Junos® OS

Dual-Stack Migration Guide for Subscriber Access Networks

Release
14.1

Published: 2014-05-14

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Dual-Stack Migration Guide for Subscriber Access Networks
Release 13.3

Revision History
May 2014—R1 Junos OS 14.1

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

Table of Contents

PART 1

Introduction to IPv4 and IPv6 Dual Stack for Broadband Edge

CHAPTER 1

Introduction to IPv4 and IPv6 Dual Stack

Audience for IPv4 and IPv6 Dual Stack

This guide is intended to assist service providers to design and plan an IPv6 implementation for their subscriber access networks, and then to use the dual-stack feature to deploy IPv6 alongside IPv4 in their networks. We intend the guide to be used by the following:

- Network architects—Responsible for creating the overall design and architecture of the dual-stack network.
- Network planners—Responsible for planning the implementation from a network perspective, including equipment.
- Network operations engineer—Responsible for creating the configuration that implements the overall design. Also responsible for deploying the implementation and actively monitoring the network.
- Sales engineers—Responsible for working with architects, planners, and operations engineers to design and implement the network solution.

Related Documentation

- Why Use IPv4/IPv6 Dual Stack? on page 3
- Basic Architecture of a Subscriber Access Dual-Stack Network on page 4

Why Use IPv4/IPv6 Dual Stack?

As a service provider, you can use the Junos OS IPv4/IPv6 dual-stack feature to begin your migration from IPv4 to IPv6 by implementing IPv6 alongside IPv4 in your existing subscriber networks. The feature allows you to implement IPv6 so that you can provide the same subscriber services over IPv6—video, voice, high-quality data—that you currently provide in your IPv4 networks. You can then perform incremental upgrades to IPv6 and avoid service disruptions while migrating from IPv4 to IPv6.

Related Documentation

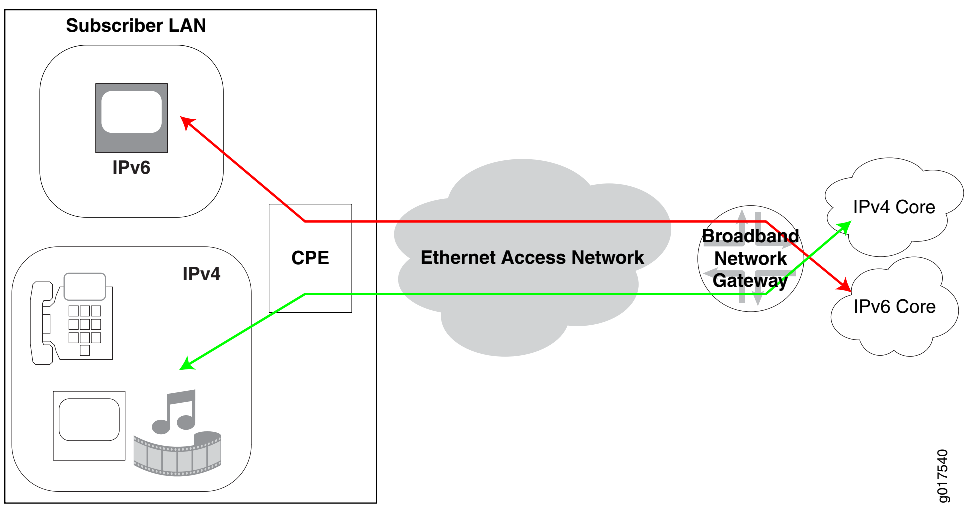
- Basic Architecture of a Subscriber Access Dual-Stack Network on page 4
- Terms Used in IPv4/IPv6 Dual-Stack Documentation on page 4
- Steps to Planning an IPv6 Implementation for a Dual-Stack Network on page 33

Basic Architecture of a Subscriber Access Dual-Stack Network

This Juniper Networks dual-stack architecture is designed for either DHCP-based or PPP/PPPoE-based subscriber access networks. In addition, this design allows you to layer DHCPv6 over PPPoE-based networks.

Figure 1 on page 4 shows the components of a basic subscriber access network in which the subscriber LAN is running both IPv4 and IPv6 and is connected to the IPv4 and IPv6 core using a broadband network gateway (BNG) configured for dual stack. Using IPv4/IPv6 dual stack, the BNG can provide both IPv4 and IPv6 services over the access network to the subscriber LAN. A single interface can operate simultaneously in IPv4 and IPv6 modes.

Figure 1: IPv4 and IPv6 Dual-Stack Architecture in a Subscriber Access Network



Related Documentation

- Why Use IPv4/IPv6 Dual Stack? on page 3
- Terms Used in IPv4/IPv6 Dual-Stack Documentation on page 4
- Steps to Planning an IPv6 Implementation for a Dual-Stack Network on page 33

Terms Used in IPv4/IPv6 Dual-Stack Documentation

Table 1 on page 5 defines terms used in the IPv4/IPv6 dual-stack documentation.

Table 1: IPv4/IPv6 Dual-Stack Terms

Term	Definition
Access network	Network that connects the subscriber premises directly to the subscriber's service provider.
BNG	Broadband network gateway. An IP edge router in which bandwidth and QoS policies may be applied. The BNG may encompass any or all of the functionality of B-RAS.
CPE	Customer premises equipment on the subscriber network that connects the subscriber network to the BNG.
Delegated addressing	Method of address assignment in which a host uses IPv6 prefixes to delegate IPv6 global addresses. In a dual-stack network, the CPE uses IPv6 prefixes that it receives to delegate global IPv6 addresses to individual subscriber equipment.
Delegating router	Role of the BNG when it delegates IPv6 prefixes to the requesting router (the CPE).
DHCPv6 IA	Identity association. A collection of addresses assigned to a client. Each IA contains one type of address. For example, IA_NA carries assigned addresses that are nontemporary addresses; IA_PD carries a prefix.
DHCPv6 IA_PD	IA for prefix delegation. An IA that carries a prefix that is assigned to the requesting router. Instead of assigning a single address, IA_PD assigns a prefix or a complete subnet. Referred to as DHCPv6 prefix delegation.
DHCPv6 IA_NA	IA for nontemporary addresses. An IA that carries assigned addresses that are not temporary addresses. DHCPv6 IA_NA is used to assign global IPv6 addresses.
Global IPv6 address	Unique IPv6 address that identifies a single interface and allows the interface to access the IPv6 internet.
IPv6 address prefix/prefix length	Combination of an IPv6 prefix (address) and a prefix length. The prefix takes the form *ipv6-prefix/prefix-length* and represents a block of address space (or a network). The */prefix-length* indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address. For example, 2001:DB8::/32 is an IPv6 prefix.
IPCP	IPv4 Control Protocol. A PPP protocol that establishes the IPv4 link between the BNG and the CPE if you are using PPPoE in your access network.
IPv6CP	IPv6 Control Protocol. A PPP protocol that establishes the IPv6 link between the BNG and the CPE if you are using PPPoE in your access network.

Table 1: IPv4/IPv6 Dual-Stack Terms *(continued)*

Term	Definition
Link-local address	Locally derived address that is designed to be used for addressing on a single link for purposes such as automatic address configuration, Neighbor Discovery, or when no routers are present. It is indicated by the prefix FE80::/10. In your dual-stack network, you can use a link-local address on the interface that connects the CPE and the BNG.
NDRA	Neighbor Discovery Router Advertisement. An IPv6 protocol that is used in the dual-stack network to allow automatic addressing on the CPE WAN link.
Neighbor dDiscovery	Protocol in the IPv6 protocol suite that allows nodes on the same link to advertise their existence to their neighbors, and to learn about the existence of their neighbors.
Prefix list	Table that contains IPv6 prefixes.
Requesting router	Role of the CPE when it requests IPv6 prefixes from the delegating router (the BNG).
Router Advertisement (RA)	Message that the BNG periodically sends to hosts or sends in response to Router Solicitation (RS) requests from another host. The message includes IPv6 prefixes and other autoconfiguration information. In a dual-stack network, the router sends RAs to CPE devices on its access network.
Router Solicitation (RS)	Message that hosts send to discover the presence of on-link routers. In a dual-stack network, CPE devices send RS messages to the BNG.
Subscriber LAN	Residential or small network.
Unnumbered address	Address that can be used on the router's PPPoE loopback interface that connects to the CPE.

Related Documentation

- Why Use IPv4/IPv6 Dual Stack? on page 3
- Basic Architecture of a Subscriber Access Dual-Stack Network on page 4

PART 2

Overview of IPv6 Addressing in a Dual-Stack Network

CHAPTER 2

Introduction to IPv6 Addresses

IPv6 Addressing Overview

IPv6 uses a 128-bit addressing model compared with the 32-bit addresses used for IPv4. In addition to being larger, IPv6 addresses differ from IPv4 addresses in several ways:

- Notation
- Prefixes
- Address types

These differences give IPv6 addressing greater simplicity and scalability than IPv4 addressing gives.

Related Documentation

- IPv6 Addressing Requirements for a Dual-Stack Network on page 13
- IPv6 Notation on page 9
- IPv6 Prefixes on page 10
- IPv6 Address Types on page 10

IPv6 Notation

IPv6 addresses are 128 bits long (expressed as 32 hexadecimal numbers) and consist of eight colon-delimited sections. Each section contains 2 bytes, and each byte is expressed as a hexadecimal number from 0 through FF.

An IPv6 address looks like this:

2001:0db8:0000:0000:0000:0800:200c:7334

By omitting the leading zeroes from each section or substituting contiguous sections that contain zeroes with a double colon, you can write the example address as:

2001:db8:0:0:0:800:200c:7334 or 2001:db8::800:200c:7334

You can use the double-colon delimiter only once within a single IPv6 address. For example, you cannot express the IPv6 address 2001:db8:0000:0000:ea34:0000:71ff:fe01 as 2001:db8::ea34::71ff:fe0.

Related Documentation

- IPv6 Addressing Overview on page 9
- IPv6 Prefixes on page 10
- IPv6 Address Types on page 10
- IPv6 Addressing Requirements for a Dual-Stack Network on page 13

IPv6 Prefixes

An IPv6 address prefix represents a block of address space or a network. The prefix is a combination of an IPv6 prefix (address) and a prefix length. It takes the form *ipv6-prefix/prefix-length*.

IPv6 addresses can be broken into prefixes of varying length. The prefix length is a decimal value that specifies the number of the leftmost bits in the address that make up the prefix. The prefix length follows a forward slash and, in most cases, identifies the portion of the address owned by an organization. All remaining bits (up to the right-most bit) represent individual nodes or interfaces.

For example, 2001:db8:0000:0000:250:af:34ff:fe26/64 has a prefix length of 64.

The first 64 bits of this address (2001:db8:0000:0000) are the prefix. The rest (250:af:34ff:fe26) identify the interface.

Related Documentation

- IPv6 Addressing Overview on page 9
- IPv6 Notation on page 9
- IPv6 Address Types on page 10
- IPv6 Addressing Requirements for a Dual-Stack Network on page 13

IPv6 Address Types

There are three major categories of IPv6 addresses:

- Unicast—For a single interface.
- Multicast—For a set of interfaces on the same physical medium. A packet is sent to all interfaces associated with the address.
- Anycast—For a set of interfaces on different physical media. A packet is sent to only one of the interfaces associated with this address, not to all the interfaces.

Unicast Addresses

A unicast address identifies a single interface. When a network device sends a packet to a unicast address, the packet goes only to the specific interface identified by that address. Unicast addresses support a global address scope and two types of local address scopes.

A unicast address consists of *n* bits for the prefix, and 128 – *n* bits for the interface ID.

In the IPv6 implementation for a subscriber access network, the following types of unicast addresses can be used:

- Global unicast address—A unique IPv6 address assigned to a host interface. These addresses have a global scope and essentially the same purposes as IPv4 public addresses. Global unicast addresses are routable on the Internet.
- Link-local IPv6 address—An IPv6 address that allows communication between neighboring hosts that reside on the same link. Link-local addresses have a local scope, and cannot be used outside the link. They always have the prefix FE80::/10.
- Loopback IPv6 address—An IPv6 address used on a loopback interfaces. The IPv6 loopback address is 0:0:0:0:0:0:0:1, which can be notated as ::1/128.
- Unspecified address—An IPv6 unspecified address is 0:0:0:0:0:0:0:0, which can be notated as ::/128.

Multicast Addresses

A multicast address identifies a set of interfaces that typically belong to different nodes. When a network device sends a packet to a multicast address, the device broadcasts the packet to all interfaces identified by that address. IPv6 does not support broadcast addresses, but instead uses multicast addresses in this role.

Multicast addresses support 16 different types of address scope, including node, link, site, organization, and global scope. A 4-bit field in the prefix identifies the address scope.

The following types of multicast addresses can be used in an IPv6 subscriber access network:

- Solicited-node multicast address—Neighbor Solicitation (NS) messages are sent to this address.
- All-nodes multicast address—Router Advertisement (RA) messages are sent to this address.
- All-routers multicast address—Router Solicitation (RS) messages are sent to this address.

Multicast addresses use the prefix FF00::/8.

Anycast Addresses

An anycast address identifies a set of interfaces that typically belong to different nodes. Anycast addresses are similar to multicast addresses, except that packets are sent only to one interface, not to all interfaces. The routing protocol used in the network usually determines which interface is physically closest within the set of anycast addresses and routes the packet along the shortest path to its destination.

There is no difference between anycast addresses and unicast addresses except for the subnet-router address. For an anycast subnet-router address, the low-order bits, typically 64 or more, are zero. Anycast addresses are taken from the unicast address space.

For more information about anycast addresses, see RFC 2526, *Reserved IPv6 Subnet Anycast Addresses*.

Related Documentation

- IPv6 Addressing Overview on page 9
- IPv6 Notation on page 9
- IPv6 Prefixes on page 10
- IPv6 Addressing Requirements for a Dual-Stack Network on page 13

CHAPTER 3

IPv6 Addressing Requirements in a Dual-Stack Network

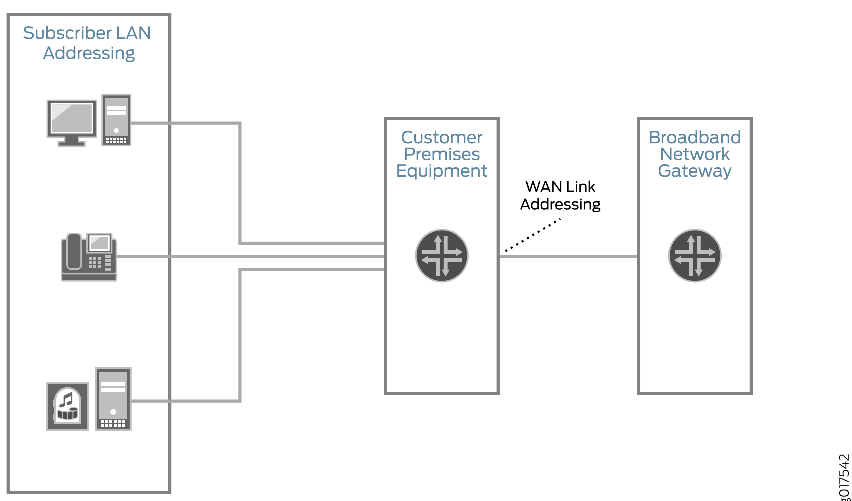
IPv6 Addressing Requirements for a Dual-Stack Network

You need to implement two types of addressing for IPv6 in a subscriber access network:

- WAN link addressing—For the WAN interface on the CPE (CPE upstream interface).
- Subscriber LAN addressing—For devices connected to the CPE on the subscriber LAN (CPE downstream interfaces).

Figure 2 on page 13 shows where WAN link addressing and subscriber addressing are assigned in a dual-stack network.

Figure 2: IPv6 Address Requirements in a Subscriber Access Network



You can use the following methods for assigning IPv6 addresses:

- For WAN link addressing, you can use Neighbor Discovery Router Advertisement (NDRA) or DHCPv6 Identity association for nontemporary addresses (IA_NA) to provision a global IPv6 address.
- For subscriber LAN addressing, you can use DHCPv6 prefix delegation to provision global IPv6 addresses to subscribers on the LAN.

Alternatives to Using a Global IPv6 Address on the CPE WAN Link

If the CPE is supplied by or recommended by the service provider, you do not need to provision a unique global IPv6 address on the CPE. In this case, the broadband network gateway (BNG) can use the loopback interface to manage the CPE. You can use one of the following methods to provision an address on the loopback interface:

- Link-local IPv6 address—Can be used on PPPoE access networks. The link-local address is provisioned by appending the interface identifier negotiated by IPv6CP with the IPv6 link-local prefix (FE80::/10).
- Address derived from DHCPv6 prefix delegation—Can be used on PPPoE access networks or on DHCP access networks. If you use DHCPv6 prefix delegation for subscriber addressing, the CPE can use the prefix it receives from the BNG to assign an IPv6 address on the loopback interface between the CPE and the BNG. This address can be used to manage the CPE, and the CPE uses it as a source address when it communicates with the BNG.

Related Documentation

- Overview of Using NDRA to Provide IPv6 WAN Link Addressing on page 15
- Overview of Using DHCPv6 IA_NA to Provide IPv6 WAN Link Addressing on page 21
- Overview of Using DHCPv6 Prefix Delegation on page 23
- Overview of Using DHCPv6 IA_NA with DHCPv6 Prefix Delegation on page 27
- Steps to Planning an IPv6 Implementation for a Dual-Stack Network on page 33

CHAPTER 4

Using NDRA to Provide IPv6 WAN Link Addressing in a Dual-Stack Network

Overview of Using NDRA to Provide IPv6 WAN Link Addressing

In a dual-stack network, NDRA provides a lightweight address assignment method for autoconfiguration of the global IPv6 address on the CPE WAN link. The CPE device can construct its own IPv6 global address by combining the interface ID that is negotiated by IPv6CP and the prefix obtained through NDRA.

Related Documentation

- IPv6 Addressing Requirements for a Dual-Stack Network on page 13
- IPv6 Neighbor Discovery Protocol Overview on page 15
- How NDRA Works in a Subscriber Access Network on page 16
- Design 2: IPv6 Addressing with NDRA and DHCPv6 Prefix Delegation on page 37
- Design 3: IPv6 Addressing with NDRA on page 38
- Configuration Tasks for PPPoE Access Networks in Which NDRA Is Used on page 78

IPv6 Neighbor Discovery Protocol Overview

Neighbor Discovery is a protocol in the IPv6 protocol suite that allows nodes on the same link to advertise their existence to their neighbors and to learn about the existence of their neighbors. Neighbor Discovery is built on top of Internet Control Message Protocol version 6 (ICMPv6). It replaces the following IPv4 protocols: Router Discovery (RDISC), Address Resolution Protocol (ARP), and ICMPv4 redirect.

Neighbor Discovery uses router advertisement messages to detect neighbors, advertise IPv6 prefixes, assist in address provisioning, and share link parameters such as MTU, hop limit, advertisement intervals, and lifetime.

Neighbor Discovery Messages

Neighbor Discovery uses the following message types:

- Router advertisement (RA)—Messages sent to announce the presence of the router, advertise prefixes, assist in address configuration, and share other link information such as MTU size and hop limit. The IPv6 nodes on the link can use this information to configure themselves with an IPv6 address and routing information such as the default gateway.
- Router solicitation (RS)—Messages sent by IPv6 nodes when they come online to solicit immediate router advertisements from the router.
- Neighbor solicitation (NS)—Messages used for duplicate address detection and to test reachability of neighbors.

  A host can verify that its address is unique by sending a neighbor solicitation message destined to the new address. If the host receives a neighbor advertisement in reply, the address is a duplicate.
- Neighbor advertisement (NA)—Messages used for duplicate address detection and to test reachability of neighbors. Neighbor advertisements are sent in response to neighbor solicitation messages.

You can specify the information that is sent in router advertisements.

Related Documentation

- Overview of Using NDRA to Provide IPv6 WAN Link Addressing on page 15
- How NDRA Works in a Subscriber Access Network on page 16

How NDRA Works in a Subscriber Access Network

Before NDRA can provide IPv6 address information to the CPE, you need to first obtain a link-local address for the CPE WAN link. NDRA provides address assignment in two phases:

1. Link-local address assignment for local connectivity to the BNG
2. Global address assignment for global connectivity

The process is as follows:

1. During IPv6CP negotiation to establish the PPPoE link between the BNG and the CPE, an interface identifier is negotiated for the CPE.
2. The CPE creates a link-local address by appending the interface identifier with the IPv6 link-local prefix (FE80::/10).

NOTE: When the interface ID is 0, such as for Windows 7 clients, PPP uses the subscriber's session ID in place of the interface ID.

The CPE now has IPv6 connectivity to the BNG, and it can use NDRA to obtain its global IPv6 address.

3. The CPE sends a router solicitation message to the BNG.
4. The BNG responds with a router advertisement message that includes an IPv6 prefix with a length of /64.

   This prefix can come directly from a local NDRA address pool configured on the BNG.

   If you are using AAA, a RADIUS server can specify the prefix in the *Framed-Ipv6-Prefix* attribute, or it can specify an NDRA pool on the BNG from which the prefix is assigned in the *Framed-Ipv6-Pool* attribute.
5. When the CPE receives the 64-bit prefix, it appends its interface ID to the supplied prefix to form a globally routable 128-bit address.
6. The CPE verifies that the global address is unique by sending a neighbor solicitation message destined to the new address. If there is a reply, the address is a duplicate. The process stops and requires operator intervention.

Related Documentation

- Overview of Using NDRA to Provide IPv6 WAN Link Addressing on page 15
- IPv6 Neighbor Discovery Protocol Overview on page 15
- Methods for Obtaining IPv6 Prefixes for NDRA on page 17

Methods for Obtaining IPv6 Prefixes for NDRA

You can set up the BNG to select IPv6 prefixes used for NDRA through one of the following methods:

- An external source such as a AAA RADIUS server.
- Dynamic assignment from a local pool of NDRA prefixes that is configured on the BNG

Using AAA RADIUS Server to Obtain IPv6 Prefixes for NDRA

When the BNG needs to obtain a prefix for NDRA, it uses the values in one of the following RADIUS attributes that it receives in Access-Accept messages from the RADIUS server:

- *Framed-IPv6-Prefix*—The attribute contains an IPv6 prefix that the BNG can send to the CPE in router advertisement messages.
- *Framed-IPv6-Pool*—The attribute contains the name of an NDRA pool configured on the BNG from which the BNG can select a prefix to include in router advertisements.

Related Documentation

- Overview of Using NDRA to Provide IPv6 WAN Link Addressing on page 15

- How NDRA Works in a Subscriber Access Network on page 16
- Configuring an Address-Assignment Pool Used for Router Advertisements on page 81

Duplicate Prefix Protection for NDRA

If you are using AAA to supply IPv6 prefixes for NDRA, you can enable duplicate prefix protection for NDRA. If enabled, the BNG checks the following attributes received from external servers:

- *Framed-IPv6-Prefix*
- *Framed-IPv6-Pool*

The router then takes one of the following actions:

- If a prefix overlaps with a prefix in an address pool, the prefix is taken from the pool if it is available.
- If the prefix is already in use, it is rejected as unavailable.
- If the prefix length requested from the external server does not match the pool's prefix length exactly, the authentication request is denied. If configured, the Acct-Stop message includes a termination cause.

Related Documentation

- Methods for Obtaining IPv6 Prefixes for NDRA on page 17
- Configuring Duplicate Prefix Protection for Router Advertisement on page 82

DNS Resolver for IPv6 DNS Overview

In a network that uses Neighbor Discovery Router Advertisement (NDRA) to provide IPv6 addressing, the DNS server address can be provided in Router Advertisements sent to IPv6 hosts. The address is included in a field called Recursive DNS Server (RDNSS). This feature is useful in networks that are not running DHCPv6.

RADIUS can populate the RDNSS field dynamically when an IPv6 subscriber logs in. On the RADIUS server, you can configure a primary and secondary DNS address in the following VSAs, which are stored in the $junos-ipv6-dns-server variable:

- Unisphere-Ipv6-Primary-Dns
- Unisphere-Ipv6-Secondary-Dns

When a subscriber logs in, RADIUS provides the actual DNS server address in the Access-Accept message.

You can also configure a static IPv6 address for DNS servers.

After the subscriber session is established, the DNS address is stored in the session database. When the router sends IPv6 router advertisements, it uses this DNS address in the RDNSS field in the Router Advertisement option.

Related Documentation

- Configuring a DNS Server Address for IPv6 Hosts on page 82
- *Configuring DNS Name Server Addresses for Subscriber Management*

CHAPTER 5

Using DHCPv6 IA_NA to Provide IPv6 WAN Link Addressing in a Dual-Stack Network

Overview of Using DHCPv6 IA_NA to Provide IPv6 WAN Link Addressing

You can use DHCPv6 IA_NA to assign a global IPv6 address to the CPE WAN link. If the CPE sends a Solicit message that contains the IA_NA option to the BNG, the BNG acts as a DHCPv6 server and assigns a single IPv6/128 address to the WAN interface of the CPE.

Related Documentation

- IPv6 Addressing Requirements for a Dual-Stack Network on page 13
- Design 1: IPv6 Addressing with DHCPv6 IA_NA and DHCPv6 Prefix Delegation on page 36
- Methods for Obtaining IPv6 Global Addresses for DHCPv6 IA_NA on page 21
- Selecting the Method of Provisioning a Global IPv6 Address for the WAN Link on page 42
- Configuring an Address-Assignment Pool for Use by DHCPv6 IA_NA on page 84

Methods for Obtaining IPv6 Global Addresses for DHCPv6 IA_NA

You can set up the BNG to select global IPv6 addresses to be delegated to the requesting router in one the following ways:

- An external source such as a AAA RADIUS server or a DHCP server using the DHCPv6 relay agent.
- Dynamic assignment from a local pool of addresses that is configured on the BNG

Using a AAA RADIUS Server to Obtain IPv6 Addresses for DHCPv6 IA_NA

When the BNG needs to obtain a global IPv6 for the CPE WAN link and optionally a DHCPv6 prefix, it uses the values in one of the following RADIUS attributes:

- *Framed-IPv6-Prefix*—The attribute contains a global IPv6 address with a prefix length of 128.

