot be limited per group-interface.

```
configure
    service
        vprn 1 customer 1 create
            subscriber-interface "sub-int-1" create
                group-interface "group-int-1" create
                    ipv6
                        dhcp6
                            proxy-server
                                no shutdown
                            exit
                        exit
                    exit
                    dhcp
                        server 172.16.0.1
                        trusted
                        lease-populate 10
                        no shutdown
                    exit
```

To check the DHCPv4 or DHCPv6 lease state for a particular service, use the following commands (detailed output as well as additional output filtering is available):

```
*A:BNG-1# show service id 1 dhcp lease-state ?
  - lease-state [wholesaler <service-id>] [sap <sap-id>|sdp <sdp-id:vc-id>|
    interface <interface-name>|ip-address <ip-address[/mask]>|chaddr
    <ieee-address>|mac <ieee-address>|{[port <port-id>] [no-inter-dest-id |
    inter-dest-id <inter-dest-id>]}] [detail]
```

```
*A:BNG-1# show service id 1 dhcp6 lease-state detail
===============================================================================
DHCP lease states for service 1
===============================================================================
Service ID           : 1
IP Address           : 2001:DB8:A001:100::/56
Client HW Address    : 00:0a:bc:00:00:01
Subscriber-interface : sub-int-1
Group-interface      : group-int-1
SAP                  : 1/1/2:1
Remaining Lifetime   : 23h59m49s
Persistence Key      : 0x0000004d

Sub-Ident            : "sub-1"
Sub-Profile-String   : "sub-profile-1"
SLA-Profile-String   : "sla-profile-1"
App-Profile-String   : ""
Lease ANCP-String    : ""
Lease Int Dest Id    : ""
Category-Map-Name    : ""
Dhcp6 ClientId (DUID): 00010001133ebdd2000c29c851ca
Dhcp6 IAID           : 1
Dhcp6 IAID Type      : prefix
Dhcp6 Client Ip      : FE80::20A:BCFF:FE00:1
Primary-Dns          : 2001:DB8:DDDD:1::1
Secondary-Dns        : 2001:DB8:DDDD:2::1

Sub-Ident origin     : Radius
Strings origin       : Radius
Lease Info origin    : Radius

ServerLeaseStart     : 09/02/2010 16:13:11
ServerLastRenew      : 09/02/2010 16:13:11
ServerLeaseEnd       : 09/03/2010 16:13:11
Radius User-Name     : "00:0a:bc:00:00:01"
-------------------------------------------------------------------------------
Service ID           : 1
IP Address           : 2001:DB8:B001:101::1/128
Client HW Address    : 00:0a:bc:00:00:01
Subscriber-interface : sub-int-1
Group-interface      : group-int-1
SAP                  : 1/1/2:1
Remaining Lifetime   : 23h59m49s
Persistence Key      : 0x0000004c

Sub-Ident            : "sub-1"
Sub-Profile-String   : "sub-profile-1"
SLA-Profile-String   : "sla-profile-1"
App-Profile-String   : ""
Lease ANCP-String    : ""
Lease Int Dest Id    : ""
Category-Map-Name    : ""
Dhcp6 ClientId (DUID): 00010001133ebdd2000c29c851ca
Dhcp6 IAID           : 1
Dhcp6 IAID Type      : non-temporary
Dhcp6 Client Ip      : FE80::20A:BCFF:FE00:1
Primary-Dns          : 2001:DB8:DDDD:1::1
Secondary-Dns        : 2001:DB8:DDDD:2::1
```

```
Sub-Ident origin     : Radius
Strings origin       : Radius
Lease Info origin    : Radius

ServerLeaseStart     : 09/02/2010 16:13:11
ServerLastRenew      : 09/02/2010 16:13:11
ServerLeaseEnd       : 09/03/2010 16:13:11
Radius User-Name     : "00:0a:bc:00:00:01"
-------------------------------------------------------------------------------
Number of lease states : 2
===============================================================================
*A:BNG-1#
```

