ERICSSON

Configuring ND

SYSTEM ADMINISTRATOR GUIDE

33/1543-CRA 119 1170/1-V1 Uen G

Contents

1 Overview

This document provides an overview of the Neighbor Discovery (ND) protocol as supported on the SmartEdge router and describes the tasks used to configure, monitor, and administer the ND protocol. This document also provides ND protocol configuration examples.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

Note: When IP version 6 (IPv6) addresses are not referenced or explicitly specified, the term IP address can refer generally to IP version 4 (IPv4) addresses, IPv6 addresses, or IP addressing. In instances where IPv6 addresses are referenced or explicitly specified, the term, IP address, refers only to IPv4 addresses. For a description of IPv6 addressing and the types of IPv6 addresses, see RFC 3513, *Internet Protocol Version 6 Addressing Architecture*.

The SmartEdge router employs the ND protocol, an IPv6 Internet standard protocol used between neighboring routers and between a router and connected host devices within an IPv6 environment. IPv6 hosts and routers on the same link use the ND protocol to:

- Determine each other's link-layer addresses.
- Purge cached values that are no longer valid.
- Maintain reachability information between neighbors.
- Detect changed link-layer addresses.

Hosts use ND to find routers that can forward packets for them and to search for functioning alternative paths when a router or a path to a router is no longer available.

ND performs the following core functions in an IPv6 environment:

- Router discovery: Allows hosts to find routers on an attached link.

- Prefix discovery: Allows hosts to discover the set of address prefixes that define which destinations are on-link for an attached link. ND gets IPv6 prefixes from:
  - The Framed-IPv6-Prefix attribute, which can be configured statically or by using the Framed-IPv6-Prefix RADIUS attribute.
  - A shared IPv6 prefix pool.

  Note: For details about shared IPv6 prefix pools and using ND for IPv6 subscriber services, see *Configuring IPV6 Subscriber Services*.
- Parameter discovery: Provides nodes a way of learning link parameters or Internet parameters to place in outgoing packets.
- Address autoconfiguration: Provides nodes the ability to configure an address for an interface in a stateless method. This function is explained in more detail in Section 1.2 on page 3.
- Address resolution: Allows nodes to learn of the link-layer address of a neighbor's destination given only the destination's IP address.
- Next-hop determination: The algorithm for mapping an IP destination address into the IP address of the neighbor to which traffic for the destination should be sent. The next-hop can be a router or the destination itself.
- Neighbor unreachability detection: Provides nodes the ability to determine that a neighbor is no longer reachable.
- Duplicate address detection: Allows a node to determine whether an address it has been assigned to use is already in use by another node. This is explained in more detail in Section 1.3 on page 4.
- Redirect: Enables a router to inform a host of a preferable first-hop node to reach a destination.

The IPv6 ND protocol for the SmartEdge router corresponds to a combination of the IPv4 Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) Router Discovery Protocol (IRDP). The ND protocol is described in RFC 4861, *Neighbor Discovery for IP Version 6*.

1.1 ND Support

The ND protocol on the SmartEdge router supports both IPv6 subscriber and nonsubscriber circuits on an IPv6 interface. Each type of support is configured differently. ND parameters do not require explicit configuration; default values are used for parameters not explicitly configured.

For ND subscriber circuits, you can configure ND parameters in an ND profile in a context and then assign this ND profile to a subscriber record by specifying the name of the profile in this record. When the subscriber circuit is brought up,

the ND profile is applied to the subscriber circuit, and ND communications on this subscriber circuit use the ND parameters configured in the ND profile.

You can define multiple ND profiles, each containing different ND parameter settings, to allow different ND attributes to be applied among different sets of subscriber circuits on the same interface. Keep the following in mind about ND support for IPv6 subscriber circuits:

- Changes to an ND profile automatically take effect on subscriber circuits using that profile.
- IPv6 subscriber records do not have to refer to an ND profile. In that case, a default ND profile (GLOBAL_DEFAULT_PROFILE) is assigned by ND to that subscriber circuit.
- Only one ND profile can be assigned to a subscriber circuit.
- ND profiles are context-specific, so a subscriber must be associated with the same context the profile is associated with before the profile can be used.
- Multiple ND profiles using different ND parameter values can be configured under a context. A SmartEdge router supports up to 4,095 ND profiles.

For ND nonsubscriber circuits, you can configure ND parameters on an interface enabled for IPv6. ND communications on this nonsubscriber circuit use the ND parameters configured on the interface.

Note: ND support for nonsubscriber circuits is also referred to as *ND router* in SmartEdge router documentation.

For conceptual and configuration information about the IPv6 subscribers that the SmartEdge router supports, see *Configuring IPV6 Subscriber Services*.

1.2 IPv6 Stateless Address Autoconfiguration

Note: The IPv6 Stateless Address Autoconfiguration (SLAAC) protocol is supported only on IPv6 subscriber circuits.

The IPv6 SLAAC protocol allows hosts connected to a SmartEdge router to automatically configure their global addresses used on the interface that is connected to the router. No manual configuration of hosts is required. SLAAC is achieved by allowing the host to generate its own address using the algorithm defined in the RFC 4862, *IPv6 Stateless Address Autoconfiguration*. To ensure the address of the host is unique on a link and is not used by another host, Duplicate Address Detection (DAD) is performed on this new address before the host is actually assigned the address.