- *Framed-IPv6-Pool*—The attribute contains the name of an address-assignment pool configured on the BNG from which the BNG can select a global IPv6 address to send to the CPE.

Both attributes are sent from the RADIUS server to the BNG in RADIUS Access-Accept messages.

Related Documentation

- Overview of Using DHCPv6 IA_NA to Provide IPv6 WAN Link Addressing on page 21
- Configuring an Address-Assignment Pool for Use by DHCPv6 IA_NA on page 84

CHAPTER 6

Using DHCPv6 Prefix Delegation for Subscriber Addressing in a Dual-Stack Network

Overview of Using DHCPv6 Prefix Delegation

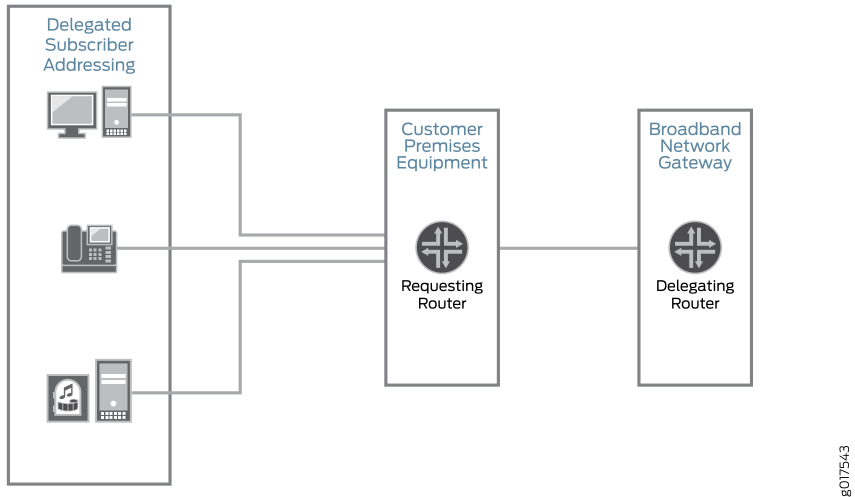
You can use DHCPv6 prefix delegation to automate the delegation of IPv6 prefixes to the CPE. With prefix delegation, a delegating router (the BNG) delegates IPv6 prefixes to a requesting router (the CPE). The requesting router then uses the prefixes to assign global IP addresses to the devices on the subscriber LAN. The requesting router can also assign subnet addresses to subnets on the LAN.

DHCPv6 prefix delegation is useful when the delegating router does not have information about the topology of the networks in which the requesting router is located. In such cases, the delegating router requires only the identity of the requesting router to choose a prefix for delegation.

DHCPv6 prefix delegation replaces the need for NAT in an IPv6 network.

Figure 3 on page 24 shows how DHCPv6 prefix delegation is used in a dual-stack network.

Figure 3: Delegated Addressing in a Dual-Stack Network Using DHCPv6



DHCPv6 prefix delegation operates as follows:

1. A delegating router is provided with IPv6 prefixes to be delegated to requesting routers. These prefixes can come from a local address-assignment pool or an external AAA server.

   Each prefix has an associated valid and preferred lifetime, which can be extended.

2. A requesting router requests one or more prefixes from the delegating router.
3. The delegating router chooses prefixes for delegation, and responds with prefixes to the requesting router.
4. The requesting router is then responsible for the delegated prefixes.

   The address allocation mechanism in the subscriber network can be performed with ICMPv6 Neighbor Discovery in router advertisements, DHCPv6, or a combination of these two methods.

Related Documentation

- IPv6 Addressing Requirements for a Dual-Stack Network on page 13
- Design 1: IPv6 Addressing with DHCPv6 IA_NA and DHCPv6 Prefix Delegation on page 36
- Design 2: IPv6 Addressing with NDRA and DHCPv6 Prefix Delegation on page 37
- Design 4: IPv6 Addressing with DHCPv6 Prefix Delegation and No NDRA Prefix on page 39
- Methods for Obtaining IPv6 Prefixes for DHCPv6 Prefix Delegation on page 26
- Selecting the Method of Assigning Global IPv6 Addresses to Subscribers on page 42

Using a Delegated Prefix on the CPE Loopback Interface

For networks in which the service provider directly controls the CPE, a delegated prefix can be used to create an IPv6 address on the loopback interface between the CPE and the BNG. This address can be used to manage the CPE, and the CPE uses it as a source address when it communicates with the BNG.

Related Documentation

- Overview of Using DHCPv6 Prefix Delegation on page 23
- Selecting the Type of Addressing Used on the CPE on page 41

DHCPv6 Prefix Delegation over PPPoE

The process of DHCPv6 prefix delegation when DHCPv6 is running over a PPPoE access network is as follows:

1. The CPE obtains a link-local address by appending the interface ID that it receives through IPv6CP negotiation to the IPv6 link-local prefix (FE80::/10). The link-local address provides an initial path for protocol communication between the BNG and CPE
2. The CPE sends a DHCPv6 Solicit message that includes an IA_PD option.
3. The BNG chooses a prefix for the CPE with information from an external AAA server or from a local prefix pool.
4. The BNG sends an Advertise message to the CPE. The message includes the delegated prefix, an IA_PD option, and an IA_PD prefix option. The prefix length in the IA_PD prefix option is 48. The message can also contain other configuration information, such as a maximum lease time.
5. The CPE sends a Request message to the BNG. The message requests the prefix that was advertised.
6. The BNG returns the delegated prefix to the CPE in a Reply message. This message also contains the delegated prefix, an IA_PD option, and an IA_PD prefix option. The prefix length in the IA_PD prefix option is 48. The message can also contain other configuration information, such as a maximum lease time.
7. The CPE uses the delegated prefix to allocate global IPv6 addresses to host devices on the subscriber network. It can use router advertisements, DHCPv6, or a combination of these two methods to allocate addresses on the subscriber LAN.

Related Documentation

- Overview of Using DHCPv6 Prefix Delegation on page 23
- Example: Configuring a Dual Stack That Uses NDRA and DHCPv6 Prefix Delegation over PPPoE on page 124

Methods for Obtaining IPv6 Prefixes for DHCPv6 Prefix Delegation

You can set up the BNG to select IPv6 prefixes to be delegated to the requesting router in one the following ways:

- An external source such as a AAA RADIUS server or a DHCP server using the DHCPv6 relay agent.
- Dynamic assignment from a local pool of prefixes that is configured on the BNG

  You can specify the name of a delegated pool to use for prefix delegation, which means that you do not need to use AAA to obtain the pool name. In this configuration, if you have also specified a pool match order, the specified delegated pool takes precedence.

Using a AAA RADIUS Server to Obtain IPv6 Prefixes for Prefix Delegation

When the BNG needs to obtain a prefix for DHCPv6 prefix delegation, it uses the values in one of the following RADIUS attributes:

- *Delegated-IPv6-Prefix*—The attribute contains an IPv6 prefix that the BNG can send to the CPE.
- *Jnpr-IPv6-Delegated-Pool-Name*—The attribute contains the name of an address-assignment pool configured on the BNG from which the BNG can select a prefix to send to the CPE.

Both attributes are sent from the RADIUS server to the BNG in RADIUS Access-Accept messages.

Related Documentation

- Overview of Using DHCPv6 Prefix Delegation on page 23
- Selecting the Method of Obtaining IPv6 Prefixes on page 43
- Configuring an Address-Assignment Pool for Use by DHCPv6 Prefix Delegation on page 83

CHAPTER 7

Using Both DHCPv6 IA_NA and DHCPv6 Prefix Delegation in a Dual-Stack Network

Overview of Using DHCPv6 IA_NA with DHCPv6 Prefix Delegation

You can use DHCPv6 IA_NA to assign a global IPv6 address to the CPE WAN link and DHCPv6 prefix delegation to provide prefixes for use on the subscriber LAN. DHCPv6 IA_NA and DHCPv6 prefix delegation are done in a single DHCPv6 session. If the CPE sends both the IA_NA and IA_PD options in the same DHCPv6 Solicit message, the BNG returns both a single IPv6/128 address and an IPv6 prefix.

When at least one address is successfully allocated, the router creates a subscriber entry and binds the entry to the assigned address. If both addresses are successfully allocated, the router creates a single subscriber entry and binds both addresses to that entry.

Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment

To configure dynamic DHCPv6 address assignment for both DHCPv6 IA_NA and DHCPv6 prefix delegation, use the **$junos-subscriber-ipv6-multi-address** variable In your dynamic profile. You use this variable in place of the **$junos-subscriber-ipv6-address** variable, which supports a single IPv6 address or prefix. The **$junos-subscriber-ipv6-multi-address** variable is applied as a demultiplexing source address array, and is expanded to include both the host and prefix addresses.

You include the **$junos-subscriber-ipv6-multi-address** variable at the **[edit dynamic-profile profile-name interfaces interface-name unit logical-unit-number family inet6 demux-source]** hierarchy level.

Lease Times and Session Timeouts for DHCPv6 IA_NA and DHCPv6 Prefix Delegation

When you use DHCPv6 IA_NA together with DHCPv6 prefix delegation, note the following about session timeouts and lease times:

- A session timeout from AAA has the highest precedence and overrides local pool lease times.

- For DHCPv6 local server, the minimum lease time associated with an address pool takes precedence over pools with longer lease times. For example, if a CPE obtains an IA_NA address from a pool with a lease time of 3600, and a prefix from a pool with a lease time of 7200, the lease time returned in the Reply message from the BNG is 3600.
- If AAA does not return a session timeout and the address pool does not have a configured lease time, the default setting of 86,400 (one day) is used.

Related Documentation

- Overview of Using DHCPv6 IA_NA to Provide IPv6 WAN Link Addressing on page 21
- Overview of Using DHCPv6 Prefix Delegation on page 23
- Design 1: IPv6 Addressing with DHCPv6 IA_NA and DHCPv6 Prefix Delegation on page 36
- Example: Configuring a Dual Stack That Uses DHCPv6 IA_NA and DHCPv6 Prefix Delegation over PPPoE on page 99

Methods for Obtaining Addresses for Both DHCPv6 Prefix Delegation and DHCPv6 IA_NA

You can set up the BNG to select global IPv6 addresses to be delegated to the requesting router in one the following ways:

- An external source such as a AAA RADIUS server or a DHCP server using the DHCPv6 relay agent.
- Dynamic assignment from a local pool of prefixes or global IPv6 addresses that is configured on the BNG

Address assignment for prefix delegation and IA_NA are independent. For example, you can use AAA RADIUS for DHCPv6 IA_NA, and use a local pool for prefix delegation.

Address Pools for DHCPv6 Prefix Delegation and DHCPv6 IA_NA

You need two separate address pools for prefix delegation and IA_NA. The pool used for IA_NA contains /128 addresses, and the pool for prefix delegation contains /56 or /48 addresses.

You can specify the name of a delegated pool to use for prefix delegation, which means that you do not need to use AAA to obtain the pool name. In this configuration, if you have also specified a pool match order, the specified delegated pool takes precedence.

You can configure pool attributes so that the IA_NA pool and the prefix delegation pool can specify different SIP servers for DNS addresses. DHCPv6 options that the BNG returns to the CPE are based on the pool from which the addresses were allocated. These options that are returned are based on the DHCPv6 Option Request option (ORO), which can be configured globally or within the IA_NA and IA_PD request.

Using a AAA RADIUS Server to Obtain IPv6 Addresses and Prefixes

When the BNG needs to obtain a global IPv6 address for the CPE WAN link and a DHCPv6 prefix, it uses the values in one of the following RADIUS attributes:

- *Framed-IPv6-Prefix*—The attribute contains a global IPv6 address and a prefix. A prefix length of 128 is associated with the global IPv6 address. Prefix lengths less than 128 are associated with prefixes.
- *Framed-IPv6-Pool*—The attribute contains the name of an address-assignment pool configured on the BNG, from which the BNG can select a global IPv6 address or an IPv6 prefix to send to the CPE.

Both attributes are sent from the RADIUS server to the BNG in RADIUS Access-Accept messages.

Related Documentation

- Overview of Using DHCPv6 IA_NA with DHCPv6 Prefix Delegation on page 27
- Selecting the Method of Assigning Global IPv6 Addresses to Subscribers on page 42
- Selecting the Method of Obtaining IPv6 Prefixes on page 43
- Configuring an Address-Assignment Pool for Use by DHCPv6 Prefix Delegation on page 83
- Configuring an Address-Assignment Pool for Use by DHCPv6 IA_NA on page 84

PART 3

Planning an IPv6 Implementation for Use in a Dual-Stack Network

CHAPTER 8

IPv6 Dual-Stack Planning Overview

Steps to Planning an IPv6 Implementation for a Dual-Stack Network

Deciding how to implement IPv6 in your network depends on a combination of existing infrastructure and future needs. We recommend that you follow these steps to plan your IPv6 implementation:

Step 1: Determine the routing platform requirements.

Step 2: Determine the IPv6 addressing requirements.

Step 3: Select the type of IPv6 addressing used on the CPE.

Step 4: Select the method of provisioning a global IPv6 address for the CPE WAN link.

Step 5: Select the method of assigning global IPv6 addresses to subscribers.

Step 6: Select the method of obtaining IPv6 addresses and prefixes.

Related Documentation

- Platform Considerations for a Dual-Stack Implementation on page 33
- IPv6 Addressing Requirements for a Dual-Stack Network on page 13
- Selecting the Type of Addressing Used on the CPE on page 41
- Selecting the Method of Provisioning a Global IPv6 Address for the WAN Link on page 42
- Selecting the Method of Assigning Global IPv6 Addresses to Subscribers on page 42
- Selecting the Method of Obtaining IPv6 Prefixes on page 43

Platform Considerations for a Dual-Stack Implementation

Table 2 on page 34 shows the combinations of routing hardware that you can use for your dual-stack implementation, along with information about access protocol and accounting support on each of the hardware combinations.

Table 2: Platform Support for a Dual-Stack Implementation

Routing Platform	PIC or MIC Support	Routing Engine Support	Access Protocol Support	Separate IPV4 and IPv6 Accounting Statistics Support	Comments
M120 Multiservice Edge Router	IQ2 PICs IQ2E PICs	RE-A-2000 RE-A-1800x2	PPPoE	No	Supports a static configuration only
M320 Multiservice Edge Router	IQ2 PICs IQ2E PICs	RE-A-2000 RE-A-1800x2	PPPoE	No	—
MX Series 3D Universal Edge Routers	3D Ethernet MICs	32-bit RE-2000 Series	PPPoE DHCPv6	Yes	—
MX Series 3D Universal Edge Routers	3D Ethernet MICs	RE-1800x2	PPPoE DHCPv6	Yes	Provides the highest level of logical interface scaling

Related Documentation

- Basic Architecture of a Subscriber Access Dual-Stack Network on page 4
- Steps to Planning an IPv6 Implementation for a Dual-Stack Network on page 33

CHAPTER 9

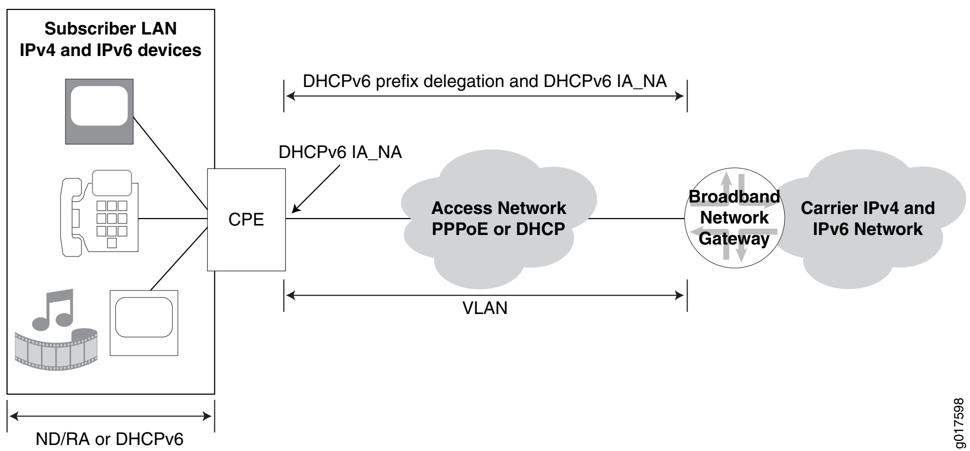
Designs for IPv6 Addressing in a Dual-Stack Network

Design 1: IPv6 Addressing with DHCPv6 IA_NA and DHCPv6 Prefix Delegation

This design (Figure 4 on page 36) uses DHCPv6 IA_NA and DHCPv6 prefix delegation in your subscriber access network as follows:

- DHCPv6 IA_NA is used to assign a global IPv6 address on the WAN link. The address can come from a local pool or AAA RADIUS.
- DHCPv6 prefix delegation is used for host device addressing. The delegated prefix can come from a local pool or from AAA RADIUS. The CPE uses the delegated prefix for subscriber addressing. The CPE can use NDRA or DHCPv6 to allocate IPv6 addresses on the LAN.

Figure 4: Subscriber Access Network with DHCPv6 IA_NA and DHCPv6 Prefix Delegation



Related Documentation

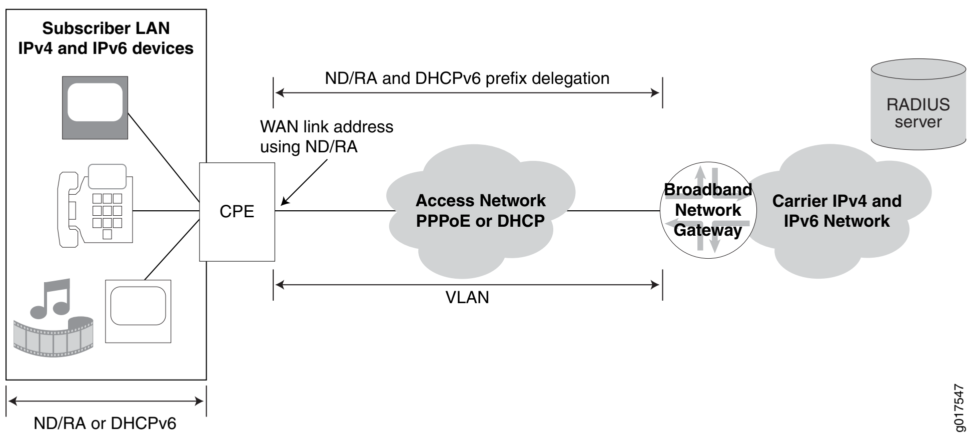
- Example: Configuring a Dual Stack That Uses DHCPv6 IA_NA and DHCPv6 Prefix Delegation over PPPoE on page 99
- Overview of Using DHCPv6 IA_NA with DHCPv6 Prefix Delegation on page 27

Design 2: IPv6 Addressing with NDRA and DHCPv6 Prefix Delegation

This design (Figure 5 on page 37) uses NDRA and DHCPv6 prefix delegation in your subscriber access network as follows:

- NDRA addressing is used to provision a global IPv6 address on the WAN link. IPv6 prefixes for NDRA come from a local pool or AAA RADIUS.
- DHCPv6 prefix delegation is used for host device addressing. The delegated prefix can come from a local pool or from AAA RADIUS. The CPE uses the delegated prefix for subscriber addressing. The CPE can use NDRA or DHCPv6 to allocate IPv6 addresses on the LAN.

Figure 5: Subscriber Access Network with NDRA and DHCPv6 Prefix Delegation



If you have a network with a combination of subscriber LANs and single PCs, you can use a combination of design 2 and design 3.

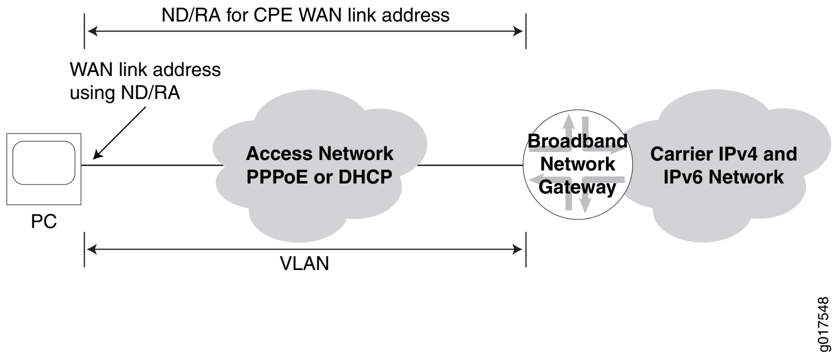
Related Documentation

- Example: Configuring a Dual Stack That Uses NDRA and DHCPv6 Prefix Delegation over PPPoE on page 124
- How NDRA Works in a Subscriber Access Network on page 16
- Overview of Using DHCPv6 Prefix Delegation on page 23

Design 3: IPv6 Addressing with NDRA

In this design (Figure 6 on page 38), NDRA is used for addressing a global IPv6 on the WAN link with prefixes from a local pool or AAA RADIUS. The PC does not need a delegated prefix.

Figure 6: Subscriber Access Network with NDRA



If you have a network with a combination of subscriber LANs and single PCs, you can use a combination of Design 2 and Design 3.

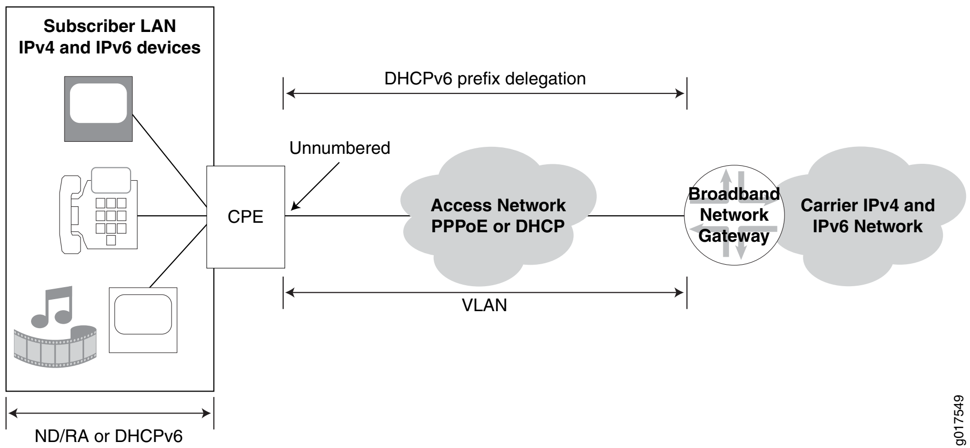
Related Documentation

- Example: Configuring a Dual Stack That Uses NDRA over PPPoE on page 145
- How NDRA Works in a Subscriber Access Network on page 16

Design 4: IPv6 Addressing with DHCPv6 Prefix Delegation and No NDRA Prefix

In this design (Figure 7 on page 39), the CPE is a model that is sold by or specified by the service provider. The CPE uses an unnumbered WAN interface. The BNG delegates an IPv6 prefix to the CPE with DHCPv6 prefix delegation. The CPE uses the delegated prefix for subscriber addressing. It can use NDRA or DHCPv6 to allocate the IPv6 addresses on the LAN.

Figure 7: Subscriber Access Network with DHCPv6 Prefix Delegation



Related Documentation

- Overview of Using DHCPv6 Prefix Delegation on page 23

CHAPTER 10

Selecting the Methods of Assigning IPv6 Addresses

Selecting the Type of Addressing Used on the CPE

In some networks, you do not need to assign a global IPv6 address on the CPE WAN link. Your decision depends on the type of CPE being used:

- If the CPE is purchased by the subscriber, and is not a device specifically recommended by the service provider, you need to assign a global IPv6 address that can be routed on the Internet.
- If the CPE is supplied by or recommended by the service provider, you can use the loopback interface to manage the CPE.

  In this case, you can use a link-local address or you can use an address that is derived from DHCPv6 prefix delegation.

Related Documentation

- IPv6 Addressing Requirements for a Dual-Stack Network on page 13

Selecting the Method of Provisioning a Global IPv6 Address for the WAN Link

To assign a global IPv6 address to the WAN link of the CPE device, you can choose one of the methods described in Table 3 on page 42.

Table 3: Choosing the Global IPv6 Address Provisioning Method for the WAN Link

NDRA Features	DHCPv6 IA_NA Features
Provides address autoconfiguration of the WAN link by means of router advertisements.	Provides a single IPv6/128 address to the WAN interface of the CPE by the BNG acting as a DHCPv6 server.
Supported on PPPoE access networks.	Supported on PPPoE and DHCP access networks.
Provides duplicate prefix prevention.	Provides the ability to use one DHCPv6 message to solicit both a global IPv6 address for the WAN link, and a prefix used to provision addresses on the subscriber LAN.
Use if the CPE does not support DHCP.	--

Related Documentation

- IPv6 Addressing Requirements for a Dual-Stack Network on page 13
- Overview of Using NDRA to Provide IPv6 WAN Link Addressing on page 15
- Overview of Using DHCPv6 IA_NA to Provide IPv6 WAN Link Addressing on page 21

Selecting the Method of Assigning Global IPv6 Addresses to Subscribers

BEST PRACTICE: For addressing on the subscriber LAN, we recommend that you provision a global IP address for each device on the LAN. IPv6 was designed to allow every IP-capable device on a subscriber LAN to obtain a globally unique address, which avoids the use of NAT between the subscriber LAN and the service provider.

DHCPv6 prefix delegation automates the delegation of IPv6 prefixes to the CPE. The CPE can then use these prefixes to assign global IPv6 addresses for use in a subscriber LAN. DHCPv6 prefix delegation is useful when the delegating router (the BNG) does not have information about the topology of the networks in which the requesting router (the CPE) is located. In such cases, the delegating router requires only the identity of the requesting router to choose a prefix for delegation.