Operation

An IPoE dual stack subscriber in a numbered Routed Gateway scenario consumes three subscriber host entries:

- IPv4 host — DHCPv4 session based
- IPv6 wan-host — DHCPv6 session based
- IPv6 Prefix Delegation host — DHCPv6 session based

```
*A:BNG-1# show service active-subscribers
===============================================================================
Active Subscribers
===============================================================================
-------------------------------------------------------------------------------
Subscriber sub-1 (sub-profile-1)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
(1) SLA Profile Instance sap:1/1/2:1 - sla:sla-profile-1
-------------------------------------------------------------------------------
IP Address
                MAC Address       PPPoE-SID Origin
-------------------------------------------------------
10.1.0.3
                00:0a:bc:00:00:01 N/A       DHCP
2001:DB8:A001:100::/56
                00:0a:bc:00:00:01 N/A       IPoE-DHCP6
2001:DB8:B001:101::1/128
                00:0a:bc:00:00:01 N/A       IPoE-DHCP6
-------------------------------------------------------------------------------
Number of active subscribers : 1
===============================================================================
*A:BNG-1#
```

The optional **hierarchy** parameter for the active-subscribers display provides a top-down level overview for this subscriber:

```
*A:BNG-1# show service active-subscribers hierarchy
===============================================================================
Active Subscriber hierarchy
===============================================================================
-- sub-1 (sub-profile-1)
   |
   |-- sap:1/1/2:1 - sla:sla-profile-1
   |   |
   |   |-- 10.1.0.3
   |   |   00:0a:bc:00:00:01 - N/A (DHCP)
   |   |
   |   |-- 2001:DB8:A001:100::/56
   |   |   00:0a:bc:00:00:01 - N/A (IPoE-DHCP6)
   |   |
   |   |-- 2001:DB8:B001:101::1/128
   |   |   00:0a:bc:00:00:01 - N/A (IPoE-DHCP6)
```

```
   |   |

===============================================================================
A:BNG-1#
```

The total number (sum) of IPv4 and IPv6 hosts per subscriber can be limited in the corresponding sla-profile with the **host-limit** parameter:

```
    subscriber-mgmt
        sla-profile "sla-profile-1" create
            host-limit 3
        exit
```

To display the IPv4/IPv6 routing table for dual stack hosts:

```
A:BNG-1# show router 1 route-table ipv4 protocol sub-mgmt
===============================================================================
Route Table (Service: 1)
===============================================================================
Dest Prefix                                     Type    Proto    Age         Pref
       Next Hop[Interface Name]                                       Metric
-------------------------------------------------------------------------------
10.1.0.3/32                                     Remote  Sub Mgmt 00h01m44s   0
       [group-int-1]                                                  0
-------------------------------------------------------------------------------
No. of Routes: 1
===============================================================================
A:BNG-1#


A:BNG-1# show router 1 route-table ipv6 protocol sub-mgmt
===============================================================================
IPv6 Route Table (Service: 1)
===============================================================================
Dest Prefix                                     Type    Proto    Age         Pref
       Next Hop[Interface Name]                                       Metric
-------------------------------------------------------------------------------
2001:DB8:A001:100::/56                          Remote  Sub Mgmt 00h01m50s   0
       [group-int-1]                                                  0
2001:DB8:B001:101::1/128                        Remote  Sub Mgmt 00h01m50s   0
       [group-int-1]                                                  0
-------------------------------------------------------------------------------
No. of Routes: 2
===============================================================================
A:BNG-1#
```

Troubleshooting

Apart from the show commands in this section, use the following commands to troubleshoot a dual stack host session:

- Default system log:

```
A:BNG-1# show log log-id 99
```

Use appropriate filtering to reduce the output if needed.