Related Documentation

- Overview of Using DHCPv6 Prefix Delegation on page 23
- Overview of Using DHCPv6 IA_NA with DHCPv6 Prefix Delegation on page 27

Selecting the Method of Obtaining IPv6 Prefixes

You can set up the BNG to select IPv6 prefixes through one of the following methods:

- An external source such as a AAA RADIUS server or a DHCP server using the DHCPv6 relay agent.
- Dynamic assignment from a local pool of global IPv6 addresses or prefixes that is configured on the BNG

Using a AAA RADIUS Server to Obtain Global IPv6 Addresses and IPv6 Prefixes

Table 4 on page 43 describes the RADIUS attributes used in a dual-stack network. These attributes are sent from the RADIUS server to the BNG in RADIUS Access-Accept messages.

Table 4: RADIUS Attributes Used to Obtain Global IPv6 Addresses and IPv6 Prefixes

RADIUS Attribute	Address Assignment Type	Attribute Description
Framed-IPv6-Prefix	NDRA	IPv6 prefix with a prefix length less than 128.
	DHCPv6 IA_NA	IPv6 prefix with a length of 128.
Framed-IPv6-Pool	NDRA	Name of an NDRA pool configured on the BNG from which the BNG selects a prefix.
	DHCPv6 IA_NA	Name of an address-assignment pool configured on the BNG from which the BNG selects a global IPv6 address.
Delegated-IPv6-Prefix	DHCPv6 prefix delegation	IPv6 prefix.
Jnpr-IPv6-Delegated-Pool-Name	DHCPv6 prefix delegation	Name of an address-assignment pool configured on the BNG from which the BNG delegates a prefix.

Related Documentation

- IPv6 Addressing Requirements for a Dual-Stack Network on page 13
- Overview of Using DHCPv6 Prefix Delegation on page 23

PART 4

IPv4 and IPv6 Dual-Stack Models

CHAPTER 11

Dual-Stack Access Models in a PPPoE Network

IPv4 and IPv6 Dual Stack in a PPPoE Access Network

In a dual-stack architecture with a PPPoE access network that connects the CPE to the BNG, IPv4 and IPv6 connectivity are provided over a single PPP logical link. The PPP IPv4 control protocol (IPCP) and the IPv6 control protocol (IPv6CP) provide independent IPv4 and IPv6 connectivity over the logical link.

The BNG and the CPE handle both IPCP and IPv6CP identically and simultaneously over a single PPP connection. The BNG or the CPE can open and close any Network Control Protocol (NCP) session without affecting the other sessions. This capability allows for a dynamic setup where IPv4 (family inet) and IPv6 (family inet6) sessions can be brought up and down individually. As long as one family is active, the subscriber remains active.

Figure 8 on page 48 shows a dual-stack interface stack in a PPPoE access network. The IPv4 family (inet) and the IPv6 family (inet6) can reside on the same PPPoE logical interfaces. The family inet and family inet6 parts of dynamic profiles are applied, and services are activated when each individual family is negotiated.

Figure 8: Dual-Stack Interface Stack over a PPPoE Access Network

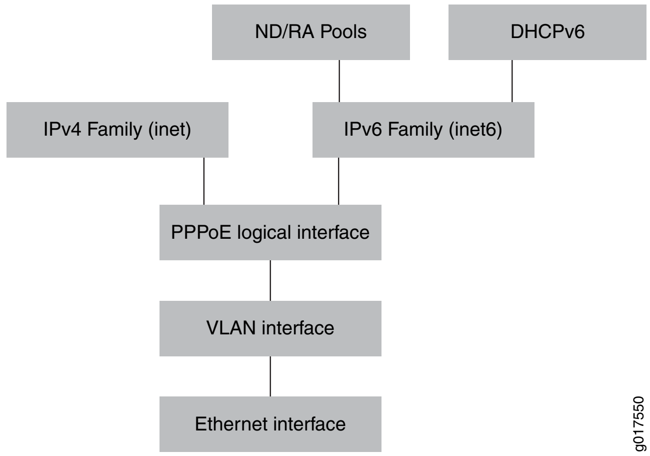
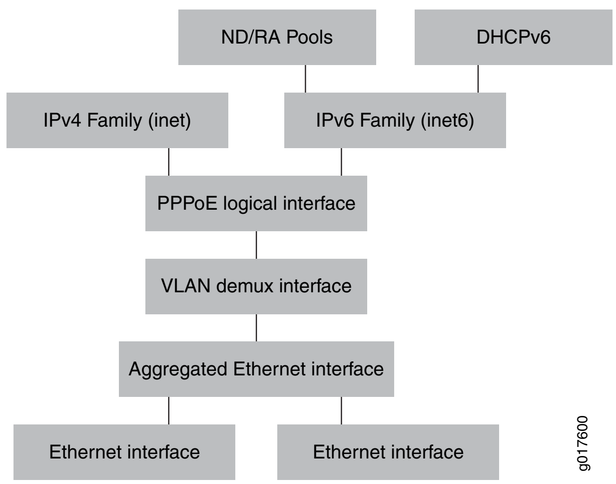


Figure 9 on page 48 shows a dual-stack interface stack over aggregated Ethernet in a PPPoE access network.

Figure 9: Dual-Stack Aggregated Ethernet Stack over a PPPoE Access Network



Support for Demultiplexing Interfaces

IPv4 and IPv6 dual stack is supported on VLAN demultiplexing (demux) interfaces. Dual stack is not supported on IP demux interfaces.

Determining the Status of CPE in a PPPoE Access Network

In a PPPoE access network, you can enable keepalives to determine the status of the CPE.

IPV6 Address Provisioning in the PPPoE Access Network

IPv6CP negotiates the interface identifier, which can be used to provision link-local addresses that are used for direct connectivity between the BNG and the CPE. Because

PPPoE negotiates only interface IDs and does not negotiate IPv6 addresses, PPPoE relies on other protocols for addressing. The protocols you can use are DHCPv6 and NDRA.

Authentication in a PPPoE Access Network

In a PPPoE network, you can use PAP and CHAP to identify and authenticate the CPE and subscriber sessions.

You can also use AAA for authentication and authorization through external RADIUS servers.

Negotiation of Network Control Protocols When Authorized Addresses Are Unavailable

NCP negotiation is initiated for subscriber sessions by default, even when authorized addresses are not available. An example of this situation is when the DHCPv6 local server is configured with an override so that the jpppd process never receives an IPv6 address or prefix from AAA, although the DHCPv6 local server receives a prefix from a delegated pool. In this situation, the client attempts to negotiate IPv6CP with the jpppd process.

By default, when IPCP negotiation is attempted for an IPv4-only PPPoE subscriber session on a dynamic interface, the jpppd process issues a Protocol-Reject message if AAA does not provide an IPv4 address. However, negotiation is allowed to proceed when the **on-demand-ip-address** statement is included at the **[edit protocols ppp-service]** or **[edit dynamic-profiles *profile-name* interfaces pp0 unit $junos-interface-unit ppp-options]** hierarchy level.

IPCP negotiation is enabled by default for an IP destination address defined on a static interface.

In contrast, IPv6CP negotiation is enabled to proceed by default for an IPv6-only session when AAA has not provided an appropriate IPv6 address or prefix. To prevent endless client negotiation of IPv6CP, you can alter the behavior by including the **reject-unauthorized-ipv6cp** statement at the **[edit protocols ppp-service]** hierarchy level. This statement enables the jpppd process to reject the negotiation attempt.

When IPv6CP rejection is enabled, jpppd also issues a Protocol-Reject message when router advertisement is not enabled in the dynamic profile that instantiates the interface but only a Framed-IPv6-Prefix attribute is received.

Related Documentation

- AAA Service Framework in a Dual Stack over a PPPoE Access Network on page 50
- Basic Architecture of a Subscriber Access Dual-Stack Network on page 4
- Configuration Tasks for a PPPoE Access Network in Which DHCP Is Used on page 75
- Configuring a PPPoE Dynamic Profile for Use with DHCP Addressing in a Dual-Stack Network on page 76
- Configuration Tasks for PPPoE Access Networks in Which NDRA Is Used on page 78
- Avoiding Negotiation of IPv6CP in the Absence of an Authorized Address on page 88
- Saving IPv4 Addresses for Dual-Stack PPP Subscribers on page 57

Shared IPv4 and IPv6 Service Sessions on PPP Access Networks

You can configure one dynamic service profile that supports IPv4, IPv6, or both IPv4 and IPv6. It allows subscribers to share the same service session using IPv4 and IPv6 address families. If you define IPv4 and IPv6 in the dynamic service profile, one address family or both address families can be activated for the service. When the service is activated, matched packets are tagged with the same traffic class and treated the same way for both IPv4 and IPv6 traffic.

Accounting for Shared IPv4 and IPv6 Service Sessions

When service sessions are shared for both IPv4 and IPv6 subscribers, only one Accounting-Start message is sent for each service session regardless of the number of address families that are active. Statistics for each address family of a service session are cumulative across service activations and deactivations of the service.

Deactivating Shared IPv4 and IPv6 Service Sessions

If both IPv4 and IPv6 service sessions are active, and a deactivation message is received for one of the address families (IPv4 or IPv6), all active services for that address family are deactivated. If one address family remains active on the service, the service session remains in the ACTIVE state. If the address family that is deactivated is the only family currently running on the service session, the service returns to the INIT state.

Related Documentation

- IPv4 and IPv6 Dual Stack in a PPPoE Access Network on page 47
- Configuring a PPPoE Dynamic Profile for Use with DHCP Addressing in a Dual-Stack Network on page 76
- Configuring a PPPoE Dynamic Profile for Use with NDRA in a Dual-Stack Network on page 78

AAA Service Framework in a Dual Stack over a PPPoE Access Network

You can use the AAA Service Framework for all authentication, authorization, accounting, address assignment, and dynamic request services that the BNG uses for network access. The framework supports authentication and authorization through external RADIUS servers. It also supports accounting and dynamic-request change of authorization (CoA) and disconnect operations through external servers, and address assignment through a combination of local address-assignment pools and RADIUS servers.

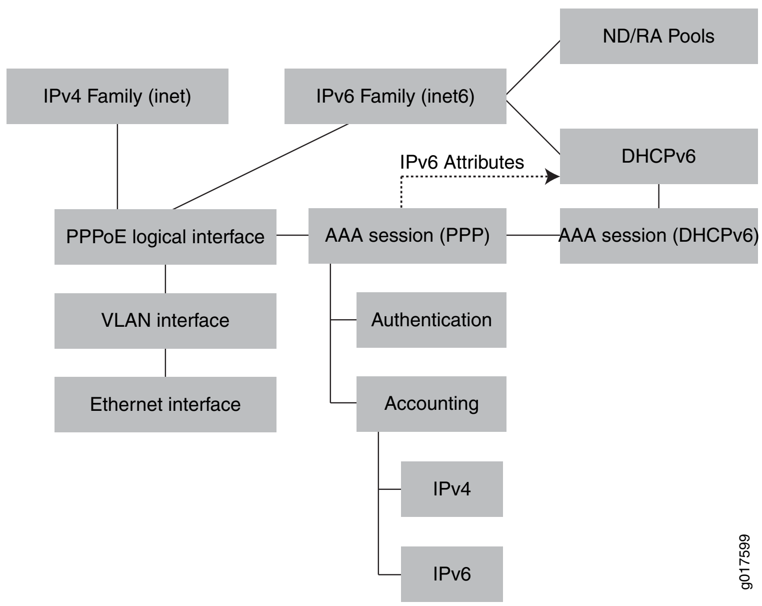
The BNG interacts with external servers to determine how individual subscribers access the broadband network. The BNG can also obtain information from external servers for the following:

- How subscribers are authenticated.
- How accounting statistics are collected and used.
- How dynamic requests, such as CoA, are handled.

As shown in Figure 10 on page 51, implementing a dual stack over a PPPoE access network that uses AAA can have the following characteristics:

- DHCPv6—If used, it runs over the IPv6 family session, and it inherits attributes from the underlying PPPoE session.
- NDRA—If used, it runs over the IPv6 family session.
- IPv4 and IPv6 accounting—One accounting session handles both IPv4 and IPv6 accounting information.

Figure 10: AAA Service Framework in a Dual Stack over a PPPoE Access Network



Collection of Accounting Statistics in a PPPoE Access Network

AAA provides support for both IPv4 and IPv6 statistics in one accounting session. On MX Series 3D Universal Edge routers AAA also provides support for separate IPv4 and IPv6 accounting statistics.

The following RADIUS attributes are included by default (when available) in Acct-Start, Interim, and Acct-Stop messages:

- Framed-IPv6-Prefix
- Framed-IPv6-Pool
- Delegated-Ipv6-Prefix
- Framed-IPv4-Route
- Framed-IPv6-Route

You can configure the BNG to exclude these attributes in Acct-Start and Acct-Stop messages.

Change of Authorization (CoA)

RADIUS servers can initiate dynamic requests to the BNG. Dynamic requests include CoA requests, which specify vendor-specific attribute (VSA) modifications and service changes.

In your access profile configuration, you specify the IP addresses of RADIUS authentication servers that can initiate dynamic requests to the router. The list of authentication servers also provides RADIUS-based dynamic service activation and deactivation during subscriber login.

Related Documentation

- IPv4 and IPv6 Dual Stack in a PPPoE Access Network on page 47

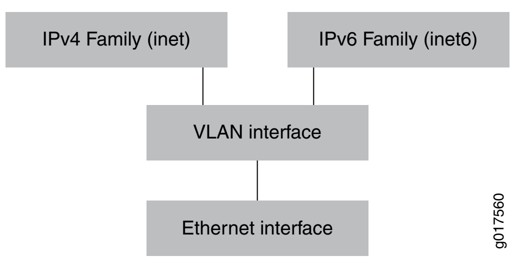
CHAPTER 12

Dual-Stack Access Models in a DHCP Network

IPv4 and IPv6 Dual Stack in a DHCP Access Network

Figure 11 on page 53 shows a dual-stack interface stack in a DHCP access network. The IPv4 family (inet) and the IPv6 family (inet6) can reside on the same VLAN interface.

Figure 11: Dual-Stack Interface Stack over a DHCP Access Network



NOTE: When you are using IPv4 and IPv6 dual stack on the same DHCP interface, you must configure one dynamic profile for both the IPv4 and IPv6 subscribers. You cannot run IPv4 and IPv6 subscriber sessions over the same interface if you configure separate dynamic profiles for IPv4 and IPv6.

Support for Demultiplexing Interfaces

IPv4 and IPv6 dual stack is supported on VLAN demultiplexing (demux) interfaces. Dual stack is not supported on IP demux interfaces.

Related Documentation

- Basic Architecture of a Subscriber Access Dual-Stack Network on page 4
- AAA Service Framework in a Dual Stack over a DHCP Access Network on page 54
- Dual-Stack Interface Stack in a DHCP Wholesale Network on page 55

- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

AAA Service Framework in a Dual Stack over a DHCP Access Network

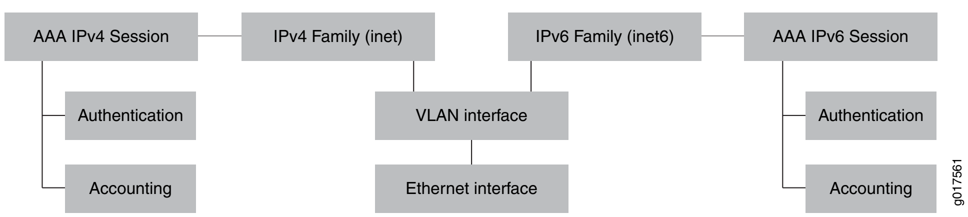
You can use the AAA Service Framework for all authentication, authorization, accounting, address assignment, and dynamic request services that the BNG uses for network access. The framework supports authentication and authorization through external RADIUS servers. It also supports accounting and dynamic-request change of authorization (CoA) and disconnect operations through external servers, and address assignment through a combination of local address-assignment pools and RADIUS servers.

The BNG interacts with external servers to determine how individual subscribers access the broadband network. The BNG can also obtain information from external servers for the following:

- How subscribers are authenticated.
- How accounting statistics are collected and used.
- How dynamic requests, such as CoA, are handled.

As shown in Figure 12 on page 54, an implementation of dual stack over a DHCP access network, there are separate AAA sessions for IPv4 and IPv6 authentication and accounting.

Figure 12: AAA Service Framework in a Dual Stack over a DHCP Access Network



Collection of Accounting Statistics in a DHCP Access Network

AAA provides support for IPv4 and IPv6 statistics in separate accounting sessions.

The following RADIUS attributes are included by default (when available) in Acct-Start, Interim, and Acct-Stop messages:

- Framed-IPv6-Prefix
- Framed-IPv6-Pool
- Delegated-Ipv6-Prefix
- Framed-IPv4-Route
- Framed-IPv6-Route

You can configure the BNG to exclude these attributes in accounting Acct-Start and Acct-Stop messages.

Change of Authorization (CoA)

RADIUS servers can initiate dynamic requests to the BNG. Dynamic requests include CoA requests, which specify VSA modifications and service changes.

In your access profile configuration, you specify the IP addresses of RADIUS authentication servers that can initiate dynamic requests to the router. The list of authentication servers also provides RADIUS-based dynamic service activation and deactivation during subscriber login.

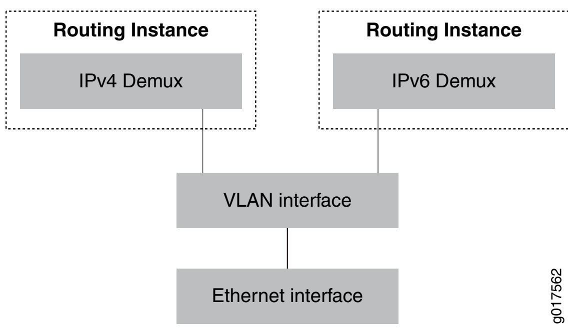
Related Documentation

- IPv4 and IPv6 Dual Stack in a DHCP Access Network on page 53

Dual-Stack Interface Stack in a DHCP Wholesale Network

Figure 13 on page 55 shows a dual-stack interface stack in a DHCP wholesale network. In this scenario, the IPv4 and IPv6 demux interfaces are configured on the same VLAN interface. The demux interfaces are configured in a separate logical system:routing instance.

Figure 13: Dual-Stack Interface Stack in a DHCP Wholesale Network



Related Documentation

- IPv4 and IPv6 Dual Stack in a DHCP Access Network on page 53
- AAA Service Framework in a Dual Stack over a DHCP Access Network on page 54

CHAPTER 13

Saving IPv4 Addresses for Dual-Stack PPP Subscribers

Saving IPv4 Addresses for Dual-Stack PPP Subscribers

You can save IPv4 addresses for dual-stack PPP subscribers when you are not using the IPv4 service. This provides on-demand IP address allocation or de-allocation after the initial PPP authentication and IPv6 address or prefix allocation. For dynamic profiles, changing this setting takes effect for any new subscribers. You can also include the Unisphere-Ipv4-release-control VSA in the Access-Request that is sent during on-demand IP address allocation. You can also include Interim-Accounting messages that are sent to report an address change.

Related Documentation

- How IPv4 Address Negotiation and Release for Static PPP Subscribers Works in a Subscriber Access Network on page 58
- How IPv4 Address Negotiation and Release for Dynamic PPP Subscribers Works in a Subscriber Access Network on page 61
- How Framed-IP-Address and Framed-Pool Attributes Work for IPv4 PPP Subscribers on page 63

How IPv4 Address Negotiation and Release for Static PPP Subscribers Works in a Subscriber Access Network

You can use on-demand IPv4 address allocation or de-allocation for static dual-stack subscribers.

IPv4 Address Negotiation for Static PPP Subscribers

The process for IPv4 address negotiation for a static inet family and address over a static PPP interface is as follows:

1. PPP Link Control Protocol (LCP) is established and an IPv6 control protocol is successfully negotiated.
2. The broadband network gateway (BNG) receives an Internet Protocol Control Protocol (IPCP) Configure Request with a 0.0.0.0 IPv4 address option from the customer premises equipment (CPE).
3. The BNG sends an IPCP Configure Request with a local IPv4 address option to the CPE.
4. The BNG sends an Access-Request message with the Unisphere-Ipv4-release-control VSA (if configured) to the RADIUS server.
5. The BNG receives an IPCP Configure ACK from the CPE.
6. The BNG receives an Access-Accept message from the RADIUS server.
    - If a Framed-IP-Address attribute is received, then a duplicate address check (if configured) is performed on the BNG. If a duplicate address check is completed successfully, then PPP continues IPCP negotiation with the CPE. Otherwise, the entire PPP session is brought down by sending an LCP terminate request to the CPE.
    - If a Framed-Pool attribute is received, then the IPv4 address is allocated from the specified local address pool configured in the BNG. If the IP pool is not configured in the BNG and there is no other IP pool available, then the IPCP protocol reject is sent to the CPE.
    - If neither a Framed-IP-Address attribute nor a Framed-Pool attribute is received, then the BNG allocates an IPv4 address from one of the configured local address pools. If the BNG cannot allocate an IPv4 address, then the IPCP protocol reject is sent to the CPE.
    - If ADFv4 filters are present in the Access-Accept message, then they need to be reinstalled for that subscriber in the BNG.
    - If both IPv4 primary and secondary DNS addresses are present in the Access-Accept message, then both need to be updated for that subscriber in the BNG. If either an IPv4 primary DNS address or an IPv4 secondary DNS address is present in the Access-Accept message, then only the corresponding DNS address needs to be updated for that subscriber.

If the BNG receives an Access-Reject message from the RADIUS server instead of an Access-Accept message, the following occurs:

- If the Access-Reject message includes the Unisphere-Ipv4-release-control VSA and Reply Message attribute #18, the BNG sends an IPCP terminate request to the CPE. The CPE is then allowed to renegotiate IP NCP.
- If the either the Unisphere-Ipv4-release-control VSA or Reply Message attribute #18 are not included in the Access-Reject message, an LCP Protocol-Reject message is sent to the CPE. The CPE must renegotiate the LCP link before it is allowed to renegotiate IP NCP.

  If the RADIUS Access-Reject message includes the IPCP Terminate-Request field, the text of Reply Message attribute #18 is appended to the information in the Terminate-Request field, and will be shown in PPP data.

If there is no response from the RADIUS server, then IPCP is terminated.

7. The BNG sends an IPCP Configure NACK with the new IPv4 address option to the CPE.
8. The subscriber secure policy service (if present for inet family) is activated.

   The BNG sends an immediate Interim-Accounting message (if configured) with the Unisphere-Ipv4-release-control VSA (if configured) and the Framed-IP-Address attribute to the RADIUS server.
9. The BNG receives an IPCP Configure Request with new IPv4 address option from the CPE.
10. The BNG receives an Interim-Accounting response from the RADIUS server.
11. The BNG sends an IPCP Configure ACK to the CPE.

IPv4 Address Release for Static PPP Subscribers

The process for IPv4 address release for static inet family and address over static PPP interface is as follows:

1. The BNG receives an IPCP terminate request from the CPE.
2. The BNG sends an IPCP terminate ACK to the CPE.
3. The following actions occur:
   - The subscriber secure policy service (if present for inet family) is de-instantiated.
   - If an IPv4 address was allocated from local address pool, the address then becomes available.
   - The IPv4 address entry is cleared from the subscriber record.

- The BNG sends an immediate Interim-Accounting message (if configured) with the Unisphere-Ipv4-release-control VSA (if configured) to the RADIUS server and the Framed-IP-Address attribute is not included.
- User Session Statistics are retained for the entire PPP session and are not cleared when the IPv4 address is released.

4. The BNG receives an Interim-Accounting response from the RADIUS server.

   No action is taken in the BNG whether or not it receives a response from the RADIUS server.

Related Documentation

- Saving IPv4 Addresses for Dual-Stack PPP Subscribers on page 57
- How IPv4 Address Negotiation and Release for Dynamic PPP Subscribers Works in a Subscriber Access Network on page 61

How IPv4 Address Negotiation and Release for Dynamic PPP Subscribers Works in a Subscriber Access Network

You can use on-demand IPv4 address allocation or de-allocation for dynamic dual-stack subscribers.

IPv4 Address Negotiation for Dynamic PPP Subscribers

The process for IPv4 address negotiation for a dynamic inet family and address over a static PPP interface is as follows:

1. PPP Link Control Protocol (LCP) is established and IPv6 control protocol is successfully negotiated.
2. The broadband network gateway (BNG) receives an Internet protocol Control Protocol (IPCP) Configure Request with a 0.0.0.0 IPv4 address option from the CPE.
3. The BNG sends an Access-Request message with the Unisphere-Ipv4-release-control VSA (if configured) to the RADIUS server.
4. The BNG receives an Access-Accept message from the RADIUS server.
   - If a Framed-IP-Address attribute is received, then a duplicate address check (if configured) is performed on the BNG. If a duplicate address check is completed successfully, then PPP continues IPCP negotiation with the CPE. Otherwise, the entire PPP session is brought down by sending an LCP terminate request to the CPE.
   - If Framed-Pool attribute is received, then the IPv4 address is allocated from the specified local address pool configured in the BNG. If the pool is not configured in the BNG and there is no other IP pool available, then an IPCP protocol reject is sent to the CPE.
   - If neither a Framed-IP-Address attribute nor a Framed-Pool attribute is received, then the BNG allocates an IPv4 address from one of the configured local address pools. If the BNG cannot allocate an IPv4 address, then an IPCP protocol reject is sent to the CPE.
   - If ADFv4 filters are present in the Access-Accept message, then they need to be reinstalled for that subscriber in the BNG.
   - If both IPv4 primary and secondary DNS addresses are present in the Access-Accept message, then both of them need to be updated for that subscriber in the BNG. If either an IPv4 primary DNS address or an IPv4 secondary DNS address is present in the Access-Accept message, then only the corresponding DNS address needs to be updated for that subscriber.