- Debug:

```
debug
    router "1"
        ip
            dhcp                                # DHCPv4
                detail-level medium
                mode egr-ingr-and-dropped
            exit
            dhcp6                               # DHCPv6
                mode egr-ingr-and-dropped
                detail-level high   # needed to see the option content
            exit
        exit
        local-dhcp-server dhcp-s1               # local dhcp server
            detail-level medium
            mode egr-ingr-and-dropped
        exit
    exit
    subscriber-mgmt
        local-user-db ludb-1                    # local user database
            detail all
        exit
    exit
    radius detail                               # RADIUS
exit
```

Note that additional filtering (such as only DHCPv6 debug for particular interface) may be needed to prevent flooding of debug messages.

- Protocol statistics:

DHCPv4 stats:

```
A:BNG-1# show router 1 dhcp statistics
===============================================================================
DHCP Global Statistics (Service: 1)
===============================================================================
Rx Packets                          : 3192
Tx Packets                          : 3177
Rx Malformed Packets                : 0
Rx Untrusted Packets                : 0
Client Packets Discarded            : 0
Client Packets Relayed              : 737
Client Packets Snooped              : 860
Client Packets Proxied (RADIUS)     : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Discarded            : 15
Server Packets Relayed              : 733
Server Packets Snooped              : 847
DHCP RELEASEs Spoofed               : 0
DHCP FORCERENEWs Spoofed            : 0
===============================================================================
A:BNG-1#
```

DHCPv6 stats:

```
*A:BNG-1# show router 1 dhcp6 statistics
===============================================================================
DHCP6 statistics (Router: 1)
===============================================================================
Msg-type                      Rx             Tx             Dropped
-------------------------------------------------------------------------------
1 SOLICIT                     3              0              0
2 ADVERTISE                   0              3              0
3 REQUEST                     3              0              0
4 CONFIRM                     0              0              0
5 RENEW                       313            0              6
6 REBIND                      0              0              0
7 REPLY                       0              312            0
8 RELEASE                     2              0              0
9 DECLINE                     0              0              0
10 RECONFIGURE                0              0              0
11 INFO_REQUEST               0              0              0
12 RELAY_FORW                 0              0              0
13 RELAY_REPLY                0              0              0

-------------------------------------------------------------------------------
Dhcp6 Drop Reason Counters :
-------------------------------------------------------------------------------
 1 Dhcp6 oper state is not Up on src itf                          0
 2 Dhcp6 oper state is not Up on dst itf                          0
 3 Relay Reply Msg on Client Itf                                  0
 4 Hop Count Limit reached                                        0
 5 Missing Relay Msg option, or illegal msg type                  0
```

```
 6 Unable to determine destination client Itf                   0
 7 Out of Memory                                                 0
 8 No global Pfx on Client Itf                                   0
 9 Unable to determine src Ip Addr                               0
10 No route to server                                            0
11 Subscr. Mgmt. Update failed                                   6
12 Received Relay Forw Message                                   0
13 Packet too small to contain valid dhcp6 msg                   0
14 Server cannot respond to this message                         0
15 No Server Id option in msg from server                        0
16 Missing or illegal Client Id option in client msg             0
17 Server Id option in client msg                                0
18 Server DUID in client msg does not match our own              0
19 Client sent message to unicast while not allowed              0
20 Client sent message with illegal src Ip address               0
21 Client message type not supported in pfx delegation           0
22 Nbr of addrs or pfxs exceeds allowed max (128) in msg         0
23 Unable to resolve client's mac address                        0
24 The Client was assigned an illegal address                    0
25 Illegal msg encoding                                          0
26 Client message not supported                                  0
27 IA options in info request                                    0
28 No IA option in client msg                                    0
29 No addresses in confirm msg                                   0
===============================================================================
A:BNG-1#
```

RADIUS stats:

```
*A:BNG-1# show subscriber-mgmt authentication "radius-1" statistics
===============================================================================
Authentication Policy Statistics
===============================================================================
-------------------------------------------------------------------------------
Policy name                           : radius-1
subscriber packets authenticated      : 16
subscriber packets rejected           : 0
-------------------------------------------------------------------------------
radius server     requests  requests  requests  requests   requests requests
idx IP-address    accepted  rejected  no reply  md5 failed pending  send failed
-------------------------------------------------------------------------------
1 172.16.1.1      16        0         0         0          0        0
===============================================================================
A:BNG-1#
```

Advanced Topics

Security

Downstream Router Advertisements

When a SAP is bound to a subscriber/group-interface which has IPv6 enabled, there will be no initial downstream Router Advertisement (RA) message sent. If a SAP is shared by multiple subscribers, it would be possible for an unauthenticated host to receive the RA.