   If the BNG receives an Access-Reject message from the RADIUS server instead of an Access-Reject message, the following occurs:

   - If the Access-Reject message includes the Unisphere-Ipv4-release-control VSA and Reply Message attribute #18, the BNG sends an IPCP terminate request to the CPE. The CPE is then allowed to renegotiate IP NCP.

- If the either the Unisphere-Ipv4-release-control VSA or Reply Message attribute #18 are not included in the Access-Reject message, an LCP Protocol-Reject message is sent to the CPE. The CPE must renegotiate the LCP link before it is allowed to renegotiate IP NCP.

  If the RADIUS Access-Reject message includes the IPCP Terminate-Request field, the text of Reply Message attribute #18 is appended to the information in the Terminate-Request field, and will be shown in PPP data.

   If an Access-Challenge message is received instead of an Access-Accept, then the IPCP protocol reject is sent to the CPE.

   If there is no response from the RADIUS server, then IPCP is terminated.

5. The BNG sends an IPCP Configure NACK with the new IPv4 address option to the CPE.
6. The dynamic inet family and local address are added and all IPv4 (family inet) services for the dynamic client profile are instantiated.

   The BNG sends an IPCP Configure Request with a local IPv4 address option to the CPE.
7. The BNG sends an immediate Interim-Accounting message (if configured) with the Unisphere-Ipv4-release-control VSA (if configured) and a Framed-IP-Address attribute to the RADIUS server.
8. All IPv4 services, such as ascend data filters (ADF) and firewall filters, for the dynamic service profile and the lawful intercept service (if present for inet family) are instantiated and the Service Accounting-Start messages (if service accounting is configured and IPv4 service is not part of a multi-family service profile) are sent to the RADIUS server. If service instantiation fails, then IPCP is terminated and an IPv4 address release process is initiated.
9. The BNG receives an IPCP Configure Request with a new IPv4 address option from the CPE.
10. The BNG sends an IPCP Configure ACK to the CPE.
11. The BNG receives a Service Accounting-Start response from the RADIUS server.
12. The BNG receives an Interim-Accounting response from the RADIUS server.
13. The BNG receives an IPCP Configure ACK from the CPE.

IPv4 Address Release for Dynamic PPP Subscribers

The process for IPv4 address release for dynamic inet family and address over static PPP interface is as follows:

1. The BNG receives an IPCP terminate request from the CPE.
2. The BNG sends an IPCP terminate ACK to the CPE.
3. The following actions occur:

- All IPv4 (family inet) services for the dynamic client profile are de-instantiated and the dynamic inet family and local address are removed.
- All IPv4 services, such as ascend data filters (ADF) and firewall filters, for a dynamic service profile and the lawful intercept service (if present for inet family) are de-instantiated. The Service Accounting-Stop messages (if service accounting is configured and IPv4 service is not part of a multi-family service profile) is sent to the RADIUS server.
- If an IPv4 address was allocated from a local address pool, then it is available.
- The IPv4 address entry is cleared from the subscriber record

4. The BNG sends an immediate Interim-Accounting message (if configured) with the Unisphere-Ipv4-release-control VSA (if configured) to the RADIUS server and the Framed-IP-Address attribute must not be included.

   User Session Statistics and service session statistics for multi-family service are retained for the entire PPP session and is not cleared when the IPv4 address is released.

5. The BNG receives an Interim-Accounting response from the RADIUS server.

   No action taken in the BNG whether or not it receives a response from the RAIDUS server.

Related Documentation

- Saving IPv4 Addresses for Dual-Stack PPP Subscribers on page 57
- How IPv4 Address Negotiation and Release for Static PPP Subscribers Works in a Subscriber Access Network on page 58

How Framed-IP-Address and Framed-Pool Attributes Work for IPv4 PPP Subscribers

If a Framed-IP-Address attribute is returned from the RADIUS server during authentication and on-demand IP address allocation is enabled, then the BNG does not go to the RADIUS server for address allocation on the first Internet Protocol Control Protocol (IPCP) negotiation. It uses the Framed-IP-Address attribute returned in the initial Access-Accept message. Accounting-Start and periodic Interim-Accounting messages include the Framed-IP-Address attribute. Immediate Interim Accounting messages are not sent to RADIUS server. Address allocation is similar to the process described for a static or dynamic subscriber.

If a Framed-Pool attribute is returned from the RADIUS server during authentication and on-demand IP address allocation is enabled, then the border network gateway (BNG) does not go to the RADIUS server for address allocation upon first IPCP negotiation and it allocates an IPv4 address from the specified local address pool. Accounting-Start and periodic Interim-Accounting messages do not include the Framed-IP-Address attribute until IPCP negotiation. Immediate Interim Accounting messages (if configured) are sent to the RADIUS server. Address allocation is similar to the process described for a static or dynamic subscriber.

When neither the Framed-IP-Address attribute nor the Framed-Pool attribute is returned from the RADIUS server during authentication for IPv4-only PPP subscribers and on-demand IP address allocation is enabled, address allocation is similar to the process described for a static or dynamic subscriber. Because IPCP is the only Network Control Protocol (NCP) active for these subscribers, the entire PPP session is terminated upon an IPCP terminate request and an Accounting-stop message is sent to the RADIUS server. Immediate Interim-Accounting messages to release the IPv4 address are not sent in this case.

When a Framed-IP-Address is returned from the RADIUS server during authentication and the customer premises equipment (CPE) does not negotiate IPCP, the IPv4 address is not released whether or not the on-demand IP address allocation is enabled.

The on-demand configuration does not take effect when the destination (peer) IP address is statically configured in the inet family of the PPP interface.

Related Documentation

- Saving IPv4 Addresses for Dual-Stack PPP Subscribers on page 57

PART 5

Implementing IPv4 and IPv6 Dual Stack

CHAPTER 14

Best Practices for Configuring IPv4 and IPv6 Dual Stack in a PPPoE Access Network

Best Practice: Static PPPoE Interfaces with NDRA

When you use static PPPoE interfaces with NDRA, the prefix configured for router advertisement must match the source address specified under family inet6 in the logical pp0 interface configuration. If these values do not match, the prefix is not advertised correctly.

For example:

```
[edit protocols router-advertisement]
interface pp0.2004 {
  prefix 2040:2004::/64;
}
```

```
[edit interface pp0]
unit 2004 {
  family inet6 {
    address 2040:2004::1.1.1.1/64;
  }
}
```

To view the prefix in the ICMPv6 packet, use the **monitor traffic interface pp0.xxx extensive** command. If the prefix is missing, make sure that there is not a mismatch between the family inet6 address configured for the interface and the prefix configured for the interface in the router advertisement configuration.

Related Documentation

- Configuring a Static PPPoE Logical Interface for NDRA on page 80
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Best Practice: DHCPv6 Prefix Delegation over a PPPoE Access Network

When you use DHCPv6 prefix delegation over a PPPoE access network, you need to enable unnumbered addressing in the family inet6 configuration.

For dynamic PPPoE interfaces, enable unnumbered addressing in the dynamic profile. For example:

```
[edit dynamic-profiles]
PPPoE-dyn-ipv4v6-dhcp {
  interfaces {
    pp0 {
      unit "$junos-interface-unit" {
        ...
        family inet6 {
          unnumbered-address lo0.0;
        }
      }
    }
  }
}
```

For static PPPoE interfaces, enable unnumbered addressing in the interface configuration. For example:

```
[edit interface pp0]
unit 2004 {
  family inet6 {
  unnumbered-address lo0.0;
```

Related Documentation

- Configuring a PPPoE Dynamic Profile for Use with DHCP Addressing in a Dual-Stack Network on page 76
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Best Practice: IPv6 Addressing for Logical Interfaces in PPPoE Dynamic Profiles with NDRA

When you use NDRA, always set the IPv6 internet address in dynamic profiles to the **$junos-ipv6-address** predefined variable. This variable is replaced with the IPv6 address of the interface used for router advertisements.

```
[edit dynamic-profiles]
dyn-v4v6-ndra {
```



```
    interfaces {
      pp0 {
        unit "$junos-interface-unit" {
          family inet6 {
            address "$junos-ipv6-address ";
          }
        }
      }
    }
  }
```

Related Documentation

- Configuring a PPPoE Dynamic Profile for Use with NDRA in a Dual-Stack Network on page 78
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Best Practice: IPv6 Addressing for Logical Interfaces in PPPoE Dynamic Profiles with DHCPv6

The IPv6 address configuration for logical interfaces in PPPoE dynamic profiles when you are using DHCPv6 depends on whether or not you are using routing instances.

If you are using routing instances, use the **$junos-loopback-interface** predefined variable for the IPv6 address. For example:

```
[edit dynamic-profiles]
dyn-v4v6-ri {
  routing-instances {
    "$junos-routing-instance" {
      interface "$junos-interface-name";
    }
  }
  interfaces {
    pp0 {
      unit "$junos-interface-unit" {
        family inet6 {
          unnumbered-address "$junos-loopback-interface";
        }
      }
    }
  }
}
```

If you are not using routing instances, use the unnumbered address for the IPv6 address. The unnumbered address enables the local address to be derived from the specified interface and allows IP processing on the interface without assigning an explicit IP address to the interface. For example:

```
[edit dynamic-profiles]
dyn-v4v6-ndra {
  interfaces {
    pp0 {
      unit "$junos-interface-unit" {
```

```
                pppoe-options {
                    underlying-interface "$junos-underlying-interface";
                    server;
                }
                family inet6 {
                    unnumbered-address lo0.0;
                }
            }
        }
    }
}
```

Related Documentation

- Configuring a PPPoE Dynamic Profile for Use with DHCP Addressing in a Dual-Stack Network on page 76
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Best Practice: IPv4 Addressing for Logical Interfaces in PPPoE Dynamic Profiles

The IPv4 address configuration for logical interfaces in PPPoE dynamic profiles depends on whether or not you are using routing instances.

If you are using routing instances, use the **$junos-loopback-interface** variable for the IPv6 address.

```
[edit dynamic-profiles]
dyn-v4v6-ri {
    routing-instances {
        "$junos-routing-instance" {
            interface "$junos-interface-name";
        }
    }
    interfaces {
        pp0 {
            unit "$junos-interface-unit" {
                family inet {
                    unnumbered-address "$junos-loopback-interface";
                }
            }
        }
    }
}
```

If you are not using routing instances, use the unnumbered address for the IPv6 address. The unnumbered address enables the local address to be derived from the specified interface and allows IP processing on the interface without assigning an explicit IP address to the interface.

```
[edit dynamic-profiles]
dyn-v4v6-ndra {
    interfaces {
        pp0 {
            unit "$junos-interface-unit" {
```



```
            pppoe-options {
              underlying-interface "$junos-underlying-interface";
              server;
            }
            family inet {
              unnumbered-address lo0.0;
            }
          }
        }
      }
    }
```

Related Documentation

- Configuring a PPPoE Dynamic Profile for Use with DHCP Addressing in a Dual-Stack Network on page 76
- Configuring a PPPoE Dynamic Profile for Use with NDRA in a Dual-Stack Network on page 78
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Best Practice: Configuring Authentication for DHCP Subscribers on a PPPoE Access Network

In most cases PPPoE is used to authenticate subscribers in a PPPoE access network. However, if you wish to use DHCP to perform the authentication, do not configure subscriber authentication at the **[edit system services dhcp-local-server]** or the **[edit system services dhcp-local-server dhcpv6]** hierarchy levels. Instead configure subscriber authentication at the **[edit system services dhcp-local-server dhcpv6 group]** hierarchy level. For example:

```
[edit system services dhcp-local-server dhcpv6]
group v6-dhcp-client {
  authentication {
    password joshua;
    username-include {
      user-prefix StaticUser;
    }
  }
}
```

Related Documentation

- Configuring a DHCPv6 Local Server for DHCPv6 over PPPoE on page 75
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

CHAPTER 15

Configuration Tasks for IPv4 and IPv6 Dual Stack

Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks

Table 5 on page 74 describes configuration tasks that are specific to IPv4 and IPv6 dual-stack networks. It does not represent a complete router configuration.

Table 5: Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks

Purpose of Task	Procedure
Create a loopback interface for use in the subscriber access network.	"Configuring a Loopback Interface" on page 75
Configure DHCPv6 over the PPPoE IPv6 family.	"Configuring a DHCPv6 Local Server for DHCPv6 over PPPoE" on page 75
For PPPoE access networks that use DHCP addressing, create a dynamic profile that allows IPv4 and IPv6 subscribers to access the network on the same logical interface.	"Configuring a PPPoE Dynamic Profile for Use with DHCP Addressing in a Dual-Stack Network" on page 76
For PPPoE access networks that use NDRA addressing, configure a dynamic profile that allows IPv4 and IPv6 subscribers to access the network on the same logical interface.	"Configuring a PPPoE Dynamic Profile for Use with NDRA in a Dual-Stack Network" on page 78
For static NDRA configurations, create a static PPPoE logical interface.	"Configuring a Static PPPoE Logical Interface for NDRA" on page 80
Create a pool of IPv6 prefixes that are used in router advertisements.	"Configuring an Address-Assignment Pool Used for Router Advertisements" on page 81
Enable duplicate prefix protection for IPv6 prefixes used in router advertisements.	"Configuring Duplicate Prefix Protection for Router Advertisement" on page 82
Create a pool of IPv6 prefixes for use by DHCPv6 prefix delegation.	"Configuring an Address-Assignment Pool for Use by DHCPv6 Prefix Delegation" on page 83
Create a pool of global IPv6 addresses for use by DHCPv6 IA_NA.	"Configuring an Address-Assignment Pool for Use by DHCPv6 IA_NA" on page 84
Specify a specific address assignment pool to be used by DHCPv6 prefix delegation.	"Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation" on page 84
Save IPv4 addresses for dual-stack PPP Subscribers	"Configuration Tasks IPv4 Addresses Saved for Dual-Stack PPP Subscribers" on page 85
Configure AAA to exclude specific attributes from Acct-Start or Acct-Stop messages.	"Suppressing Accounting Information That Comes from AAA" on page 87
Reject IPv6CP negotiation when authorized IPv6 addresses are unavailable.	"Avoiding Negotiation of IPv6CP in the Absence of an Authorized Address" on page 88

Configuring a Loopback Interface

You must configure a loopback interface for use in the subscriber access network. The loopback interface is automatically used for unnumbered interfaces.

If you are using routing instances, you can configure the loopback interface for the default routing instance or for a specific routing instance. The following procedure adds the loopback interface to the default routing instance.

To configure a loopback interface:

1. Create the loopback interface, and assign a unit number to the interface.

   ```
   [edit]
   user@host# edit interfaces lo0 unit 0
   ```

2. Configure the interface for IPv4.

   ```
   [edit interfaces lo0 unit 0]
   user@host# set family inet unnumbered-address
   ```

3. Configure the interface for IPv6.

   ```
   [edit interfaces lo0 unit 0]
   user@host# set family inet6 unnumbered-address
   ```

Related Documentation

- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Configuration Tasks for a PPPoE Access Network in Which DHCP Is Used

- Configuring a DHCPv6 Local Server for DHCPv6 over PPPoE on page 75
- Configuring a PPPoE Dynamic Profile for Use with DHCP Addressing in a Dual-Stack Network on page 76

Configuring a DHCPv6 Local Server for DHCPv6 over PPPoE

To layer DHCPv6 above the PPPoE IPv6 family (inet6), create a DHCPv6 local server and associate DHCPv6 with the PPPoE interfaces by adding the PPPoE interfaces to the DHCPv6 local server configuration. Specify static and dynamic PPPoE interfaces as follows:

- Dynamic—Use the pp0.0 (PPPoE) logical interface as a wildcard to indicate that a DHCPv6 binding can be made on top of a PPPoE interface.
- Static—Use unit numbers to explicitly specify static interfaces; for example, pp0.2000.

To configure a DHCPv6 local server:

1. Access the DHCPv6 local server configuration.

   ```
   [edit]
   user@host# edit system services dhcp-local-server dhcpv6
   [edit system services dhcp-local-server dhcpv6]
   ```

2. Create a group for dynamic PPPoE interfaces and assign a name.

   The group feature groups a set of interfaces and then applies a common DHCP configuration to the named interface group.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# edit group group-pppoe
   ```

3. For dynamic PPPoE logical interfaces, add an interface.

   ```
   [edit system services dhcp-local-server dhcpv6 group group-pppoe]
   user@host# set interface pp0.0
   ```

4. For static PPPoE, add a range of interfaces.

   ```
   [edit system services dhcp-local-server dhcpv6 group group-pppoe]
   user@host# set interface pp0.2000 upto pp0.2999
   ```

Configuring a PPPoE Dynamic Profile for Use with DHCP Addressing in a Dual-Stack Network

Configure a dynamic profile for IPv4 and IPv6 subscribers that access the network. The dynamic profile defines the attributes of the dynamic PPPoE logical subscriber interface.

To configure a PPPoE dynamic profile for both IPv4 and IPv6 subscribers:

1. Create and name the dynamic profile.

   ```
   [edit]
   user@host# edit dynamic profiles PPPOE-dyn-ipv4v6
   ```

2. If you are using routing instances, add a routing instance to the profile, and add an interface to the routing instance.

   - Specify the **$junos-routing-instance** variable for the routing instance. The routing instance variable is dynamically replaced with the routing instance the accessing subscriber uses when connecting to the BNG.
   - Specify the **$junos-interface-name** variable for the interface. The interface variable is dynamically replaced with the interface that the accessing subscriber uses when connecting to the BNG.

   ```
   [edit dynamic profiles PPPOE-dyn-ipv4v6]
   user@host# set routing-instances $junos-routing-instance interface
     $junos-interface-name
   ```

3. Add a PPPoE logical interface (pp0) to the profile, and specify **$junos-interface-unit** as the predefined variable to represent the logical unit number for the interface. The variable is dynamically replaced with the actual unit number supplied by the network when the subscriber logs in.

   ```
   [edit dynamic profiles PPPOE-dyn-ipv4v6]
   user@host# edit interfaces pp0 unit $junos-interface-unit
   ```

4. Configure the IPv4 family for the pp0 interface as follows:

   - If you are not using routing instances, assign an unnumbered address. The unnumbered address enables the local address to be derived from the specified interface and allows IP processing on the interface without an explicit IP address assigned to the interface.

For example:

```
[edit dynamic-profiles PPPOE-dyn-ipv4v6 interfaces pp0 unit "$junos-interface-unit"]
user@host# set family inet unnumbered-address lo0.0
```

- If you are using routing instances, assign the predefined variable **$junos-loopback-interface**.

  For example:

  ```
  [edit dynamic-profiles PPPOE-dyn-ipv4v6 interfaces pp0 unit "$junos-interface-unit"]
  user@host# set family inet unnumbered-address $junos-loopback-interface
  ```

5. Configure the IPv6 family for the pp0 interface as follows:

   - If you are not using routing instances, assign an unnumbered address that specifies the loopback interface. The unnumbered address enables the local address to be derived from the loopback interface and allows IP processing on the interface without an explicit IP address assigned to the interface.

     For example:

     ```
     [edit dynamic-profiles PPPOE-dyn-ipv4v6 interfaces pp0 unit "$junos-interface-unit"]
     user@host# set family inet6 unnumbered-address lo0.0
     ```

   - If you are using routing instances, assign the predefined variable **$junos-loopback-interface**.

     For example:

     ```
     [edit dynamic-profiles PPPOE-dyn-ipv4v6 interfaces pp0 unit "$junos-interface-unit"]
     user@host# set family inet6 unnumbered-address $junos-loopback-interface
     ```

6. Specify **$junos-underlying-interface** as the predefined variable to represent the name of the underlying Ethernet interface on which the router creates the dynamic PPPoE logical interface. The variable is dynamically replaced with the actual name of the underlying interface.

   ```
   [edit dynamic-profiles PPPOE-dyn-ipv4v6 interfaces pp0 unit "$junos-interface-unit"]
   user@host# set pppoe-options underlying-interface $junos-underlying-interface
   ```

7. Define the router to act as a PPPoE server when a PPPoE logical interface is dynamically created.

   ```
   [edit dynamic-profiles PPPOE-dyn-ipv4v6 interfaces pp0 unit "$junos-interface-unit"]
   user@host# set pppoe-options server
   ```

8. (Optional) Configure the PPP authentication protocol for the pp0 interface. Specify either **chap** or **pap** (or both).

   ```
   [edit dynamic-profiles PPPOE-dyn-ipv4v6 interfaces pp0 unit "$junos-interface-unit"]
   user@host# set ppp-options chap
   user@host# set ppp-options pap
   ```

9. (Optional) Enable keepalives and set an interval for keepalives. We recommend an interval of 30 seconds. For example:

   ```
   [edit dynamic-profiles PPPOE-dyn-ipv4v6 interfaces pp0 unit "$junos-interface-unit"]
   ```

user@host# **set keepalives interval 30**

Related Documentation

- IPv4 and IPv6 Dual Stack in a PPPoE Access Network on page 47
- Best Practice: Configuring Authentication for DHCP Subscribers on a PPPoE Access Network on page 72
- Best Practice: IPv6 Addressing for Logical Interfaces in PPPoE Dynamic Profiles with DHCPv6 on page 69
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74
- Best Practice: IPv6 Addressing for Logical Interfaces in PPPoE Dynamic Profiles with DHCPv6 on page 69

Configuration Tasks for PPPoE Access Networks in Which NDRA Is Used

Configuring a PPPoE Dynamic Profile for Use with NDRA in a Dual-Stack Network

Configure a dynamic profile for IPv4 and IPv6 PPPoE subscribers that access the network. The dynamic profile defines the attributes of the dynamic PPPoE logical subscriber interface.

This dynamic profile is for configurations that use NDRA to assign a global IP address to the CPE WAN link.

To configure a PPPoE dynamic profile for NDRA:

1. Create and name the dynamic profile.

   [edit]
   user@host# **edit dynamic profiles PPPOE-dyn-ipv4v6-ndra**

2. If you are using routing instances, add a routing instance to the profile and add an interface to the routing instance.

   - Specify the **$junos-routing-instance** variable for the routing instance. The routing instance variable is dynamically replaced with the routing instance the accessing subscriber uses when connecting to the BNG.
   - Specify the **$junos-interface-name** variable for the interface. The interface variable is dynamically replaced with the interface that the accessing subscriber uses when connecting to the BNG.

   [edit dynamic profiles PPPOE-dyn-ipv4v6-ndra]

```
user@host# set routing-instances $junos-routing-instance interface
  $junos-interface-name
```

3. Add a PPPoE logical interface (pp0) to the profile, and specify **$junos-interface-unit** as the predefined variable to represent the logical unit number for the interface. The variable is dynamically replaced with the actual unit number supplied by the network when the subscriber logs in.

```
[edit dynamic profiles PPPOE-dyn-ipv4v6-ndra]
user@host# edit interfaces pp0 unit $junos-interface-unit
```

4. Configure the IPv4 family for the pp0 interface as follows:

   - If you are not using routing instances, assign an unnumbered address. The unnumbered address enables the local address to be derived from the specified interface and allows IP processing on the interface without assigning an explicit IP address to the interface.

     For example:

     ```
     [edit dynamic-profiles PPPOE-dyn-ipv4v6-ndra interfaces pp0 unit
       "$junos-interface-unit"]
     user@host# set family inet unnumbered-address lo0.0
     ```

   - If you are using routing instances, assign the predefined variable **$junos-loopback-interface**.

     For example:

     ```
     [edit dynamic-profiles PPPOE-dyn-ipv4v6-ndra interfaces pp0 unit
       "$junos-interface-unit"]
     user@host# set family inet unnumbered-address $junos-loopback-interface
     ```

5. Configure the IPv6 family for the pp0 interface, and assign **$junos-ipv6-address** as the predefined variable. Use this variable when you are using router advertisement with or without routing instances. This variable is replaced with the IPv6 address of the interface used for router advertisements.

```
[edit dynamic profiles PPPOE-dyn-ipv4v6-ndra interfaces pp0 unit
  "$junos-interface-unit"]
user@host# set family inet6 address $junos-ipv6-address
```

6. Specify **$junos-underlying-interface** as the predefined variable to represent the name of the underlying Ethernet interface on which the router creates the dynamic PPPoE logical interface. The variable is dynamically replaced with the actual name of the underlying interface.

```
[edit dynamic profiles PPPOE-dyn-ipv4v6-ndra pp0 interfaces pp0 unit
  "$junos-interface-unit"]
user@host# set pppoe-options underlying-interface $junos-underlying-interface
```

7. Define the router to act as a PPPoE server when a PPPoE logical interface is dynamically created.

```
[edit dynamic profiles PPPOE-dyn-ipv4v6-ndra interfaces pp0 unit
  "$junos-interface-unit"]
user@host# set pppoe-options server
```

8. (Optional) Configure the PPP authentication protocol that is used to identify and authenticate the CPE. Specify either **chap** or **pap** (or both).

   [edit dynamic-profiles PPPOE-dyn-ipv4v6-ndra interfaces pp0 unit "$junos-interface-unit"]
   user@host# **set ppp-options chap**
   user@host# **set ppp-options pap**

9. (Optional) Enable keepalives and set an interval for keepalives. We recommend an interval of 30 seconds. For example:

   [edit dynamic-profiles PPPOE-dyn-ipv4v6-ndra interfaces pp0 unit "$junos-interface-unit"]
   user@host# **set keepalives interval 30**

10. Configure the router advertisement protocol.

    a. Access the router advertisement configuration.

       [edit dynamic-profiles PPPOE-dyn-ipv4v6-ndra]
       user@host# **edit protocols router-advertisement**

    b. Specify the interface on which the NDRA configuration is applied. Assign **$junos-interface-name** as the predefined variable. The variable is replaced with the actual name of the interface.

       [edit dynamic-profiles PPPOE-dyn-ipv4v6-ndra protocols router-advertisement]
       user@host# **edit interface $junos-interface-name**

    c. Specify a prefix value contained in router advertisement messages sent to the CPE on interfaces created with this dynamic profile.

       If you specify the $junos-ipv6-ndra-prefix predefined variable, the actual value is obtained from a local pool or through AAA.

       [edit dynamic-profiles PPPOE-dyn-ipv4v6-ndra protocols router-advertisement]
       user@host# **set prefix $junos-ipv6-ndra-prefix**

Configuring a Static PPPoE Logical Interface for NDRA

To configure a static PPPoE logical interface for static NDRA configurations:

1. Specify the name and logical unit number of the interface.

   [edit]
   user@host# **edit interfaces pp0 unit 1000**

2. Configure a description for the interface.

   [edit interfaces pp0 unit 1000]
   user@host# **set description "static IPv4v6 dual stack, NDRA"**

3. Specify the family inet6 source address.

   [edit interfaces pp0 unit 1000]
   user@host# **set family inet6 address 2040:2004::1.1.1.1/64**

4. Configure an unnumbered address for family inet.

   [edit interfaces pp0 unit 1000]

user@host# **set family inet unnumbered-address lo0.0**

5. Specify the underlying Ethernet interface.

   [edit interfaces pp0 unit 1000]
   user@host# **set pppoe-options underlying-interface ge-1/0/0.1000**

6. Define the router to act as a PPPoE server when the PPPoE logical interface is created.

   [edit interfaces pp0 unit 1000]
   user@host# **set pppoe-options server**

7. Access the router advertisement configuration, and specify the prefixes that the BNG sends in router advertisements for the static interface. Make sure that the prefixes match the source address configured for the static PPPoE logical interface configured in Step 3.

   [edit]
   user@host# **edit protocols router-advertisement**
   user@host# **set interface pp0.1000 prefix 2040:2004::/64**

Configuring an Address-Assignment Pool Used for Router Advertisements

If you are using local address-assignment pools to be used for router advertisement, create a pool and add IPv6 prefixes to the pool.

You must configure separate pools for DHCPv6 prefix delegation, DHCPv6 IA_NA, and router advertisement.

To configure an NDRA address-assignment pool.

1. Create a pool for IPv6 prefixes used by NDRA.

   [edit]
   user@host# **edit access address-assignment pool ndra-2010 family inet6**

2. Add IPv6 network prefixes to the pool.

   [edit access address-assignment pool ndra-2010 family inet6]
   user@host# **set prefix 2001::/64**

3. Configure the name of the IPv6 address range and define the range. For NDRA pools, specify the range by setting a prefix length of 64.

   [edit access address-assignment pool ndra-2010 family inet6]
   user@host# **set range ndra-range prefix-length 64**

4. Specify that the address-assignment pool is used for NDRA.

   [edit access address-assignment]
   user@host# **set neighbor-discovery-router-advertisement ndra-2010**

Configuring Duplicate Prefix Protection for Router Advertisement

If you are using AAA to supply IPv6 prefixes for router advertisement, you can enable duplicate prefix protection to prevent prefixes from being used more than once. If enabled, the following attributes received from external servers are checked:

- *Framed-IPv6-Prefix*
- *Framed-IPv6-Pool*

If a prefix overlaps with a prefix in an address pool, the prefix is taken from the pool if it is available. If the prefix is already in use, it is rejected as unavailable. If the prefix length requested from the external server does not match the pool's prefix length exactly, the authentication request is denied. If configured, the Acct-Stop message will include a termination cause.

To configure duplicate prefix protection:

1. Enter the **access** configuration.

   [edit]
   user@host# **edit access**

2. Enable duplicate prefix protection.

   [edit access]
   user@host# **address-protection**

Configuring a DNS Server Address for IPv6 Hosts

To configure a dynamic DNS server address for IPv6 hosts:

1. Specify that the router receives the DNS server address in the $junos-ipv6-dns-server-address variable sent from RADIUS servers in the Access-Accept message when the subscriber logs in.

   [edit dynamic-profiles *dynamic-profile-name* protocols router-advertisement interface *interface-name*]
   user@host# **set dns-server-address $junos-ipv6-dns-server-address**

2. Specify the time in seconds for which the DNS server address remains valid.

   [edit dynamic-profiles *dynamic-profile-name* protocols router-advertisement interface *interface-name* dns-server-address *address*]
   user@host# **set lifetime 2400**

   The default value of the lifetime is 1800 seconds.

To configure a static DNS server address for IPv6 hosts:

1. Specify the IPv6 address of the DNS server.

   [edit dynamic-profiles *dynamic-profile-name* protocols router-advertisement interface *interface-name*]
   user@host# **set dns-server-address** ***ipv6-address***

2. Specify the time in seconds for which the DNS server address remains valid.

```
[edit dynamic-profiles dynamic-profile-name protocols router-advertisement interface
   interface-name dns-server-address  address]
user@host# set lifetime 2400
```

The default value of the lifetime is 1800 seconds.

Related Documentation

- Best Practice: IPv6 Addressing for Logical Interfaces in PPPoE Dynamic Profiles with NDRA on page 68
- Best Practice: Static PPPoE Interfaces with NDRA on page 67
- IPv4 and IPv6 Dual Stack in a PPPoE Access Network on page 47
- How NDRA Works in a Subscriber Access Network on page 16
- Methods for Obtaining IPv6 Prefixes for NDRA on page 17
- Duplicate Prefix Protection for NDRA on page 18
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Configuration Tasks for DHCP Address Assignment Pools

Configuring an Address-Assignment Pool for Use by DHCPv6 Prefix Delegation

This procedure shows how to configure IPv6 local address pools to allocate IPv6 prefixes for use by DHCPv6 prefix delegation.

You must configure separate pools for DHCPv6 prefix delegation, DHCPv6 IA_NA, and NDRA.

To configure the pool to be used for prefix delegation:

1. Create a pool and assign a name to it.

   ```
   [edit access]
   user@host# edit address-assignment pool v6-prefix-pool-2001
   ```

2. Under family inet6, add IPv6 prefixes to the pool.

   ```
   [edit access address-assignment pool v6-prefix-pool-2001]
   user@host# edit family inet6
   user@host# set prefix 2001:0000:0000:0000::/64
   ```

3. Configure the name of the IPv6 prefix range, and define the range by setting a prefix length of 64.

   ```
   [edit access address-assignment pool v6-prefix-pool-2001 family inet6]
   user@host# edit range prefix-range
   ```

```
user@host# set prefix-length 64
```

Configuring an Address-Assignment Pool for Use by DHCPv6 IA_NA

This procedure shows how to configure IPv6 local address pools to allocate global IPv6 addresses to the CPE WAN link.

You must configure separate pools for DHCPv6 prefix delegation, DHCPv6 IA_NA, and NDRA.

To configure the pool to be used for DHCPv6 IA_NA:

1. Create a pool and assign a name to it.

   ```
   [edit access]
   user@host# edit address-assignment pool v6-ia-na-pool
   ```

2. Under family inet6, add IPv6 network prefixes to the pool.

   ```
   [edit access address-assignment pool v6-ia-na-pool]
   user@host# edit family inet6
   user@host# set prefix 2001:0000::/64
   ```

3. Configure the name of the IPv6 address range, and define the range by setting a low and high range of /128 addresses.

   ```
   [edit access address-assignment pool v6-ia-na-pool family inet6]
   user@host# edit range v6-range
   user@host# set low 2001::1/128
   user@host# set high 2001::ffff:ffff/128
   ```

Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation

You can explicitly specify which address pool the BNG uses to assign IPv6 prefixes for use by DHCPv6 prefix delegation. This feature enables you to identify the address pool without using RADIUS or a network match.

NOTE: You can also use by Juniper Networks VSA 26-161 to specify the delegated address pool. The VSA-specified value takes precedence over the **delegated-address** statement.

To specify the pool to be used for prefix delegation:

1. Specify that you want to configure override options for DHCPv6 local server.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# edit overrides
   ```

2. Specify the name of the delegated address pool.

   ```
   [edit system services dhcp-local-server overrides]
   user@host# set delegated-pool paris-cable-12
   ```

Related Documentation

- Overview of Using DHCPv6 Prefix Delegation on page 23
- Overview of Using DHCPv6 IA_NA to Provide IPv6 WAN Link Addressing on page 21
- Methods for Obtaining IPv6 Prefixes for DHCPv6 Prefix Delegation on page 26
- Methods for Obtaining IPv6 Global Addresses for DHCPv6 IA_NA on page 21
- Configuring an Address-Assignment Pool for Use by DHCPv6 Prefix Delegation on page 83
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Configuration Tasks IPv4 Addresses Saved for Dual-Stack PPP Subscribers

Configuring Static On-Demand IPv4 Address Allocation for Dual-Stack PPP Subscribers

To configure static on-demand IPv4 address allocation for dual-stack PPP subscribers:

1. Specify the name and logical unit number of the interface.

   ```
   [edit]
   user@host# edit interfaces pp0 unit 1000
   ```

2. Enable on-demand IP address allocation.

   ```
   [edit interfaces pp0 unit 1000]
   user@host# set ppp-options on-demand-ip-address
   ```

Configuring Dynamic On-Demand IPv4 Address Allocation for Dual-Stack PPP Subscribers

To configure dynamic on-demand IP address IPv4 address allocation for dual-stack PPP subscribers:

1. Create and name the dynamic profile.

   ```
   [edit]
   user@host# edit dynamic profiles ppp-dyn-ipv4
   ```

2. Specify the name and logical unit number of the interface.

   ```
   [edit]
   user@host# edit interfaces ppp unit 1000
   ```

3. Enable on-demand IP address allocation.


```
[edit interfaces pp0 unit 1000]
user@host# set ppp-options on-demand-ip-address
```

Configuring System Level On-Demand IPv4 Address Allocation for Dual-Stack PPP Subscribers

To configure static on-demand IP address IPv4 address allocation for dual-stack PPP subscribers at the system level:

1. Specify the protocol.

   ```
   [edit]
   user@host# edit protocols
   ```

2. Specify the ppp-service option.

   ```
   [edit protocols]
   user@host# edit ppp-service
   ```

3. Enable on-demand IP address allocation.

   ```
   [edit protocols ppp-service]
   user@host# set on-demand-ip-address
   ```

Enabling Immediate Interim Accounting Messages

To enable an immediate interim accounting message:

1. Create a profile and assign a name to it.

   ```
   [edit access]
   user@host# edit profile profile1
   ```

2. Under accounting, specify the address-change-immediate-update option.

   ```
   [edit access profile profile1]
   user@host# edit accounting
   user@host# set address-change-immediate-update
   ```

Enabling Unisphere IPv4 Release Control VSA in RADIUS Messages

This procedure shows how to enable the Unisphere IPv4 release control VSA in RADIUS messages:

To configure a RADIUS message:

1. Create a profile and assign a name to it.

   ```
   [edit access]
   user@host# edit profile profile1
   ```

2. Specify that you want to configure RADIUS.

   ```
   [edit access profile profile1]
   user@host# edit radius
   ```

3. (Optional) Configure the message RADIUS message.

   ```
   user@host# set ip-address-change-notify message
   ```

Related Documentation

- *address-change-immediate-update*
- *ip-address-change-notify*
- *on-demand-ip-address*
- Saving IPv4 Addresses for Dual-Stack PPP Subscribers on page 57

Suppressing Accounting Information That Comes from AAA

The following standard and vendor-specific IPv6 RADIUS attributes are included by default (when available) in Acct-Start and Acct-Stop messages:

- Framed-IPv6-Prefix
- Framed-IPv6-Pool
- Delegated-Ipv6-Prefix
- Framed-IPv4-Route
- Framed-IPv6-Route

You can configure the software to exclude these attributes from Acct-Start or Acct-Stop messages. To do so, configure the access profile:

1. Access the access profile.

   [edit]
   user@host# **edit access profile dual-stack radius attributes**

2. The following examples show how to use the **exclude** statement to exclude attributes from messages.

   [edit access profile dual-stack radius attributes]
   user@host# **set exclude delegated-ipv6-prefix accounting-start**

   [edit access profile dual-stack radius attributes]
   user@host# **set exclude framed-ipv6-pool [accounting-start accounting-stop]**

   [edit access profile dual-stack radius attributes]
   user@host# **set exclude framed-ipv6-prefix accounting-start framed-ipv6-route accounting-start**

   [edit access profile dual-stack radius attributes]
   user@host# **set exclude framed-ipv6-prefix accounting-start framed-ipv6-route accounting-start**

Related Documentation

- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

Avoiding Negotiation of IPv6CP in the Absence of an Authorized Address

You can control the behavior of the router in a situation where IPv6CP negotiation is initiated for subscriber sessions when no authorized addresses are available.

By default, IPv6CP negotiation is enabled to proceed for an IPv6-only session when AAA has not provided an appropriate IPv6 address or prefix. In the absence of the address, the negotiation cannot successfully complete. To prevent endless client negotiation of IPv6CP, include the **reject-unauthorized-ipv6cp** statement at the **[edit protocols ppp-service]** hierarchy level, which enables the jpppd process to reject the negotiation attempt.

To configure the router to reject IPv6CP negotiation messages when no IPv6 address is available for a dynamic interface:

- Enable rejection of unauthorized IPv6CP negotiation messages.

  ```
  [edit protocols ppp-service]
  user@host# set reject-unauthorized-ipv6cp
  ```

NOTE: The **reject-unauthorized-ipv6cp** statement does not prevent IPv6CP negotiation for static interfaces, because the jpppd process cannot determine whether router advertisement of DHCPv6 is configured to run above the PPP interface.

Related Documentation

- IPv4 and IPv6 Dual Stack in a PPPoE Access Network on page 47

CHAPTER 16

Monitoring and Managing IPv6 Subscribers

Monitoring Active Subscriber Sessions

Purpose View a summary of active subscriber sessions.

Action From operational mode, enter the **show subscribers summary** command.

```
user@host>show subscribers summary
Subscribers by State
   Active: 2
   Total: 2

Subscribers by Client Type
   DHCP: 1
   PPPoE: 1
   Total: 2
```

Meaning The output under **Subscribers by State** shows the number of active subscriber sessions.

The output under **Subscribers by Client Type** shows the number of active sessions by type. The two subscriber sessions above represent a DHCPv6 subscriber on a PPPoE access network. When DHCPv6 is layered over PPPoE, two separate subscriber sessions are created for a subscriber.

Related Documentation

- *show subscribers summary*

Monitoring Both IPv4 and IPv6 Address in Correct Routing Instance

Purpose Verify that the subscriber has both an IPv4 and an IPv6 address and is placed in the correct routing-instance.

Action From operational mode, enter the **show subscribers** command.

```
user@host>show subscribers
Interface         IP Address/VLAN ID    User Name            LS:RI
pp0.1073741825    10.16.0.2             ipv4-v6-subscriber   default:default
pp0.1073741825    2001:DB8::1                                default:default
```

Meaning The **Interface** field shows that there are two subscriber sessions running on the same interface. The **IP Address** field shows that one session is assigned an IPv4 address, and one session is assigned on IPv6 address.

The **LS:RI** field shows that the subscriber is placed in the correct routing instance and that traffic can be sent and received.

Related Documentation

- *show subscribers*

Monitoring Dynamic Subscriber Sessions

Purpose Display dynamic PPPoE and DHCPv6 subscriber sessions.

Action From operational mode, enter the **show subscribers detail** command.

```
user@host>show subscribers detail
Type: PPPoE
User Name: SBRSTATICUSER
IP Address: 10.16.0.2
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: pppoe-subscriber-profile
MAC Address: 00:01:02:00:00:01
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-12-08 09:11:41 PST

Type: DHCP
IPv6 Address: 2001::1
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:01:02:00:00:01
State: Active
Radius Accounting ID: 3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-12-08 09:12:11 PST
```

```
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 01 02 00 00 01
00 06 00 02 00 03 00 03 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

Meaning If you are using DHCPv6 over a PPPoE access network, the output shows the relationship of the DHCPv6 subscriber session with its underlying PPPoE subscriber session. In the output for the PPPoE session, the **Session ID** is 2. The output of the DHCP session shows that the **Underlying Session ID** is 2.

Related Documentation

- *show subscribers*

Monitoring Address Pools Used for Subscribers

Purpose Verify the pool used for NDRA, the delegated address pool used for DHCPv6 prefix delegation, and the length of the IPv6 prefixes that were delegated to the CPE.

Action From operational mode, enter the **show subscribers extensive** command.

```
user@host>show subscribers extensive
Type: PPPoE
User Name: dual-stack-v4v6-pd
IP Address: 2.2.0.5
IP Netmask: 255.255.0.0
IPv6 User Prefix: 2010:0:0:8::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073741864
Interface type: Dynamic
Dynamic Profile Name: DS-dyn-ipv4v6-ra
MAC Address: 00:07:64:11:07:02
State: Active
Radius Accounting ID: 87
Session ID: 87
Login Time: 2012-01-17 14:45:30 PST
IPv6 Delegated Address Pool: dhcpv6-pd-pool
IPv6 Delegated Address Pool: ndra-2010
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2010:0:0:8::1/64

Type: DHCP
IPv6 Prefix: 2040:2000:2000:5::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073741864
Interface type: Static
MAC Address: 00:07:64:11:07:02
State: Active
Radius Accounting ID: 88
Session ID: 88
Underlying Session ID: 87
Login Time: 2012-01-17 14:46:00 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 07 64 11 07 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Address Pool: dhcpv6-pd-pool
```

IPv6 Delegated Network Prefix Length: 64
IPv6 Delegated Network Prefix Length: 48

Meaning Under the PPPoE session, the **IPv6 Delegated Address Pool** fields show the names of the pools used for DHCPv6 prefix delegation and for NDRA prefixes. The **IPv6 Delegated Network Prefix Length** field shows the length of the prefix used to assign the IPv6 address for this subscriber session. The **IPv6 Interface Address** field shows the IPv6 address assigned to the CPE interface from the NDRA pool.

Under the DHCP session, the **IPv6 Delegated Address Pool** fields show the name of the pool used for DHCPv6 prefix delegation. The **IPv6 Delegated Network Prefix Length** fields shows the length of the prefix used in DHCPv6 prefix delegation.

Related Documentation

- *show subscribers*

Monitoring Specific Subscriber Sessions

Purpose Display information about specific subscriber sessions. If you have many subscriber sessions running, you can use this command to display specific sessions.

Action From operational mode, enter the **show subscribers extensive id** command.

```
user@host>show subscribers extensive id 2
Type: PPPoE
User Name: SBRSTATICUSER
IP Address: 10.16.0.2
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: pppoe-subscriber-profile
MAC Address: 00:01:02:00:00:01
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-12-08 09:11:41 PST

user@host> show subscribers extensive id 3
Type: DHCP
IPv6 Address: 2001::1
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:01:02:00:00:01
State: Active
Radius Accounting ID: 3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-12-08 09:12:11 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 01 02 00 00 01
00 06 00 02 00 03 00 03 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```


Meaning The output shows details about specific subscriber sessions.

Related Documentation
- *show subscribers*

Monitoring the Status of the PPPoE Logical Interface

Purpose Display status information about the PPPoE logical interface.

Action

```
user@host> show interfaces pp0.1073741888
  Logical interface pp0.1073741888 (Index 123) (SNMP ifIndex 707)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
    PPPoE:
      State: SessionUp, Session ID: 16,
      Session AC name: centaurus, Remote MAC address: 00:00:64:01:06:02,
      Underlying interface: ge-1/0/0.1104 (Index 95)
    Input packets : 8
    Output packets: 51816
  LCP state: Opened
  NCP state: inet: Opened, inet6: Opened, iso: Not-configured, mpls:
  Not-configured
  CHAP state: Closed
  PAP state: Success
    Protocol inet, MTU: 1500
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Primary
        Local: 77.1.1.1
    Protocol inet6, MTU: 1500
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 2001:DB8:0:21::/64, Local: 2001:DB8:0:21::1
      Addresses, Flags: Is-Preferred
        Destination: fe80::/64, Local: fe80::2a0:a50f:fc61:6d0
```

Meaning Displays session information about the ppp0 interface.

Related Documentation
- *show interfaces (PPPoE)*

Monitoring Service Sessions for Subscribers

Purpose Display a details about dual-stack subscriber session.

Action

```
user@host> show subscribers interface pp0.1073741888 extensive
Type: PPPoE
User Name: dual-stack-v4v6-2svc-good
IP Address: 10.10.12.140
Logical System: default
Routing Instance: default
Interface: pp0.1073741888
Interface type: Dynamic
Dynamic Profile Name: DS-dyn-ipv4v6-ra
MAC Address: 00:00:64:01:06:02
State: Active
Radius Accounting ID: 155
Session ID: 155
Login Time: 2011-01-30 20:36:53 PST
Service Sessions: 2

  Service Session ID: 174
  Service Session Name: l3-v4-service
  State: Active
  IPv4 Input Filter Name: upstrm-filter-ge-1/0/0.1104-in
  IPv4 Output Filter Name: dwnstrm-filter-ge-1/0/0.1104-out

  Service Session ID: 175
  Service Session Name: l3-v6-service
  State: Active
  IPv6 Input Filter Name: v6-up-filter-ge-1/0/0.1104-in
  IPv6 Output Filter Name: v6-dn-filter-ge-1/0/0.1104-out
```

Meaning The highlighted output includes details about a subscriber's service sessions.

Related Documentation

- *show subscribers*

Monitoring PPP Options Negotiated with the Remote Peer

Purpose Display the PPP options that were negotiated with the CPE. You can also view the IPv4 address that was negotiated with the remote peer. This address matches the address returned from AAA. You can also see this address by using the **show subscribers** command.

Note that this is the only command that will provide the details about the negotiated interface IDs.

Action

```
user@host> show ppp interface pp0.1073741888 extensive
  Session pp0.1073741888, Type: PPP, Phase: Network
    LCP
      State: Opened
      Last started: 2011-01-30 20:36:53 PST
      Last completed: 2011-01-30 20:36:53 PST
      Negotiated options:
        Authentication protocol: pap, Magic number: 1174596353, MRU: 1492
    Authentication: PAP
      State: Grant
      Last started: 2011-01-30 20:36:53 PST
      Last completed: 2011-01-30 20:36:53 PST
    IPCP
      State: Opened
      Last started: 2011-01-30 20:36:54 PST
      Last completed: 2011-01-30 20:36:54 PST
      Negotiated options:
        Local address: 77.1.1.1, Remote address: 99.11.12.140
    IPV6CP
      State: Opened
      Last started: 2011-01-30 20:36:54 PST
      Last completed: 2011-01-30 20:36:54 PST
      Negotiated options:
        Local interface identifier: 2a0:a50f:fc61:6d0,
        Remote interface identifier: 200:64ff:fe01:602
```

Related Documentation

- *show ppp interface*

Monitoring the RADIUS Attribute Used for NDRA

Purpose Display the RADIUS attribute used for IPv6 NDRA.

Action To display the RADIUS attribute used for IPv6 Neighbor Discovery router advertisements:

```
host1#show aaa ipv6-nd-ra-prefix

IPv6 ND RA Prefix       : IPv6-NdRa-Prefix (Juniper VSA)
```

Related Documentation

- Configuration Tasks for PPPoE Access Networks in Which NDRA Is Used on page 78

Monitoring Address Bindings on the DHCPv6 Local Server

Purpose Display address bindings in the client table on the DHCPv6 local server.