Instead the RAs are sent in unicast to allow per-host IPv6 link configuration. This requires the host information (MAC address and link-local IPv6 address) to be known. Hence for IPoE, until a DHCPv6 session is bound, no unsolicited or solicited RAs are send.

Processing of Neighbor Discovery Messages

Processing of Neighbor Discovery messages: Neighbor Advertisements (NA), Neighbor Solicitations (NS) and Router Solicitations (RS).

Neighbor discovery messages are not processed prior to IPoE IPv6 host authentication to avoid DoS attacks consuming CPU resources. This implies that an IPoE host should initiate the DHCPv6 session without link information and knowledge of routers on the link as required by the Broadband Forum standards (ref. TR-124 issue 2 — Functional Requirements for Broadband Residential Gateway Devices). This is not a problem as the DHCPv6 solicit/request messages are sent to a well-known multicast address with direct link-layer mapping.

After DHCP host authentication, Neighbor Discovery messages will not result in a neighbor cache entry. Instead a managed neighbor cache entry is created based on the DHCPv6 lease state. This managed neighbor cache entry cannot be displayed. The above mechanism prevents DoS attacks from poisoning the neighbor cache with bogus entries.

Router advertisements in response to a router solicitation are internally throttled so that they are not sent more often than once every three seconds.

Anti-spoof Filters

For each authenticated IPoE IPv6 host, an anti-spoof filter entry is created that allows upstream traffic with exact match on the tuple {masked source IP, source MAC}. Traffic from unauthenticated hosts is silently dropped.

1:1 VLAN Model

This model implicitly enforces security in the Access/Aggregation network as there is a clean separation of the subscriber traffic in a dedicated C-VLAN from the home network up to the BNG.

Managed SAPs

To allow the creation of managed SAPs in a dual stack environment, both DHCPv4 discover and DHCPv6 solicit messages received on a capture SAP should trigger RADIUS authentication:

```
service
    vpls 2 customer 1 create
        sap 1/1/2:* capture-sap create
            trigger-packet dhcp dhcp6
            authentication-policy "radius-1"
        exit
        no shutdown
    exit
```

A full description of the managed SAP functionality is out of the scope of this section.

RADIUS Change of Authorization (CoA)

The only CoA action that is allowed for IPoE IPv6 hosts is a change of ESM strings (SLA-profile, subscriber-profile, application-profile, etc). Creation of a new IPv6 host or forcing a DHCPv6 renew is not supported.

Only a single address attribute (Framed-IP-Address, Delegated-IPv6-Prefix or Alc-IPv6-Address) may be given in a single request. When host-accounting is enabled, only the host specific accounting session IDs (Acct-Session-Id) can be used. This means that to change for example the sla-profile for all three hosts of a dual stack subscriber, three CoA messages should be sent.

A full description of the RADIUS CoA functionality is out of the scope of this section.

Accounting

There are no separate accounting statistics available for IPv4 and IPv6 traffic unless they are mapped in a different Forwarding Class/queue.

In RADIUS accounting, host-accounting could be enabled to see the IPv4 and IPv6 host instantiations separately: an accounting start/stop is generated for each individual subscriber host. The actual accounting data is included in the interim updates and accounting stop message for the sla-profile instance.

A full description of the accounting functionality is out of the scope of this section.

Lease State Persistency

A DHCPv4/DHCPv6 (hereafter referred to as DHCP) session does not have a keep-alive mechanism to detect unavailability. A new DHCP session set-up is only attempted after expiration of the DHCP lease time. A node reboot causing the loss of DHCP lease state and the corresponding anti-spoof filters could therefore result in unacceptable long service outages.