Action To display address bindings in the client table on the DHCPv6 local server:

user@host>**show dhcpv6 server binding detail**

```
user@host> show dhcpv6 server binding detail
Session Id:  6
     Client IPv6 Prefix:                       2001:bd8:1111:2222::/64
     Client DUID:                            LL_TIME0x1-0x2e159c0-00:10:94:00:00:01

     State:
BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
     Lease Expires:                            2009-07-21 10:41:15 PDT
     Lease Expires in:                         86308 seconds
     Lease Start:                              2009-07-20 10:41:15 PDT
     Incoming Client Interface:                ge-1/0/0.0
     Server Ip Address:                        0.0.0.0
     Server Interface:                         none
     Client Id Length:                         14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0001

Session Id:  7
     Client IPv6 Prefix:                       2001:bd8:1111:2222::/64
     Client DUID:                            LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:
BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
     Lease Expires:                            2009-07-21 10:41:15 PDT
     Lease Expires in:                         86308 seconds
     Lease Start:                              2009-07-20 10:41:15 PDT
     Incoming Client Interface:                ge-1/0/0.0
     Server Ip Address:                        0.0.0.0
     Server Interface:                         none
     Client Id Length:                         14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

Related Documentation

- *show dhcpv6 server binding*

PART 6

Examples: IPv4 and IPv6 Dual-Stack Designs

CHAPTER 17

Example: Dual-Stack Design That Uses DHCPv6 IA_NA and DHCPv6 Prefix Delegation over PPPoE

Example: Configuring a Dual Stack That Uses DHCPv6 IA_NA and DHCPv6 Prefix Delegation over PPPoE

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Router
- Junos OS Release 11.4 or later

Overview

This design uses DHCPv6 IA_NA and DHCPv6 prefix delegation in your subscriber access network as follows:

- The access network is PPPoE.
- DHCPv6 IA_NA is used to assign a global IPv6 address on the WAN link. The address comes from a local pool that is specified using AAA RADIUS.
- DHCPv6 prefix delegation is used for subscriber LAN addressing. It uses a delegated prefix from a local pool that is specified by AAA RADIUS.
- DHCPv4 is used for subscriber LAN addressing.
- DHCPv6 subscriber sessions are layered over an underlying PPPoE subscriber session.

Topology

Figure 14: PPPoE Subscriber Access Network with DHCPv6 IA_NA and DHCPv6 Prefix Delegation

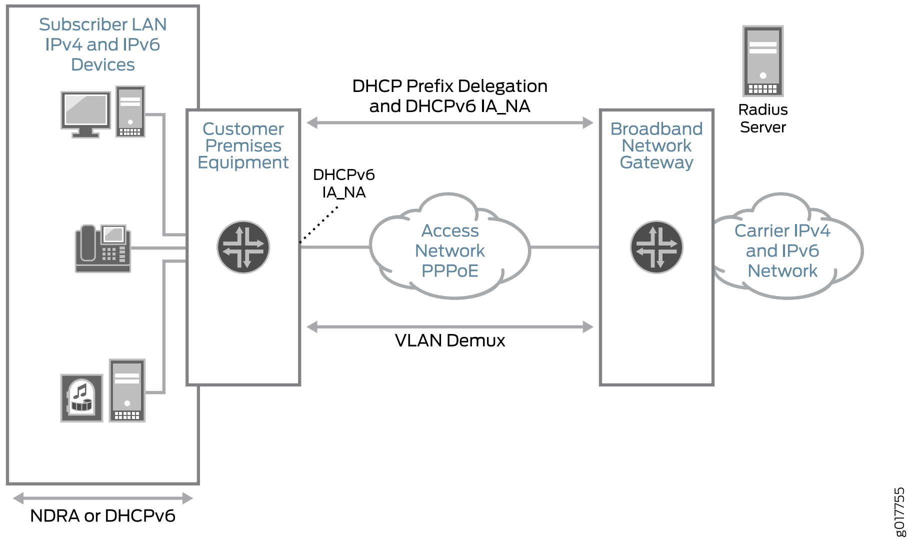


Table 6 on page 100 describes the configuration components used in this example.

Table 6: Configuration Components Used in Dual Stack with DHCPv6 IA_NA and DHCPv6 Prefix Delegation

Configuration Component	Component Name	Purpose
Dynamic profile	pppoe-subscriber-profile	Profile that creates a PPPoE logical interface when the subscriber logs in.
Interfaces	ge-0/2/5	Interface used for communication with the RADIUS server.
	ge-0/3/0	Underlying Ethernet interface.
	demux0	VLAN demux interface that runs over the underlying Ethernet interface.
	lo0	Loopback interface for use in the access network. The loopback interface is automatically used for unnumbered interfaces.
Address-assignment pools	pool v4-pool	Pool that provides IPv4 addresses for the subscriber LAN.
	pool v6-ia-na-pool	Pool that provides a global IPv6 address to the CPE WAN link.
	pool v6-pd-pool	Pool that provides a pool of prefixes that are delegated to the CPE and used for assigning IPv6 global addresses on the subscriber LAN.

Configuration

CLI Quick Configuration

The following is the complete configuration for this example:

```
dynamic-profiles {
  pppoe-subscriber-profile {
    routing-instances {
      "$junos-routing-instance" {
        interface "$junos-interface-name";
      }
    }
    interfaces {
      pp0 {
        unit "$junos-interface-unit" {
          ppp-options {
            chap;
            pap;
          }
          pppoe-options {
            underlying-interface "$junos-underlying-interface";
            server;
          }
          keepalives interval 30;
          family inet {
            unnumbered-address "$junos-loopback-interface";
          }
          family inet6 {
            unnumbered-address "$junos-loopback-interface";
          }
        }
      }
    }
  }
}
  system {
    services {
      dhcp-local-server {
        dhcpv6 {
          group v6-ppp-subscriber {
            interface pp0.0;
          }
```

```
            }
        }
    }
}
interfaces {
    ge-0/2/5 {
        gigether-options {
            no-auto-negotiation;
        }
        unit 0 {
            family inet {
                address 10.9.0.9/32;
            }
        }
    }
    ge-0/3/0 {
        hierarchical-scheduler maximum-hierarchy-levels 2;
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 1;
    }
    demux0 {
        unit 1 {
            proxy-arp;
            vlan-tags outer 1 inner 1;
            demux-options {
                underlying-interface ge-0/3/0;
            }
            family pppoe {
                duplicate-protection;
                dynamic-profile pppoe-subscriber-profile;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.1/32 {
                    primary;
                    preferred;
                }
            }
            family inet6 {
                address 2001:0::1/128 {
                    primary;
                    preferred;
                }
            }
        }
    }
}
routing-options {
    router-id 10.0.0.0;
}
access {
    radius-server {
```



```
      10.9.0.9 {
        secret "$9$lXRv87GUHm5FYgF/CA1I"; ## SECRET-DATA
        timeout 45;
        retry 4;
        source-address 10.0.0.1;
      }
    }
    profile Access-Profile {
      authentication-order radius;
      radius {
        authentication-server 10.9.0.9;
        accounting-server 10.9.0.9;
      }
      accounting {
        order [ radius none ];
        update-interval 120;
        statistics volume-time;
      }
    }
    address-assignment {
      pool v4-pool {
        family inet {
          network 10.16.0.1/32;
          range v4-range-0 {
            low 10.16.0.1;
            high 10.31.255.255;
          }
          dhcp-attributes {
            maximum-lease-time 99999;
          }
        }
      }
      pool v6-ia-na-pool {
        family inet6 {
          prefix 1000:0000::/64;
          range v6-range-0 {
            low 1000::1/128;
            high 1000::ffff:ffff/128;
          }
        }
      }
      pool v6-pd-pool {
        family inet6 {
          prefix 2012::/48;
          range v6-pd prefix-length 64;
        }
      }
    }
    address-protection;
  }
```

Configuring a DHCPv6 Local Server for DHCPv6 over PPPoE

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit system services dhcp-local-server dhcpv6
edit group v6-ppp-subscriber
set interface pp0.0
```

Step-by-Step Procedure

To layer DHCPv6 above the PPPoE IPv6 family (inet6), associate DHCPv6 with the PPPoE interfaces by adding the PPPoE interfaces to the DHCPv6 local server configuration. Because this example uses a dynamic PPPoE interface, we are using the pp0.0 (PPPoE) logical interface as a wildcard to indicate that a DHCPv6 binding can be made on top of a PPPoE interface.

To configure a DHCPv6 local server:

1. Access the DHCPv6 local server configuration.

   ```
   [edit]
   user@host# edit system services dhcp-local-server dhcpv6
   ```

2. Create a group for dynamic PPPoE interfaces and assign a name.

   The group feature groups a set of interfaces and then applies a common DHCP configuration to the named interface group.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# edit group v6-ppp-subscriber
   ```

3. Add an interface for dynamic PPPoE logical interfaces.

   ```
   [edit system services dhcp-local-server dhcpv6 group v6-ppp-subscriber]
   user@host# set interface pp0.0
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit]
user@host# show
system {
  services {
    dhcp-local-server {
      dhcpv6 {
        group v6-ppp-subscriber {
          interface pp0.0;
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Dynamic Profile for the PPPoE Logical Interface

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit dynamic-profiles pppoe-subscriber-profile
edit routing-instances $junos-routing-instance
set interface $junos-interface-name
exit
edit interfaces pp0 unit $junos-interface-unit
set family inet unnumbered-address "$junos-loopback-interface"
set family inet6 unnumbered-address "$junos-loopback-interface"
set pppoe-options underlying-interface "$junos-underlying-interface"
set pppoe-options server
set ppp-options pap
set ppp-options chap
set keepalives interval 30
```

Step-by-Step Procedure

Create a dynamic profile for the PPPoE logical interface. This dynamic profile supports both IPv4 and IPv6 sessions on the same logical interface.

To configure the dynamic profile:

1. Create and name the dynamic profile.

   ```
   [edit]
   user@host# edit dynamic-profiles pppoe-subscriber-profile
   ```

2. Add a routing instance to the profile.

   ```
   [edit dynamic-profiles pppoe-subscriber-profile]
   user@host# edit routing-instances $junos-routing-instance
   user@host# set interface $junos-interface-name
   ```

3. Configure a PPPoE logical interface (pp0) that is used to create logical PPPoE interfaces for the IPv4 and IPv6 subscribers.

   ```
   [edit dynamic-profiles pppoe-subscriber-profile]
   user@host# edit interfaces pp0
   ```

4. Specify **$junos-interface-unit** as the predefined variable to represent the logical unit number for the **pp0** interface. The variable is dynamically replaced with the actual unit number supplied by the network when the subscriber logs in.

   ```
   [edit dynamic-profiles pppoe-subscriber-profile interfaces pp0]
   user@host# edit unit $junos-interface-unit
   ```

5. Specify **$junos-underlying-interface** as the predefined variable to represent the name of the underlying Ethernet interface on which the router creates the dynamic PPPoE logical interface. The variable is dynamically replaced with the actual name of the underlying interface, which is supplied by the network when the subscriber logs in.

   ```
   [edit dynamic-profiles pppoe-subscriber-profile interfaces pp0 unit
     "$junos-interface-unit"]
   ```



```
user@host# set pppoe-options underlying-interface $junos-underlying-interface
```

6. Configure the router to act as a PPPoE server when a PPPoE logical interface is dynamically created.

```
[edit dynamic-profiles pppoe-subscriber-profile interfaces pp0 unit
  "$junos-interface-unit"]
user@host# set pppoe-options server
```

7. Configure the IPv4 family for the pp0 interface. Specify the unnumbered address to dynamically apply loopback interfaces. Because the example uses routing instances, assign the predefined variable **$junos-loopback-interface**.

```
[edit dynamic-profiles pppoe-subscriber-profile interfaces pp0 unit
  "$junos-interface-unit"]
user@host# set family inet unnumbered-address $junos-loopback-interface
```

8. Configure the IPv6 family for the pp0 interface. Specify the unnumbered address to dynamically create loopback interfaces. Because the example uses routing instances without router advertisement, assign the predefined variable **$junos-loopback-interface**.

```
[edit dynamic-profiles pppoe-subscriber-profile interfaces pp0 unit
  "$junos-interface-unit"]
user@host# set family inet6 unnumbered-address $junos-loopback-interface
```

9. Configure one or more PPP authentication protocols for the pp0 interface.

```
[edit dynamic-profiles pppoe-subscriber-profile interfaces pp0 unit
  "$junos-interface-unit"]
user@host# set ppp-options chap
user@host# set ppp-options pap
```

10. Enable keepalives and set an interval for keepalives. We recommend an interval of 30 seconds.

```
[edit dynamic-profiles pppoe-subscriber-profile interfaces pp0 unit
  "$junos-interface-unit"]
user@host# set keepalives interval 30
```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit dynamic-profiles pppoe-subscriber-profile]
user@host# show
routing-instances {
  "$junos-routing-instance" {
    interface "$junos-interface-name";
  }
}
  interfaces {
    pp0 {
      unit "$junos-interface-unit" {
        ppp-options {
          chap;
          pap;
        }
        pppoe-options {
          underlying-interface "$junos-underlying-interface";
```



```
            server;
          }
          keepalives interval 30;
          family inet {
            unnumbered-address "$junos-loopback-interface";
          }
          family inet6 {
            unnumbered-address "$junos-loopback-interface";
          }
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Loopback Interface

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit interfaces lo0
set unit 0 family inet address 10.0.0.1/32 primary
set unit 0 family inet address 10.0.0.1/32 preferred
set unit 0 family inet6 address 2001:0::1/128 primary
set unit 0 family inet6 address 2001:0::1/128 preferred
```

Step-by-Step Procedure

To configure a loopback interface:

1. Create the loopback interface and specify a unit number.

   ```
   [edit]
   user@host# edit interfaces lo0 unit 0
   ```

2. Configure the interface for IPv4.

   ```
   [edit interfaces lo0 unit 0]
   user@host# set family inet address 10.0.0.1/32 primary preferred
   ```

3. Configure the interface for IPv6.

   ```
   [edit interfaces lo0 unit 0]
   user@host# set family inet6 address 2001:0::1/128 primary preferred
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit interfaces lo0]
user@host# show
unit 0 {
  family inet {
    address 10.0.0.1/32 {
      primary;
      preferred;
    }
  }
  family inet6 {
```

```
        address 2001:0::1/128 {
            primary;
            preferred;
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a VLAN Demux Interface over an Ethernet Underlying Interface

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit interfaces
set ge-0/3/0 hierarchical-scheduler maximum-hierarchy-levels 2
set ge-0/3/0 flexible-vlan-tagging
set ge-0/3/0 encapsulation flexible-ethernet-services
exit
edit interfaces demux0 unit 1
set vlan-tags outer 1
set vlan-tags inner 1
set demux-options underlying-interface ge-0/3/0
set family pppoe dynamic-profile pppoe-subscriber-profile
set family pppoe duplicate-protection
set proxy-arp
```

Step-by-Step Procedure

To configure a VLAN demux interface over an Ethernet underlying interface:

1. Configure the underlying Ethernet interface.

```
[edit]
user@host# edit interfaces ge-0/3/0
user@host# set flexible-vlan-tagging
user@host# set encapsulation flexible-ethernet-services
user@host# set hierarchical-scheduler maximum-hierarchy-levels 2
```

2. Create the VLAN demux interface, and specify a unit number.

```
[edit]
user@host# edit interfaces demux0 unit 1
```

3. Configure the VLAN tags.

```
[edit interfaces demux0 unit 1]
user@host# set vlan-tags outer 1 inner 1
```

4. Specify the underlying Ethernet interface.

```
[edit interfaces demux0 unit 1]
user@host# set demux-options underlying-interface ge-0/3/0
```

5. Specify the dynamic profile.

```
[edit interfaces demux0 unit 1]
user@host# set family pppoe dynamic-profile pppoe-subscriber-profile
```

6. Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on the same VLAN interface.

```
[edit interfaces demux0 unit 1]
user@host# set family pppoe duplicate-protection
```

7. (Optional) Specify that you want the demux interface to use proxy ARP.

```
[edit interfaces demux0 unit 1]
```

user@host# **set proxy-arp**

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit interfaces]
user@host# show
ge-0/3/0 {
  hierarchical-scheduler maximum-hierarchy-levels 2;
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
}
  demux0 {
    unit 1 {
      proxy-arp;
      vlan-tags outer 1 inner 1;
      demux-options {
        underlying-interface ge-0/3/0;
      }
      family pppoe {
        duplicate-protection;
        dynamic-profile pppoe-subscriber-profile;
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring an Interface for Communication with RADIUS Server

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit interfaces ge-0/2/5
set unit 0 family inet address 10.9.0.9
set gigether-options no-auto-negotiation
```

Step-by-Step Procedure

To configure the interface:

1. Create the interface, specify a unit number, and configure the address.

   ```
   [edit]
   user@host# edit interfaces ge-0/2/5
   ```

2. Configure the interface for IPv4 and specify the address.

   ```
   [edit interfaces ge-0/2/5]
   user@host# set unit 0 family inet address 10.9.0.9
   ```

3. Specify that Gigabit Ethernet options are not automatically negotiated.

   ```
   [edit interfaces ge-0/2/5]
   user@host# set gigether-options no-auto-negotiation
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit interfaces ge-0/2/5]
user@host# show
gigether-options {
  no-auto-negotiation;
}
  unit 0 {
    family inet {
      address 10.9.0.9/32;
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Specifying the BNG IP Address

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit routing-options
set router-id 10.0.0.0
```

BEST PRACTICE: We strongly recommend that you configure the BNG IP address, thereby avoiding unpredictable behavior if the interface address on a loopback interface changes.

Step-by-Step Procedure

To configure the IP address of the BNG:

1. Access the routing-options configuration.

   [edit]
   user@host# **edit routing-options**

2. Specify the IP address or the BNG.

   [edit routing-options]
   user@host# **set router-id 10.0.0.0**

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit routing-options]
user@host# show
router-id 10.0.0.0;
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring RADIUS Server Access

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit access radius-server 10.9.0.9
set secret "$9$lXRv87GUHm5FYgF/CA1I"
set timeout 45
set retry 4
set source-address 10.0.0.1
```

Step-by-Step Procedure

To configure RADIUS servers:

1. Create a RADIUS server configuration, and specify the address of the server.

   [edit]
   user@host# **edit access radius-server 10.9.0.9**

2. Configure the required secret (password) for the server. Secrets enclosed in quotation marks can contain spaces.

   [edit access radius-server 10.9.0.9]
   user@host# **set secret "9lXRv87GUHm5FYgF/CA1I"**

3. Configure the source address that the BNG uses when it sends RADIUS requests to the RADIUS server.

   [edit access radius-server 10.9.0.9]

```
user@host# set source address 10.0.0.1
```

4. (Optional) Configure the number of times that the router attempts to contact a RADIUS accounting server. You can configure the router to retry from 1 through 16 times. The default setting is 3 retry attempts.

```
[edit access radius-server 10.9.0.9]
user@host# set retry 4
```

5. (Optional) Configure the length of time that the local router or switch waits to receive a response from a RADIUS server. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

```
[edit access radius-server 10.9.0.9]
user@host# set timeout 45
```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
radius-server {
  10.9.0.9 {
    secret "$9$lXRv87GUHm5FYgF/CA1I"; ## SECRET-DATA
    timeout 45;
    retry 4;
    source-address 10.0.0.1;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring RADIUS Server Access Profile

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit access profile Access-Profile
set authentication-order radius
set radius authentication-server 10.9.0.9
set radius accounting-server 10.9.0.9
set accounting order radius
set accounting order none
set accounting update-interval 120
set accounting statistics volume-time
```

Step-by-Step Procedure To configure a RADIUS server access profile:

1. Create a RADIUS server access profile.

```
[edit]
user@host# edit access profile Access-Profile
```

2. Specify the order in which authentication methods are used.

```
[edit access profile Access-Profile]
```

```
user@host# set authentication-order radius
```

3. Specify the address of the RADIUS server used for authentication and the server used for accounting.

```
[edit access profile Access-Profile]
user@host# set radius authentication-server 10.9.0.9
user@host# set radius accounting-server 10.9.0.9
```

4. Configure RADIUS accounting values for the access profile.

```
[edit access profile Access-Profile]
user@host# set accounting order [ radius none ]
user@host# set accounting update-interval 120
user@host# set accounting statistics volume-time
```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
profile Access-Profile {
  authentication-order radius;
  radius {
    authentication-server 10.9.0.9;
    accounting-server 10.9.0.9;
  }
  accounting {
    order [ radius none ];
    update-interval 120;
    statistics volume-time;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring Local Address-Assignment Pools

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit access address-assignment
set pool v4-pool family inet network 10.16.0.1/32
set pool v4-pool family inet range v4-range-0 low 10.16.0.1
set pool v4-pool family inet range v4-range-0 high 10.31.255.255
set pool v4-pool family inet dhcp-attributes maximum-lease-time 99999
set pool v6-ia-na-pool family inet6 prefix 1000:0000::/64
set pool v6-ia-na-pool family inet6 range v6-range-0 low 1000::1/128
set pool v6-ia-na-pool family inet6 range v6-range-0 high 1000::ffff:ffff/128
set pool v6-pd-pool family inet6 prefix 2012::/48
set pool v6-pd-pool family inet6 range v6-pd prefix-length 64
```


Step-by-Step Procedure

Configure three address-assignment pools for DHCPv4, DHCPv6 IA_NA, and DHCPv6 prefix delegation.

To configure the address-assignment pools:

1. Configure the address-assignment pool for DHCPv4.

```
[edit]
user@host# edit access address-assignment pool v4-pool
user@host# edit family inet
user@host# set network 10.16.0.1
user@host# set range v4-range-0 low 10.16.0.1
user@host# set range v4-range-0 high 10.31.255.255
user@host# set dhcp-attributes maximum-lease-time 99999
```

2. Configure the address-assignment pool for DHCPv6 IA_NA.

```
[edit]
user@host# edit access address-assignment pool v6-ia-na-pool
user@host# edit family inet6
user@host# set prefix 1000:0000::/64
user@host# set range v6-range-0 low 1000::1/128
user@host# set range v6-range-0 high 1000::ffff:ffff/128
```

3. Configure the address-assignment pool for DHCPv6 prefix delegation.

```
[edit]
user@host# edit access address-assignment pool v6-pd-pool
user@host# edit family inet6
user@host# set prefix 2012::/48
user@host# set range v6-pd prefix-length 64
```

4. (Optional) Enable duplicate prefix protection.

```
[edit access]
user@host# set address-protection
```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
address-assignment {
  pool v4-pool {
    family inet {
      network 10.16.0.1/32;
      range v4-range-0 {
        low 10.16.0.1;
        high 10.31.255.255;
      }
      dhcp-attributes {
        maximum-lease-time 99999;
      }
    }
  }
  pool v6-ia-na-pool {
    family inet6 {
      prefix prefix 1000:0000::/64 ;
      range v6-range-0 {
```

```
            low 1000::1/128;
            high 1000::ffff:ffff/128;
          }
        }
      }
      pool v6-pd-pool {
        family inet6 {
          prefix 2012::/48;
          range v6-pd prefix-length 64;
        }
      }
      }
    address-protection;
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Active Subscriber Sessions

Purpose Verify active subscriber sessions.

Action From operational mode, enter the **show subscribers summary** command.

```
user@host>show subscribers summary
Subscribers by State
   Active: 2
   Total: 2

Subscribers by Client Type
   DHCP: 1
   PPPoE: 1
   Total: 2
```

Meaning The fields under **Subscribers by State** show the number of active subscribers.

The fields under **Subscribers by Client Type** show the number of active DHCP and PPPoE subscriber sessions.

Verifying Both IPv4 and IPv6 Address in Correct Routing Instance

Purpose Verify that the subscriber has both an IPv4 and an IPv6 address and is placed in the correct routing instance.

Action From operational mode, enter the **show subscribers** command.

```
user@host>show subscribers
Interface            IP Address/VLAN ID       User Name           LS:RI
pp0.1073741825       10.16.0.2               SBRSTATICUSER       default:default
pp0.1073741825       1000::1                                     default:default
```

Meaning The **Interface** field shows that two subscriber sessions are running on the same interface. The **IP Address** field shows that one session is assigned an IPv4 address, and the second session is assigned an IPv6 address by DHCPv6 IA_NA.

The **LS:RI** field shows that the subscriber is placed in the correct routing instance and that traffic can be sent and received.

Verifying Dynamic Subscriber Sessions

Purpose Verify dynamic PPPoE and DHCPv6 subscriber sessions. In this sample configuration, the DHCPv6 subscriber session should be layered over the underlying PPPoE subscriber session.

Action From operational mode, enter the **show subscribers detail** command.

```
user@host>show subscribers detail
Type: PPPoE
User Name: SBRSTATICUSER
IP Address: 10.16.0.2
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: pppoe-subscriber-profile
MAC Address: 00:01:02:00:00:01
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-12-08 09:11:41 PST

Type: DHCP
IPv6 Address: 1000::1
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:01:02:00:00:01
State: Active
Radius Accounting ID: 3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-12-08 09:12:11 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 01 02 00 00 01
00 06 00 02 00 03 00 03 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

Meaning When a subscriber has logged in and started both an IPv4 and an IPv6 session, the output shows the active underlying PPPoE session and the active DHCPv6 session.

The **Session ID** field for the PPPoE session is 2. The **Underlying Session ID** for the DHCP session is 2, which shows that the PPPoE session is the underlying session.

Verifying DHCPv6 Address Pools Used for DHCPv6 Prefix Delegation

Purpose Verify the delegated address pool used for DHCPv6 prefix delegation and the length of the IPv6 prefix that was delegated to the CPE.

Action From operational mode, enter the **show subscribers extensive** command.

```
user@host>show subscribers extensive
Type: PPPoE
User Name: SBRSTATICUSER
IP Address: 10.16.0.2
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: pppoe-subscriber-profile
MAC Address: 00:01:02:00:00:01
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-12-08 09:11:41 PST
IPv6 Delegated Address Pool: v6-na-pool

Type: DHCP
IPv6 Address: 1000::1
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:01:02:00:00:01
State: Active
Radius Accounting ID: 3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-12-08 09:12:11 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 01 02 00 00 01
00 06 00 02 00 03 00 03 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Address Pool: v6-na-pool
IPv6 Delegated Network Prefix Length: 64
```

Meaning The **IPv6 Delegated Address Pool** field shows the name of the pool that DHCPv6 used to assign the IPv6 address for this subscriber session.

Verifying DHCPv6 Address Bindings

Purpose Display the address bindings in the client table on the DHCPv6 local server.

Action From operational mode, enter the **show dhcpv6 server binding detail** command.

```
user@host>show dhcpv6 server binding detail
Session Id:  580547
     Client IPv6 Address:              1000::4/128
     Client DUID:                           LL0x1-00:01:02:00:00:01
     State:                               BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)

     Lease Expires:                         2012-01-05 07:06:04 PST
     Lease Expires in:                      82943 seconds
     Lease Start:                           2012-01-04 07:06:04 PST
     Last Packet Received:                  2012-01-04 07:06:04 PST
     Incoming Client Interface:             pp0.1073926645
     Server Ip Address:                     0.0.0.0
     Client Pool Name:                 v6-na-pool-0
     Client Id Length:                      10
     Client Id:                             /0x00030001/0x00010200/0x0001
```

Meaning The **Client IPv6 Address** field shows the /128 address that was assigned to the CPE WAN link using DHCPv6 IA_NA.

The **Client Pool Name** field shows the name of the address pool that was used to assign the **Client IPv6 Address**.

Verifying PPP Options Negotiated with the Remote Peer

Purpose Verify PPP options negotiated with the remote peer.

Action From operational mode, enter the **show ppp interface *interface* extensive** command.

```
user@host>show ppp interface pp0.1073741825 extensive
  Session pp0.1073926645, Type: PPP, Phase: Network
    LCP
      State: Opened
      Last started: 2012-01-04 07:05:33 PST
      Last completed: 2012-01-04 07:05:33 PST
      Negotiated options:
        Authentication protocol: pap, Magic number: 191301485, Local MRU: 1492,
        Peer MRU: 65531
    Authentication: PAP
      State: Grant
      Last started: 2012-01-04 07:05:33 PST
      Last completed: 2012-01-04 07:05:33 PST
    IPCP
      State: Opened
      Last started: 2012-01-04 07:05:34 PST
      Last completed: 2012-01-04 07:05:34 PST
      Negotiated options:
        Local address: 10.0.0.1, Remote address: 10.16.0.2
    IPV6CP
      State: Opened
      Last started: 2012-01-04 07:05:34 PST
      Last completed: 2012-01-04 07:05:34 PST
      Negotiated options:
        Local interface identifier: 2a0:a50f:fc71:e049,
        Remote interface identifier: 201:2ff:fe00:1
```

Meaning The output shows the PPP options that were negotiated with the remote peer.

Under IPCP, the **Negotiated options** field shows the IPv4 local and remote addresses that were negotiated by IPCP.

Under IPV6CP, the **Negotiated options** field shows the IPv6 local and remote interface identifiers that were negotiated by IPv6CP.

Related Documentation

- Overview of Using DHCPv6 IA_NA with DHCPv6 Prefix Delegation on page 27
- Design 1: IPv6 Addressing with DHCPv6 IA_NA and DHCPv6 Prefix Delegation on page 36
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

CHAPTER 18

Example: Dual-Stack Design That Uses NDRA and DHCPv6 Prefix Delegation over PPPoE

Example: Configuring a Dual Stack That Uses NDRA and DHCPv6 Prefix Delegation over PPPoE

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Router
- Junos OS Release 11.4 or later

Overview

This design uses NDRA and DHCPv6 prefix delegation in your subscriber access network as follows:

- The access network is PPPoE.
- NDRA is used to assign a global IPv6 address on the WAN link. The prefixes used in router advertisements come from a local pool that is specified using AAA RADIUS.
- DHCPv6 prefix delegation is used for subscriber LAN addressing. It uses a delegated prefix from a local pool that is specified using AAA RADIUS.
- DHCPv4 is used for subscriber LAN addressing.
- DHCPv6 subscriber sessions are layered over an underlying PPPoE subscriber session.

Topology

Figure 15: PPPoE Subscriber Access Network with NDRA and DHCPv6 Prefix Delegation

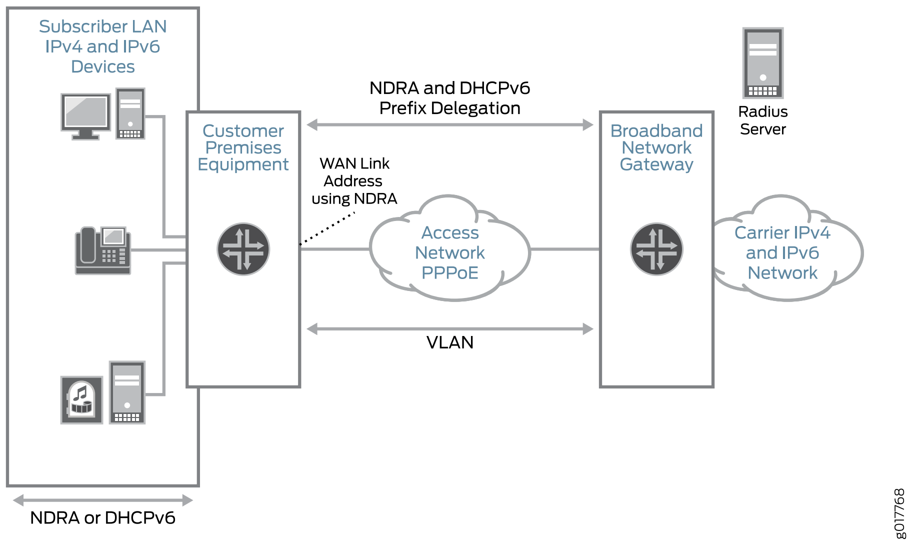


Table 7 on page 125 describes the configuration components used in this example.

Table 7: Configuration Components Used in Dual Stack with NDRA and DHCPv6 Prefix Delegation

Configuration Component	Component Name	Purpose
Dynamic profiles	DS-dyn-ipv4v6-ndra	Profile that creates a PPPoE logical interface when the subscriber logs in.
Interfaces	ge-3/3/0	Underlying Ethernet interface.
	lo0	Loopback interface for use in the access network. The loopback interface is automatically used for unnumbered interfaces.
Address-assignment pools	default-ipv4-pool-2	Pool that provides IPv4 addresses for the subscriber LAN.
	ndra-2010	Pool that provides IPv6 prefixes used in router advertisements. These prefixes are used to create a global IPv6 address that is assigned to the CPE WAN link.
	dhcpv6-pd-pool	Pool that provides a pool of prefixes that are delegated to the CPE and are used for assigning IPv6 global addresses on the subscriber LAN.

Configuration

CLI Quick Configuration

The following is the complete configuration for this example:

```
dynamic-profiles {
  DS-dyn-ipv4v6-ra {
    interfaces {
      pp0 {
        unit "$junos-interface-unit" {
          ppp-options {
            chap;
            pap;
          }
          pppoe-options {
            underlying-interface "$junos-underlying-interface";
            server;
          }
          keepalives interval 30;
          family inet {
            unnumbered-address lo0.0;
          }
          family inet6 {
            address $junos-ipv6-address;
          }
        }
      }
    }
    protocols {
      router-advertisement {
        interface "$junos-interface-name" {
          prefix $junos-ipv6-ndra-prefix;
        }
      }
    }
  }
}
system {
  services {
    dhcp-local-server {
```



```
            dhcpv6 {
                overrides {
                    delegated-pool dhcpv6-pd-pool;
                }
                group DHCPv6-over-pppoe {
                    interface pp0.0;
                }
            }
        }
    }
}
interfaces {
    ge-3/3/0 {
        unit 1109 {
            description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd";
            encapsulation ppp-over-ether;
            vlan-id 1109;
            pppoe-underlying-options {
                duplicate-protection;
                dynamic-profile DS-dyn-ipv4v6-ra;
            }
        }
    }
    lo0 {
        description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd";
        unit 0 {
            family inet {
                address 77.1.1.1/32 {
                    primary;
                }
            }
            family inet6 {
                address 2030:0:0:0::1/64 {
                    primary;
                }
            }
        }
    }
}
routing-options {
    router-id 10.0.0.0;
}
access {
    radius-server {
        10.9.0.9 {
            secret "$9$lXRv87GUHm5FYgF/CA1I"; ## SECRET-DATA
            timeout 45;
            retry 4;
            source-address 10.0.0.1;
        }
    }
    profile Access-Profile {
        authentication-order radius;
        radius {
            authentication-server 10.9.0.9;
            accounting-server 10.9.0.9;
```

```
        }
        accounting {
            order [ radius none ];
            update-interval 120;
            statistics volume-time;
        }
    }
    address-assignment {
        pool default-ipv4-pool-2 {
            family inet {
                network 10.10.0.0/16;
                range r5 {
                    low 10.10.0.1;
                    high 10.10.250.250;
                }
            }
        }
        pool dhcpv6-pd-pool {
            family inet6 {
                prefix 2040:2000:2000::/48;
                range r1 prefix-length 64;
            }
        }
        pool ndra-2010 {
            family inet6 {
                prefix 2010:0:0:0::/48;
                range L prefix-length 64;
            }
        }
    }
    address-protection;
}
```

Configuring a DHCPv6 Local Server for DHCPv6 over PPPoE

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit system services dhcp-local-server dhcpv6
edit group DHCPv6-over-pppoe
set interface pp0.0
```

Step-by-Step Procedure

To layer DHCPv6 above the PPPoE IPv6 family (inet6), associate DHCPv6 with the PPPoE interfaces by adding the PPPoE interfaces to the DHCPv6 local server configuration. Because this example uses a dynamic PPPoE interface, we are using the pp0.0 (PPPoE) logical interface as a wildcard to indicate that a DHCPv6 binding can be made on top of a PPPoE interface.

To configure a DHCPv6 local server:

1. Access the DHCPv6 local server configuration.

   ```
   [edit]
   ```



```
user@host# edit system services dhcp-local-server dhcpv6
```

2. Create a group for dynamic PPPoE interfaces and assign a name.

   The group feature groups a set of interfaces and then applies a common DHCP configuration to the named interface group.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# edit group DHCPv6-over-pppoe
   ```

3. Add an interface for dynamic PPPoE logical interfaces.

   ```
   [edit system services dhcp-local-server dhcpv6 group DHCPv6-over-pppoe]
   user@host# set interface pp0.0
   ```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit]
user@host# show
system {
  services {
    dhcp-local-server {
      dhcpv6 {
        group DHCPv6-over-pppoe {
          interface pp0.0;
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Dynamic Profile for the PPPoE Logical Interface

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit dynamic-profiles DS-dyn-ipv4v6-ra
edit interfaces pp0 unit $junos-interface-unit
set family inet unnumbered-address lo0.0
set family inet6 address $junos-ipv6-address
set pppoe-options underlying-interface "$junos-underlying-interface"
set pppoe-options server
set ppp-options pap
set ppp-options chap
set keepalives interval 30
up 3
edit protocols router-advertisement
edit interface $junos-interface-name
set prefix $junos-ipv6-ndra-prefix
```


Step-by-Step Procedure

Create a dynamic profile for the PPPoE logical interface. This dynamic profile supports both IPv4 and IPv6 sessions on the same logical interface.

To configure the dynamic profile:

1. Create and name the dynamic profile.

   ```
   [edit]
   user@host# edit dynamic-profiles DS-dyn-ipv4v6-ra
   ```

2. Configure a PPPoE logical interface (pp0) that is used to create logical PPPoE interfaces for the IPv4 and IPv6 subscribers.

   ```
   [edit dynamic-profiles DS-dyn-ipv4v6-ra]
   user@host# edit interfaces pp0
   ```

3. Specify **$junos-interface-unit** as the predefined variable to represent the logical unit number for the **pp0** interface. The variable is dynamically replaced with the actual unit number supplied by the network when the subscriber logs in.

   ```
   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0]
   user@host# edit unit $junos-interface-unit
   ```

4. Specify **$junos-underlying-interface** as the predefined variable to represent the name of the underlying Ethernet interface on which the router creates the dynamic PPPoE logical interface. The variable is dynamically replaced with the actual name of the underlying interface supplied by the network when the subscriber logs in.

   ```
   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# set pppoe-options underlying-interface $junos-underlying-interface
   ```

5. Configure the router to act as a PPPoE server when a PPPoE logical interface is dynamically created.

   ```
   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# set pppoe-options server
   ```

6. Configure the IPv4 family for the pp0 interface. Specify the unnumbered address to dynamically create loopback interfaces.

   ```
   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# set family inet unnumbered-address lo0.0
   ```

7. Configure the IPv6 family for the pp0 interface. Because the example uses router advertisement, assign the predefined variable **$junos-ipv6-address**.

   ```
   [edit dynamic-profilesDS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# set family inet6 unnumbered-address $junos-ipv6-address
   ```

8. Configure one or more PPP authentication protocols for the pp0 interface.

   ```
   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# set ppp-options chap
   user@host# set ppp-options pap
   ```

9. Enable keepalives and set an interval for keepalives. We recommend an interval of 30 seconds.

   ```
   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# set keepalives interval 30
   ```

10. Access the router advertisement configuration.

    ```
    [edit dynamic-profiles DS-dyn-ipv4v6-ra]
    user@host# edit protocols router-advertisement
    ```

11. Specify the interface on which the NDRA configuration is applied.

    ```
    [edit dynamic-profiles DS-dyn-ipv4v6-ra protocols router-advertisement]
    user@host# edit interface $junos-interface-name
    ```

12. Specify a prefix value contained in router advertisement messages sent to the CPE on interfaces created with this dynamic profile. If you specify the $junos-ipv6-ndra-prefix predefined variable, the actual value is obtained from a local pool or through AAA.

    ```
    [edit dynamic-profiles DS-dyn-ipv4v6-ra protocols router-advertisement interface
      "$junos-interface-name"]
    user@host# set prefix $junos-ipv6-ndra-prefix
    ```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit dynamic-profiles DS-dyn-ipv4v6-ra]
user@host# show
interfaces {
  pp0 {
    unit "$junos-interface-unit" {
      ppp-options {
        chap;
        pap;
      }
      pppoe-options {
        underlying-interface "$junos-underlying-interface";
        server;
      }
      keepalives interval 30;
      family inet {
        unnumbered-address lo0.0;
      }
      family inet6 {
        address $junos-ipv6-address;
      }
    }
  }
}
  protocols {
    router-advertisement {
      interface "$junos-interface-name" {
        prefix $junos-ipv6-ndra-prefix;
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Loopback Interface

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit interfaces lo0 unit 0
set family inet address 77.1.1.1/32 primary
set family inet6 address 2030:0:0:0::1/64 primary
```

Step-by-Step Procedure

To configure a loopback interface:

1. Create the loopback interface and specify a unit number.

   ```
   [edit]
   user@host# edit interfaces lo0 unit 0
   ```

2. Configure the interface for IPv4.

   ```
   [edit interfaces lo0 unit 0]
   user@host# set family inet address 77.1.1.1/32 primary
   ```

3. Configure the interface for IPv6.

   ```
   [edit interfaces lo0 unit 0]
   user@host# set family inet6 address 2030:0:0:0::1/64 primary
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit interfaces lo0]
user@host# show
unit 0 {
  family inet {
    address 77.1.1.1/32 {
      primary;
    }
  }
  family inet6 {
    address 2030:0:0:0::1/64 {
      primary;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Static Underlying Ethernet Interface for Dynamic PPPoE Subscriber Interfaces

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit interfaces ge-3/3/0 unit 1109
set description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd"
set encapsulation ppp-over-ether
set vlan-id 1109
set pppoe-underlying-options duplicate-protection
set pppoe-underlying-options dynamic-profile DS-dyn-ipv4v6-ra
```

Step-by-Step Procedure

To configure the underlying Ethernet interface:

1. Specify the name and logical unit number of the static underlying Ethernet interface to which you want to attach the IPv4 and IPv6 dynamic profile.

   ```
   [edit]
   user@host# edit interfaces ge-3/3/0 unit 1109
   ```

2. Configure a description for the interface.

   ```
   [edit interfaces ge-3/3/0 unit 1109]
   user@host# set description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd”
   ```

3. Configure PPPoE encapsulation on the underlying interface.

   ```
   [edit interfaces ge-3/3/0 unit 1109]
   user@host# set encapsulation ppp-over-ether
   ```

4. Configure the VLAN ID.

   ```
   [edit interfaces ge-3/3/0 unit 1109]
   user@host# set vlan-id 1109
   ```

5. Attach the dynamic profile to the underlying interface.

   ```
   [edit interfaces ge-3/3/0 unit 1109]
   user@host# set pppoe-underlying-options dynamic-profile DS-dyn-ipv4v6-ra
   ```

6. (Optional) Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on the same VLAN interface.

   ```
   [edit interfaces ge-3/3/0 unit 1109]
   user@host# set pppoe-underlying-options duplicate-protection
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit interfaces]
user@host# show
ge-3/3/0 {
  unit 1109 {
    description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd";
    encapsulation ppp-over-ether;
    vlan-id 1109;
    pppoe-underlying-options {
      duplicate-protection;
      dynamic-profile DS-dyn-ipv4v6-ra;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Specifying the BNG IP Address

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit routing-options
set router-id 10.0.0.0
```

BEST PRACTICE: **We strongly recommend that you configure the BNG IP address to avoid unpredictable behavior if the interface address on a loopback interface changes.**

Step-by-Step Procedure

To configure the IP address of the BNG:

1. Access the routing-options configuration.

   ```
   [edit]
   user@host# edit routing-options
   ```

2. Specify the IP address or the BNG.

   ```
   [edit routing-options]
   user@host# set router-id 10.0.0.0
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit routing-options]
user@host# show
router-id 10.0.0.0;
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring RADIUS Server Access

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit access radius-server 10.9.0.9
set secret "$9$lXRv87GUHm5FYgF/CA1I"
set timeout 45
set retry 4
set source-address 10.0.0.1
```

Step-by-Step Procedure

To configure RADIUS servers:

1. Create a RADIUS server configuration, and specify the address of the server.

   ```
   [edit]
   ```



```
user@host# edit access radius-server 10.9.0.9
```

2. Configure the required secret (password) for the server. Secrets enclosed in quotation marks can contain spaces.

```
[edit access radius-server 10.9.0.9]
user@host# set secret "$9$lXRv87GUHm5FYgF/CA1I"
```

3. Configure the source address that the BNG uses when it sends RADIUS requests to the RADIUS server.

```
[edit access radius-server 10.9.0.9]
user@host# set source address 10.0.0.1
```

4. (Optional) Configure the number of times that the router attempts to contact a RADIUS accounting server. You can configure the router to retry from 1 through 16 times. The default setting is 3 retry attempts.

```
[edit access radius-server 10.9.0.9]
user@host# set retry 4
```

5. (Optional) Configure the length of time that the local router or switch waits to receive a response from a RADIUS server. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

```
[edit access radius-server 10.9.0.9]
user@host# set timeout 45
```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
radius-server {
  10.9.0.9 {
    secret "$9$lXRv87GUHm5FYgF/CA1I"; ## SECRET-DATA
    timeout 45;
    retry 4;
    source-address 10.0.0.1;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring RADIUS Server Access Profile

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit access profile Access-Profile
set authentication-order radius
set radius authentication-server 10.9.0.9
set radius accounting-server 10.9.0.9
set accounting order radius
set accounting order none
set accounting update-interval 120
```


set accounting statistics volume-time

Step-by-Step Procedure

To configure a RADIUS server access profile:

1. Create a RADIUS server access profile.

   [edit]
   user@host# **edit access profile Access-Profile**

2. Specify the order in which authentication methods are used.

   [edit access profile Access-Profile]
   user@host# **set authentication-order radius**

3. Specify the address of the RADIUS server used for authentication and the server used for accounting.

   [edit access profile Access-Profile]
   user@host# **set radius authentication-server 10.9.0.9**
   user@host# **set radius accounting-server 10.9.0.9**

4. Configure RADIUS accounting values for the access profile.

   [edit access profile Access-Profile]
   user@host# **set accounting order [radius none]**
   user@host# **set accounting update-interval 120**
   user@host# **set accounting statistics volume-time**

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
profile Access-Profile {
  authentication-order radius;
  radius {
    authentication-server 10.9.0.9;
    accounting-server 10.9.0.9;
  }
  accounting {
    order [ radius none ];
    update-interval 120;
    statistics volume-time;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring Local Address-Assignment Pools

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

edit access
set address-assignment pool default-ipv4-pool-2 family inet network 10.10.0.0/16
set address-assignment pool default-ipv4-pool-2 family inet range r5 low 10.10.0.1

```
set address-assignment pool default-ipv4-pool-2 family inet range r5 high 10.10.250.250
set address-assignment pool dhcpv6-pd-pool family inet6 prefix 2040:2000:2000::/48
set address-assignment pool dhcpv6-pd-pool family inet6 range r1 prefix-length 64
set address-assignment pool ndra-2010 family inet6 prefix 2010:0:0:0::/48
set address-assignment pool ndra-2010 family inet6 range L prefix-length 64
set address-protection
```

Step-by-Step Procedure

Configure three address-assignment pools for DHCPv4, DHCPv6 prefix delegation, and NDRA.

To configure the address-assignment pools:

1. Configure the address-assignment pool for DHCPv4.

   ```
   [edit]
   user@host# edit access address-assignment pool default-ipv4-pool-2
   user@host# edit family inet
   user@host# set network 10.10.0.0/16
   user@host# set range r5 low 10.10.0.1
   user@host# set range r5 high 10.10.250.250
   ```

2. Configure the address-assignment pool for DHCPv6 prefix delegation.

   ```
   [edit]
   user@host# edit access address-assignment pool dhcpv6-pd-pool
   user@host# edit family inet6
   user@host# set prefix 2040:2000:2000::/48
   user@host# set range r1 prefix-length 64
   ```

3. Configure the address-assignment pool for NDRA.

   ```
   [edit]
   user@host# edit access address-assignment pool ndra-2010
   user@host# edit family inet6
   user@host# set prefix 2010:0:0:0::/48
   user@host# set range L prefix-length 64
   ```

4. (Optional) Enable duplicate prefix protection.

   ```
   [edit access]
   user@host# set address-protection
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
address-assignment {
  pool default-ipv4-pool-2 {
    family inet {
      network 10.10.0.0/16;
      range r5 {
        low 10.10.0.1;
        high 10.10.250.250;
      }
    }
  }
  pool dhcpv6-pd-pool {
    family inet6 {
```

```
            prefix 2040:2000:2000::/48;
            range r1 prefix-length 64;
        }
    }
    pool ndra-2010 {
        family inet6 {
            prefix 2010:0:0:0::/48;
            range L prefix-length 64;
        }
    }
}
address-protection;
```

If you are done configuring the device, enter **commit** from configuration mode.

Specifying the Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit system services dhcp-local-server dhcpv6
set overrides delegated-pool dhcpv6-pd-pool
```

Step-by-Step Procedure

To specify that the dhcp-pd-pool is used for DHCPv6 prefix delegation:

1. Access the DHCPv6 local server configuration.

   ```
   [edit]
   user@host# edit system services dhcp-local-server dhcpv6
   ```

2. Specify the address pool that assigns the delegated prefix.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set overrides delegated-pool dhcpv6-pd-pool
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit system]
user@host# show
services {
    dhcp-local-server {
        dhcpv6 {
            overrides {
                delegated-pool dhcpv6-pd-pool;
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Active Subscriber Sessions

Purpose Verify active subscriber sessions.

Action From operational mode, enter the **show subscribers summary** command.

```
user@host>show subscribers summary
Subscribers by State
   Active: 2
   Total: 2

Subscribers by Client Type
   DHCP: 1
   PPPoE: 1
   Total: 2
```

Meaning The fields under **Subscribers by State** show the number of active subscribers.

The fields under **Subscribers by Client Type** show the number of active DHCP and DHCPoE subscriber sessions.

Verifying Both IPv4 and IPv6 Address in Correct Routing Instance

Purpose Verify that the subscriber has both an IPv4 and IPv6 address and is placed in the correct routing instance.

Action From operational mode, enter the **show subscribers** command.

```
user@host>show subscribers
Interface          IP Address/VLAN ID   User Name               LS:RI
pp0.1073741864     2.2.0.5              dual-stack-v4v6-pd     default:default
*                  2010:0:0:8::/64
pp0.1073741864     2040:2000:2000:5::/64                       default:default
```

Meaning The **Interface** field shows that there are two subscriber sessions running on the same interface. The **IP Address** field shows that one session is assigned an IPv4 address, and one session is assigned on IPv6 address.

The **LS:RI** field shows that the subscriber is placed in the correct routing instance and that traffic can be sent and received.

Verifying Dynamic Subscriber Sessions

Purpose Verify dynamic PPPoE and DHCPv6 subscriber sessions. In this sample configuration, the DHCPv6 subscriber session should be layered over the underlying PPPoE subscriber session.

Action From operational mode, enter the **show subscribers detail** command.

```
user@host>show subscribers detail
Type: PPPoE
User Name: dual-stack-v4v6-pd
IP Address: 2.2.0.5
IP Netmask: 255.255.0.0
IPv6 User Prefix: 2010:0:0:8::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073741864
Interface type: Dynamic
Dynamic Profile Name: DS-dyn-ipv4v6-ra
MAC Address: 00:07:64:11:07:02
State: Active
Radius Accounting ID: 87
Session ID: 87
Login Time: 2012-01-17 14:45:30 PST

Type: DHCP
IPv6 Prefix: 2040:2000:2000:5::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073741864
Interface type: Static
MAC Address: 00:07:64:11:07:02
State: Active
Radius Accounting ID: 88
Session ID: 88
Underlying Session ID: 87
Login Time: 2012-01-17 14:46:00 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 07 64 11 07 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

Meaning When a subscriber has logged in and started both an IPv4 and an IPv6 session, the output shows the active underlying PPPoE session and the active DHCPv6 session.

The **Session ID** field for the PPPoE session is 87. The **Underlying Session ID** for the DHCP session is 87, which shows that the PPPoE session is the underlying session.

Verifying DHCPv6 Address Pools Used for NDRA and DHCPv6 Prefix Delegation

Purpose Verify the pool used for NDRA, the delegated address pool used for DHCPv6 prefix delegation, and the length of the IPv6 prefixes that were delegated to the CPE.

Action From operational mode, enter the **show subscribers extensive** command.

```
user@host>show subscribers extensive
Type: PPPoE
User Name: dual-stack-v4v6-pd
IP Address: 2.2.0.5
IP Netmask: 255.255.0.0
IPv6 User Prefix: 2010:0:0:8::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073741864
Interface type: Dynamic
Dynamic Profile Name: DS-dyn-ipv4v6-ra
MAC Address: 00:07:64:11:07:02
State: Active
Radius Accounting ID: 87
Session ID: 87
Login Time: 2012-01-17 14:45:30 PST
IPv6 Delegated Address Pool: dhcpv6-pd-pool
IPv6 Delegated Address Pool: ndra-2010
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2010:0:0:8::1/64

Type: DHCP
IPv6 Prefix: 2040:2000:2000:5::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073741864
Interface type: Static
MAC Address: 00:07:64:11:07:02
State: Active
Radius Accounting ID: 88
Session ID: 88
Underlying Session ID: 87
Login Time: 2012-01-17 14:46:00 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 07 64 11 07 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Address Pool: dhcpv6-pd-pool
IPv6 Delegated Network Prefix Length: 64
IPv6 Delegated Network Prefix Length: 48
```

Meaning Under the PPPoE session, the **IPv6 Delegated Address Pool** fields show the names of the pools used for DHCPv6 prefix delegation and for NDRA prefixes. The **IPv6 Delegated Network Prefix Length** field shows the length of the prefix used to assign the IPv6 address for this subscriber session. The **IPv6 Interface Address** field shows the IPv6 address assigned to the CPE interface from the NDRA pool.

Under the DHCP session, the **IPv6 Delegated Address Pool** field shows the name of the pool used for DHCPv6 prefix delegation. The **IPv6 Delegated Network Prefix Length** fields show the length of the prefix used in DHCPv6 prefix delegation.