The DHCP lease state can be made persistent across node reboots: DHCP lease state is restored from a persistency file stored on the compact flash file system. As a result, DHCP sessions will only loose connectivity during the time of reboot without being completely disconnected.

To activate the DHCP lease state persistency:

```
configure
    system
        persistence
            subscriber-mgmt
                description "DHCP lease state persistency"
                location cf2:
            exit
        exit
```

A dedicated persistency file will be created on the specified compact flash file system. The file is initialized to store the maximum number of allowed hosts; its size is fixed to avoid file system space problems during operations.

```
*A:BNG-1# file dir cf2:

 Volume in drive cf2 on slot A has no label.

 Volume in drive cf2 on slot A is formatted as FAT32.

Directory of cf2:\

09/02/2010  01:27p           536871424 submgmt.006
               1 File(s)              536871424 bytes.
               0 Dir(s)              1558183424 bytes free.
```

Each time the DHCP session is renewed, the persistency file is updated together with the lease state. If the file update fails, an event is generated to indicate that persistency can not be guaranteed.

The content of the persistency file may vary between different SR-OS software releases. When upgrading, the persistency file is automatically upgraded to the new format. To downgrade the persistency file to a lower SR-OS release version, use the following command:

```
*A:BNG-1# tools perform subscriber-mgmt downgrade ?
  - downgrade target-version <target> [reboot]

 <target>             : The version you want to downgrade to
                          8.0 (current)  - submgmt.006
                          7.0            - submgmt.005
                          6.0            - submgmt.004
                          5.0            - submgmt.003
                          4.0            - submgmt.pst
 <reboot>             : reboot system after successful conversion
```

The content of the persistency file can be looked at using the following commands:

```
*A:BNG-1# show service id 1 dhcp6 lease-state detail
===============================================================================
DHCP lease states for service 1
===============================================================================
Service ID           : 1
IP Address           : 2001:DB8:A001:100::/56
Client HW Address    : 00:0a:bc:00:00:01
Subscriber-interface : sub-int-1
Group-interface      : group-int-1
SAP                  : 1/1/2:1
Remaining Lifetime   : 23h49m47s
Persistence Key      : 0x0000004d

- - - snip - - -

*A:BNG-1# tools dump persistence submgt record 0x0000004d
-----------------------------------
Persistency File Record
-----------------------------------
Filename    : cf2:\submgmt.006
Key         : 0000004d
Last Update : 2010/09/02 16:13:12 (UTC)
Action      : ADD
Data :
 Host Type      : IpV6 node address
 Service ID     : 1
 SAP ID         : 1/1/2:1
 IP             : 2001:DB8:A001:100::/56
 NH MAC         : 00:0a:bc:00:00:01
 Created        : 2010/09/02 16:13:11 (UTC)
 Session Timeout: 0 (seconds)
 Sub-ID         : sub-1
 Sub-prof-ID    : sub-profile-1
 SLA-prof-ID    : sla-profile-1
 App-prof-ID    : NULL
 ANCP-Str       : NULL
 Int-dest-ID    : NULL
 Cat-map-str    : NULL
 Sub-Id is def  : NO
 Int-dest is def: YES
 Address Origin : 1
 SubId Origin   : 1
 Strings Origin : 1
```

```
RADIUS Fallback: NO
Managed routes : None
BgpPrngPlcyAttr: None
Class Attr     : 1 bytes
Radius Username: 00:0a:bc:00:00:01
Pri. IPv6 DNS  : 2001:DB8:DDDD:1::1
Sec. IPv6 DNS  : 2001:DB8:DDDD:2::1
```

Conclusion

This section provides configuration, operation and troubleshooting commands for dual stack IPoE subscribers on Routed Gateways. Focus is on the ESMv6 part where DHCPv6 is used for IPv6 address assignment on the RG network interface (wan host) and for allocation of an IPv6 prefix delegation prefix for use in the home network (pd host). In the BNG, authentication, authorization and IPv6 prefix configuration for an IPoE IPv6 host is done by a local user database or RADIUS.