Verifying DHCPv6 Address Bindings

Purpose Display the address bindings in the client table on the DHCPv6 local server.

Action From operational mode, enter the **show dhcpv6 server binding** command.

```
user@host>show dhcpv6 server binding
Prefix                  Session Id  Expires  State    Interface     Client DUID
2040:2000:2000:5::/64   88          86189    BOUND    pp0.1073741864
LL0x1-00:07:64:11:07:02
```

If you have many active subscriber sessions, you can display the server binding for a specific interface.

```
user@host>show dhcpv6 server binding interface pp0.1073741864
Prefix                  Session Id  Expires  State    Interface     Client DUID
2040:2000:2000:5::/64   88          86182    BOUND    pp0.1073741864
LL0x1-00:07:64:11:07:02
```

Meaning The **Prefix** field shows the DHCPv6 prefix assigned to the subscriber session from the pool used for DHCPv6 prefix delegation.

Verifying Router Advertisements

Purpose Verify that router advertisements are being sent, and that router solicits are being received.

Action From operational mode, enter the **show ipv6 router-advertisement** command.

```
user@host>show ipv6 router-advertisement
Interface: pp0.1073741864
  Advertisements sent: 3, last sent 00:03:29 ago
  Solicits received: 0
  Advertisements received: 0
```

If you have a large number of subscriber interfaces, you can display router advertisements for a specific interface.

```
user@host>show ipv6 router-advertisement interface pp0.1073741864
Interface: pp0.1073741864
  Advertisements sent: 3, last sent 00:03:34 ago
  Solicits received: 0
  Advertisements received: 0
```

Meaning The display shows the number of advertisements that the router sent, the number of solicits that the router received, and the number of advertisements that the router received.

Verifying the Status of the PPPoE Logical Interface

Purpose Display status information about the PPPoE logical interface (pp0).

Action From operational mode, enter the **show interfaces pp0.*logical*** command.

```
user@host>show interfaces pp0.1073741864
```



```
Logical interface pp0.1073741864 (Index 388) (SNMP ifIndex 681)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 10,
    Session AC name: almach, Remote MAC address: 00:07:64:11:07:02,
    Underlying interface: ge-3/3/0.1109 (Index 367)
  Bandwidth: 1000mbps
  Input packets : 22
  Output packets: 50
Keepalive settings: Interval 30 seconds, Up-count 1, Down-count 3
LCP state: Opened
NCP state: inet: Opened, inet6: Opened, iso: Not-configured, mpls: Not-configured

CHAP state: Closed
PAP state: Success
  Protocol inet, MTU: 65531
    Flags: Sendbcast-pkt-to-re
    Addresses, Flags: Is-Primary
    Local: 77.1.1.1
  Protocol inet6, MTU: 65531
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 2010:0:0:8::/64, Local: 2010:0:0:8::1
      Local: fe80::2a0:a50f:fc63:a842
```

Meaning

The **Underlying interface** field shows the underlying Ethernet interface configured in the example.

The **Destination** field under **Protocol inet6** shows the IPv6 address obtained through NDRA. This is the value of the **$junos-ipv6-ndra-prefix** variable configured in the dynamic profile.

The **Local** field under **Protocol inet6** shows the value of the *$junos-ipv6-address* variable configured for family inet6 in the pp0 configuration of the dynamic profile.

Related Documentation

- Design 2: IPv6 Addressing with NDRA and DHCPv6 Prefix Delegation on page 37
- How NDRA Works in a Subscriber Access Network on page 16
- DHCPv6 Prefix Delegation over PPPoE on page 25
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74

CHAPTER 19

Example: Dual-Stack Design That Uses NDRA over PPPoE

Example: Configuring a Dual Stack That Uses NDRA over PPPoE

This example shows a dual-stack configuration for a residential subscriber with a single PC. It uses NDRA to provide a prefix used to obtain a global IPv6 address for the PC.

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Router
- Junos OS Release 11.4 or later

Overview

This design uses NDRA in your subscriber access network as follows:

- The access network is PPPoE.
- NDRA is used to assign a global IPv6 address on the WAN link. The prefixes used in router advertisements come from a local pool that is specified by AAA RADIUS.

Topology

Figure 16: PPPoE Subscriber Access Network with NDRA

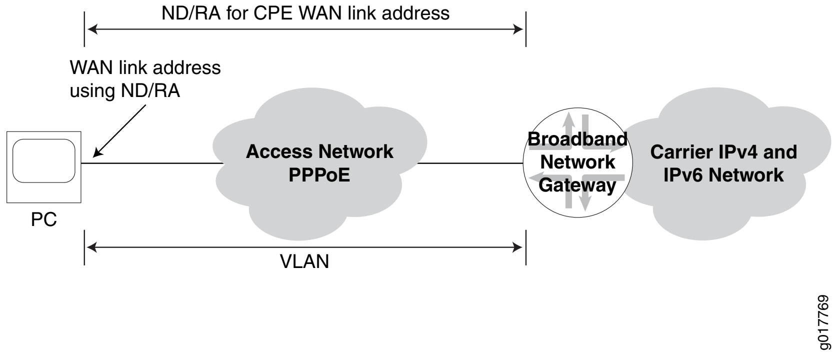


Table 8 on page 146 describes the configuration components used in this example.

Table 8: Configuration Components Used in Dual Stack with NDRA and DHCPv6 Prefix Delegation

Configuration Component	Component Name	Purpose
Dynamic profiles	DS-dyn-ipv4v6-ndra	Profile that creates a PPPoE logical interface when the subscriber logs in.
Interfaces	ge-3/3/0	Underlying Ethernet interface.
	lo0	Loopback interface for use in the access network. The loopback interface is automatically used for unnumbered interfaces.
Address-assignment pools	default-ipv4-pool-2	Pool that provides IPv4 addresses for the subscriber LAN.
	ndra-2010	Pool that provides IPv6 prefixes used in router advertisements. These prefixes are used to create a global IPv6 address that is assigned to the CPE WAN link.

Configuration

To configure this example, perform these tasks:

CLI Quick Configuration

The following is the complete configuration for this example:

```
dynamic-profiles {
  DS-dyn-ipv4v6-ra {
    interfaces {
      pp0 {
        unit "$junos-interface-unit" {
          ppp-options {
            chap;
            pap;
          }
          pppoe-options {
            underlying-interface "$junos-underlying-interface";
            server;
          }
          keepalives interval 30;
          family inet {
            unnumbered-address lo0.0;
          }
          family inet6 {
            address $junos-ipv6-address;
          }
        }
      }
    }
    protocols {
      router-advertisement {
        interface "$junos-interface-name" {
          prefix $junos-ipv6-ndra-prefix;
        }
      }
    }
  }
}
system {
  services {
    dhcp-local-server {
      dhcpv6 {
        group DHCPv6-over-pppoe {
```

```
                interface pp0.0;
              }
            }
          }
        }
      }
      interfaces {
        ge-3/3/0 {
          unit 1004 {
            description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd";
            encapsulation ppp-over-ether;
            vlan-id 1004;
            pppoe-underlying-options {
              duplicate-protection;
              dynamic-profile DS-dyn-ipv4v6-ra;
            }
          }
        }
        lo0 {
          description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd";
          unit 0 {
            family inet {
              address 77.1.1.1/32 {
                primary;
              }
            }
            family inet6 {
              address 2030:0:0:0::1/64 {
                primary;
              }
            }
          }
        }
      }
      routing-options {
        router-id 10.0.0.0;
      }
      access {
        radius-server {
          10.9.0.9 {
            secret "$9$lXRv87GUHm5FYgF/CA1I"; ## SECRET-DATA
            timeout 45;
            retry 4;
            source-address 10.0.0.1;
          }
        }
        profile Access-Profile {
          authentication-order radius;
          radius {
            authentication-server 10.9.0.9;
            accounting-server 10.9.0.9;
          }
          accounting {
            order [ radius none ];
            update-interval 120;
            statistics volume-time;
```



```
      }
    }
    address-assignment {
      neighbor-discovery-router-advertisement ndra-2010;
        pool default-ipv4-pool-2 {
        family inet {
          network 10.10.0.0/16;
          range r5 {
            low 10.10.0.1;
            high 10.10.250.250;
          }
        }
      }
      pool ndra-2010 {
        family inet6 {
          prefix 2010:0:0:0::/48;
          range L prefix-length 64;
        }
      }
    }
    address-protection;
  }
```

Configuring a Dynamic Profile for the PPPoE Logical Interface

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit dynamic-profiles DS-dyn-ipv4v6-ra
edit interfaces pp0 unit $junos-interface-unit
set family inet unnumbered-address lo0.0
set family inet6 address $junos-ipv6-address
set pppoe-options underlying-interface "$junos-underlying-interface"
set pppoe-options server
set ppp-options pap
set ppp-options chap
set keepalives interval 30
up 3
edit protocols router-advertisement
edit interface $junos-interface-name
set prefix $junos-ipv6-ndra-prefix
```

Step-by-Step Procedure

Create a dynamic profile for the PPPoE logical interface. This dynamic profile supports both IPv4 and IPv6 sessions on the same logical interface.

To configure the dynamic profile:

1. Create and name the dynamic profile.

```
[edit]
user@host# edit dynamic-profiles DS-dyn-ipv4v6-ra
```


2. Configure a PPPoE logical interface (pp0) that is used to create logical PPPoE interfaces for the IPv4 and IPv6 subscribers.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra]
   user@host# **edit interfaces pp0**

3. Specify **$junos-interface-unit** as the predefined variable to represent the logical unit number for the pp0 interface. The variable is dynamically replaced with the actual unit number supplied by the network when the subscriber logs in.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0]
   user@host# **edit unit $junos-interface-unit**

4. Specify **$junos-underlying-interface** as the predefined variable to represent the name of the underlying Ethernet interface on which the router creates the dynamic PPPoE logical interface. The variable is dynamically replaced with the actual name of the underlying interface supplied by the network when the subscriber logs in.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# **set pppoe-options underlying-interface $junos-underlying-interface**

5. Configure the router to act as a PPPoE server when a PPPoE logical interface is dynamically created.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# **set pppoe-options server**

6. Configure the IPv4 family for the pp0 interface. Specify the unnumbered address to dynamically create loopback interfaces.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# **set family inet unnumbered-address lo0.0**

7. Configure the IPv6 family for the pp0 interface. Because the example uses router advertisement, assign the predefined variable **$junos-ipv6-address**.

   [edit dynamic-profilesDS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# **set family inet6 unnumbered-address $junos-ipv6-address**

8. Configure one or more PPP authentication protocols for the pp0 interface.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# **set ppp-options chap**
   user@host# **set ppp-options pap**

9. Enable keepalives and set an interval for keepalives. We recommend an interval of 30 seconds.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra interfaces pp0 unit "$junos-interface-unit"]
   user@host# **set keepalives interval 30**

10. Access the router advertisement configuration.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra]
   user@host# **edit protocols router-advertisement**

11. Specify the interface on which the NDRA configuration is applied.

   [edit dynamic-profiles DS-dyn-ipv4v6-ra protocols router-advertisement]
   user@host# **edit interface $junos-interface-name**

12. Specify a prefix value contained in router advertisement messages sent to the CPE on interfaces created with this dynamic profile. If you specify the **$junos-ipv6-ndra-prefix** predefined variable, the actual value is obtained from a local pool or through AAA.

```
[edit dynamic-profiles DS-dyn-ipv4v6-ra protocols router-advertisement interface
   "$junos-interface-name"]
user@host# set prefix $junos-ipv6-ndra-prefix
```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit dynamic-profiles DS-dyn-ipv4v6-ra]
user@host# show
interfaces {
   pp0 {
      unit "$junos-interface-unit" {
         ppp-options {
            chap;
            pap;
         }
         pppoe-options {
            underlying-interface "$junos-underlying-interface";
            server;
         }
         keepalives interval 30;
         family inet {
            unnumbered-address lo0.0;
         }
         family inet6 {
            address $junos-ipv6-address;
         }
      }
   }
}
   protocols {
      router-advertisement {
         interface "$junos-interface-name" {
            prefix $junos-ipv6-ndra-prefix;
         }
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Loopback Interface

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit interfaces lo0 unit 0
set family inet address 77.1.1.1/32 primary
set family inet6 address 2030:0:0:0::1/64 primary
```

Step-by-Step Procedure

To configure a loopback interface:

1. Create the loopback interface and specify a unit number.

   ```
   [edit]
   user@host# edit interfaces lo0 unit 0
   ```

2. Configure the interface for IPv4.

   ```
   [edit interfaces lo0 unit 0]
   user@host# set family inet address 77.1.1.1/32 primary
   ```

3. Configure the interface for IPv6.

   ```
   [edit interfaces lo0 unit 0]
   user@host# set family inet6 address 2030:0:0:0::1/64 primary
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit interfaces lo0]
user@host# show
unit 0 {
  family inet {
    address 77.1.1.1/32 {
      primary;
    }
  }
  family inet6 {
    address 2030:0:0:0::1/64 {
      primary;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Static Underlying Ethernet Interface for Dynamic PPPoE Subscriber Interfaces

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit interfaces ge-3/3/0 unit 1004
set description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd"
set encapsulation ppp-over-ether
set vlan-id 1004
set pppoe-underlying-options duplicate-protection
set pppoe-underlying-options dynamic-profile DS-dyn-ipv4v6-ra
```

Step-by-Step Procedure

To configure the underlying Ethernet interface:

1. Specify the name and logical unit number of the static underlying Ethernet interface to which you want to attach the IPv4 and IPv6 dynamic profile.

   ```
   [edit]
   ```


user@host# **edit interfaces ge-3/3/0 unit 1004**

2. Configure a description for the interface.

   [edit interfaces ge-3/3/0 unit 1004]
   user@host# **set description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd"**

3. Configure PPPoE encapsulation on the underlying interface.

   [edit interfaces ge-3/3/0 unit 1004]
   user@host# **set encapsulation ppp-over-ether**

4. Configure the VLAN ID.

   [edit interfaces ge-3/3/0 unit 1004]
   user@host# **set vlan-id 1004**

5. Attach the dynamic profile to the underlying interface.

   [edit interfaces ge-3/3/0 unit 1004]
   user@host# **set pppoe-underlying-options dynamic-profile DS-dyn-ipv4v6-ra**

6. (Optional) Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on the same VLAN interface.

   [edit interfaces ge-3/3/0 unit 1004]
   user@host# **set pppoe-underlying-options duplicate-protection**

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit interfaces]
user@host# show
ge-3/3/0 {
  unit 1004 {
    description "dynamic ipv4v6 dual stack, ndra, dhcpv6 pd";
    encapsulation ppp-over-ether;
    vlan-id 1004;
    pppoe-underlying-options {
      duplicate-protection;
      dynamic-profile DS-dyn-ipv4v6-ra;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Specifying the BNG IP Address

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit routing-options
set router-id 10.0.0.0
```

BEST PRACTICE: We strongly recommend that you configure the BNG IP address to avoid unpredictable behavior if the interface address on a loopback interface changes.

Step-by-Step Procedure

To configure the IP address of the BNG:

1. Access the routing-options configuration.

   ```
   [edit]
   user@host# edit routing-options
   ```

2. Specify the IP address or the BNG.

   ```
   [edit routing-options]
   user@host# set router-id 10.0.0.0
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit routing-options]
user@host# show
router-id 10.0.0.0;
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring RADIUS Server Access

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit access radius-server 10.9.0.9
set secret "$9$lXRv87GUHm5FYgF/CA1I"
set timeout 45
set retry 4
set source-address 10.0.0.1
```

Step-by-Step Procedure

To configure RADIUS servers:

1. Create a RADIUS server configuration, and specify the address of the server.

   ```
   [edit]
   user@host# edit access radius-server 10.9.0.9
   ```

2. Configure the required secret (password) for the server. Secrets enclosed in quotation marks can contain spaces.

   ```
   [edit access radius-server 10.9.0.9]
   user@host# set secret "$9$lXRv87GUHm5FYgF/CA1I"
   ```

3. Configure the source address that the BNG uses when it sends RADIUS requests to the RADIUS server.

   ```
   [edit access radius-server 10.9.0.9]
   ```

user@host# **set source address 10.0.0.1**

4. (Optional) Configure the number of times that the router attempts to contact a RADIUS accounting server. You can configure the router to retry from 1 through 16 times. The default setting is 3 retry attempts.

   ```
   [edit access radius-server 10.9.0.9]
   user@host# set retry 4
   ```

5. (Optional) Configure the length of time that the local router or switch waits to receive a response from a RADIUS server. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

   ```
   [edit access radius-server 10.9.0.9]
   user@host# set timeout 45
   ```

Results

From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
radius-server {
  10.9.0.9 {
    secret "$9$lXRv87GUHm5FYgF/CA1l"; ## SECRET-DATA
    timeout 45;
    retry 4;
    source-address 10.0.0.1;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring RADIUS Server Access Profile

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit access profile Access-Profile
set authentication-order radius
set radius authentication-server 10.9.0.9
set radius accounting-server 10.9.0.9
set accounting order radius
set accounting order none
set accounting update-interval 120
set accounting statistics volume-time
```

Step-by-Step Procedure

To configure a RADIUS server access profile:

1. Create a RADIUS server access profile.

   ```
   [edit]
   user@host# edit access profile Access-Profile
   ```

2. Specify the order in which authentication methods are used.

   ```
   [edit access profile Access-Profile]
   ```

```
user@host# set authentication-order radius
```

3. Specify the address of the RADIUS server used for authentication and the server used for accounting.

```
[edit access profile Access-Profile]
user@host# set radius authentication-server 10.9.0.9
user@host# set radius accounting-server 10.9.0.9
```

4. Configure RADIUS accounting values for the access profile.

```
[edit access profile Access-Profile]
user@host# set accounting order [ radius none ]
user@host# set accounting update-interval 120
user@host# set accounting statistics volume-time
```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
profile Access-Profile {
  authentication-order radius;
  radius {
    authentication-server 10.9.0.9;
    accounting-server 10.9.0.9;
  }
  accounting {
    order [ radius none ];
    update-interval 120;
    statistics volume-time;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring Local Address-Assignment Pools

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
edit access
set address-assignment pool default-ipv4-pool-2 family inet network 10.10.0.0/16
set address-assignment pool default-ipv4-pool-2 family inet range r5 low 10.10.0.1
set address-assignment pool default-ipv4-pool-2 family inet range r5 high 10.10.250.250
set address-assignment pool ndra-2010 family inet6 prefix 2010:0:0:0::/48
set address-assignment pool ndra-2010 family inet6 range L prefix-length 64
set address-assignment neighbor-discovery-router-advertisement ndra-2010
set address-protection
```

Step-by-Step Procedure Configure two address-assignment pools for DHCPv4 and NDRA.

To configure the address-assignment pools:

1. Configure the address-assignment pool for DHCPv4.


```
[edit]
user@host# edit access address-assignment pool default-ipv4-pool-2
user@host# edit family inet
user@host# set network 10.10.0.0/16
user@host# set range r5 low 10.10.0.1
user@host# set range r5 high 10.10.250.250
```

2. Configure the address-assignment pool for NDRA.

```
[edit]
user@host# edit access address-assignment pool ndra-2010
user@host# edit family inet6
user@host# set prefix 2010:0:0:0::/48
user@host# set range L prefix-length 64
```

3. Specify that the address-assignment pool is used for NDRA.

```
[edit]
user@host# edit access address-assignment
user@host# set neighbor-discovery-router-advertisement ndra-2010
```

4. (Optional) Enable duplicate prefix protection.

```
[edit access]
user@host# set address-protection
```

Results From configuration mode, confirm your configuration by entering the **show** command.

```
[edit access]
user@host# show
address-assignment {
  neighbor-discovery-router-advertisement ndra-2010;
  pool default-ipv4-pool-2 {
    family inet {
      network 10.10.0.0/16;
      range r5 {
        low 10.10.0.1;
        high 10.10.250.250;
      }
    }
  }
  pool ndra-2010 {
    family inet6 {
      prefix 2010:0:0:0::/48;
      range L prefix-length 64;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Active Subscriber Sessions

Purpose Verify active subscriber sessions.

Action From operational mode, enter the **show subscribers summary** command.

```
user@host>show subscribers summary
Subscribers by State
   Active: 2
   Total: 2

Subscribers by Client Type
   DHCP: 1
   PPPoE: 1
   Total: 2
```

Meaning The fields under **Subscribers by State** show the number of active subscribers.

The fields under **Subscribers by Client Type** show the number of active DHCP and underlying PPPoE subscriber sessions.

Verifying Both IPv4 and IPv6 Address in Correct Routing Instance

Purpose Verify that the subscriber has both an IPv4 and IPv6 address and is placed in the correct routing instance.

Action From operational mode, enter the **show subscribers** command.

```
user@host>show subscribers
Interface           IP Address/VLAN ID   User Name               LS:RI
pp0.1073741864      2.2.0.5              dual-stack-v4v6-pd   default:default
*                   2010:0:0:8::/64
pp0.1073741864      2040:2000:2000:5::/64                     default:default
```

Meaning The **Interface** field shows that there are two subscriber sessions running on the same interface. The **IP Address** field shows that one session is assigned an IPv4 address, and one session is assigned on IPv6 address.

The **LS:RI** field shows that the subscriber is placed in the correct routing instance and that traffic can be sent and received.

Verifying Dynamic Subscriber Sessions

Purpose Verify that the dynamic subscriber session is active and that the IPv6 prefix is obtained from the NDRA pool.

Action From operational mode, enter the **show subscribers detail** command.

```
user@host>show subscribers detail
Type: PPPoE
User Name: dual-stack-v4v6-nas
IP Address: 2.2.0.4
IP Netmask: 255.255.0.0
IPv6 User Prefix: 2010:0:0:6::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073741859
Interface type: Dynamic
Dynamic Profile Name: DS-dyn-ipv4v6-ra
MAC Address: 00:00:64:10:04:02
State: Active
Radius Accounting ID: 81
Session ID: 81
Login Time: 2012-01-17 14:19:41 PST
```

Meaning The **IPv6 User Prefix** field shows the prefix that was obtained from the NDRA pool. The **State** field shows that the session is active.

Verifying the NDRA Prefix Pool and Prefix Length

Purpose Verify the pool used for NDRA and the prefix length used with the pool

Action From operational mode, enter the **show subscribers extensive** command.

```
user@host>show subscribers extensive
Type: PPPoE
User Name: dual-stack-v4v6-nas
IP Address: 2.2.0.4
IP Netmask: 255.255.0.0
IPv6 User Prefix: 2010:0:0:6::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073741859
Interface type: Dynamic
Dynamic Profile Name: DS-dyn-ipv4v6-ra
MAC Address: 00:00:64:10:04:02
State: Active
Radius Accounting ID: 81
Session ID: 81
Login Time: 2012-01-17 14:19:41 PST
IPv6 Delegated Address Pool: ndra-2010
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2010:0:0:6::1/64
```

Meaning Under the PPPoE session, the **IPv6 Delegated Address Pool** field shows the name of the pool used for NDRA prefixes. The **IPv6 Delegated Network Prefix Length** field shows the length of the prefix used to assign the IPv6 address for this subscriber session. The **IPv6**

Interface Address field shows the IPv6 address assigned to the CPE interface from the NDRA pool.

Verifying the Status of the PPPoE Logical Interface

Purpose Display status information about the PPPoE logical interface (pp0).

Action From operational mode, enter the **show interfaces pp0.*logical*** command.

```
user@host>show interfaces pp0.1073741859
Logical interface pp0.1073741859 (Index 388) (SNMP ifIndex 674)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
    PPPoE:
      State: SessionUp, Session ID: 10,
      Session AC name: almach, Remote MAC address: 00:00:64:10:04:02,
      Underlying interface: ge-3/3/0.1004 (Index 354)
    Bandwidth: 1000mbps
    Input packets : 15
    Output packets: 44
  Keepalive settings: Interval 30 seconds, Up-count 1, Down-count 3
  LCP state: Opened
  NCP state: inet: Opened, inet6: Opened, iso: Not-configured, mpls: Not-configured

  CHAP state: Closed
  PAP state: Success
    Protocol inet, MTU: 65531
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Primary
        Local: 77.1.1.1
    Protocol inet6, MTU: 65531
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 2010:0:0:6::/64, Local: 2010:0:0:6::1
        Local: fe80::2a0:a50f:fc63:a842
```

Meaning The **Local** field under **Protocol inet** shows the IPv4 address of the pp0 interface. This is the IPv4 address configured for the loopback interface.

The **Destination** field under **Protocol inet6** shows the IPv6 address obtained through NDRA. This is the value of the *$junos-ipv6-ndra-prefix* variable configured in the dynamic profile.

The **Local** field under **Protocol inet6** shows the value of the *$junos-ipv6-address* variable configured for family inet6 in the pp0 configuration of the dynamic profile.

Verifying Router Advertisements

Purpose Verify that router advertisements are being sent and that router solicits are being received.

Action From operational mode, enter the **show ipv6 router-advertisement** command.

```
user@host>show ipv6 router-advertisement
Interface: pp0.1073741859
  Advertisements sent: 3, last sent 00:09:53 ago
  Solicits received: 0
  Advertisements received: 0
```


If you have a large number of subscriber interfaces, you can display router advertisements for a specific interface.

```
user@host>show ipv6 router-advertisement interface pp0.1073741859
Interface: pp0.1073741859
  Advertisements sent: 3, last sent 00:10:31 ago
  Solicits received: 0
  Advertisements received: 0
```

Meaning The display shows the number of advertisements that the router sent, the number of solicits that the router received, and the number of advertisements that the router received.

Related Documentation

- How NDRA Works in a Subscriber Access Network on page 16
- Design 3: IPv6 Addressing with NDRA on page 38
- Best Practice: IPv6 Addressing for Logical Interfaces in PPPoE Dynamic Profiles with NDRA on page 68
- Overview of Configuration Tasks for IPv4 and IPv6 Dual-Stack in Subscriber Access Networks on page 74