SLAAC requires the SmartEdge router to perform the router responsibilities to allow hosts to autoconfigure their global IPv6 addresses on an interface. The ND protocol is used to advertise a variable-length IPv6 prefix (typically 64 bits),

or group of prefixes, to the host. The host, in turn, appends its interface ID to this prefix to configure the interface address for that link. The SmartEdge router uses the following ND messages for SLAAC:

- Router Solicitation (RS) message—This message is sent by the host to solicit the attached router (SmartEdge router) to immediately send a Router Advertisement (RA) message. The message is sent to the all-routers multicast address.
- Router Advertisement (RA) message—The SmartEdge router sends this message to the host, both periodically and in response to an RS message transmitted by the host. When SLAAC is enabled for a subscriber circuit, which automatically occurs after an IPv6 prefix is assigned to the subscriber, the following takes place:
  - The RA message advertises one or more variable-length IPv6 prefixes that can be used by the host for subscriber circuits.
  - The RA message enables the Autonomous flag bit (A=1).

  To create a unique 128-bit global unicast address for the subscriber circuit to use, the host appends it's own interface identifier to this prefix .

The IPv6 prefixes advertised in the RA messages must be assigned to the IPv6 subscribers by configuring the associated subscriber records. You can assign up to 100 prefixes for each IPv6 subscriber. The prefix configuration within a subscriber record allows SLAAC to be enabled for that subscriber. If there are no prefixes assigned to the subscriber, then SLAAC remains disabled for that subscriber.

1.3 Duplicate Address Detection

Note: Duplicate address detection (DAD) is supported on both IPv6 subscriber and nonsubscriber circuits.

DAD is performed by all ND nodes (routers and hosts) to verify that no other node is using either the link-local or global IP addresses of the ND node prior to assigning them to a local IPv6 interface. DAD must occur before the IPv6 address can be used.

Note: RFC 4862, *IPv6 Stateless Address Autoconfiguration*, states that after joining a multicast address, the node should send a multicast listener discovery (MLD) report message for that address, if MLD-snooping switches exist in the network. It is assumed that MLD-snooping switches are not present in the network in which the SmartEdge router is deployed. The SmartEdge router does not send MLD report messages.

By default, DAD is enabled in the default ND profile using the **`dad-transmit`** command. This command is enabled by default with a value of 1 and is used to configure the number of NS messages the SmartEdge router sends to its

peers to perform DAD. You can disable DAD by setting the number of NS message transmissions to 0.

The following ND messages are used to perform DAD:

- Neighbor solicitation (NS) message: The host transmits this message a configurable number of times (default is 1) to the solicited-node multicast address before the IPv6 address can be used on the associated circuit. During this time, the address is considered to be in a tentative state, and is not in use. The target address is included in the NS message, with the IP source address set to all zeros (an unspecified address). The unspecified address identifies this message as reserved for DAD. If no other node responds to this query, the address is unique on that circuit and can be applied to the interface.

- Neighbor Advertisement (NA) message: The SmartEdge router (or host) transmits an NA message in response to a DAD NS message only if the target address in the message matches either the link-local or global IP address assigned to that interface on the SmartEdge router. The match indicates that some host is trying to use the same address. The NA message notifies the host (or SmartEdge router) that a misconfiguration has occurred, which must be addressed in the router.

  The SmartEdge router performs the DAD process in two ways:

  – DAD is first performed on the link-local address of the SmartEdge router and the global unicast address of the interface that is bound to the circuit before these addresses are considered valid.

  – The SmartEdge router also listens for DAD NS messages sent by other nodes, and if the target address in this message represents one of its own interface addresses, the router responds with an NA message informing the requester that its tentative address is a duplicate address.

By default, an error message is logged after a DAD is detected. The log provides information about the duplicate address and the impacted circuit. You can resolve the duplicate address issue by enabling the SmartEdge router to send a request to bring down the associated IPv6 stack by configuring the **`proto-down-on-dad`** command in the ND profile. If the subscriber circuit consists of only an IPv6 stack (without an IPV4 stack), then the entire subscriber circuit is brought down.

2 Configuration and Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see *Command List*.

2.1 Configuration and Operations Tasks for Subscriber Circuits

Table 1 and Table 2 provide information on how to configure ND-related features for IPv6 subscribers or subscriber circuits. Table 5 provides information on how to monitor and troubleshoot ND features for IPv6 subscriber circuits. Perform the configuration and operations tasks in the order presented.

For information about configuring IPv6 subscribers, see *Configuring IPV6 Subscriber Services*.

2.1.1 Configuring an ND Profile (for IPv6 Subscribers)

By default, ND assigns a default ND profile to each IPv6 subscriber circuit. The default ND profile contains ND parameters with default values assigned to each. If you want to customize specific ND parameters (for example, an RA lifetime of 20,000 seconds) to use, explicitly configure an ND profile. Configuring ND profiles for IPv6 subscribers is optional. To configure an ND profile, perform the tasks described in Table 1; enter all commands in ND profile configuration mode, unless otherwise noted.

Table 1 Configure an ND Profile (for IPv6 Subscribers)

Step	Task	Root Command	Notes
1.	Create or select the context in which to apply the ND profile.	*context*	Enter this command in global configuration mode.
2.	Create the ND profile and access ND profile configuration mode.	*nd profile*	Enter this command in context configuration mode.
3.	Optional. Configure ND parameters for the ND profile by performing one or more of the following tasks, in any order:		
3a.	Optional. Specify the number of NS messages the SmartEdge router sends to its peers for DAD.	*dad-transmits*	

Table 1 Configure an ND Profile (for IPv6 Subscribers)

Step	Task	Root Command	Notes
3b.	Optional. Specify a value for the Retrans Timer field, which is the length of time between retransmitted NS messages.	*ns-retry-interval*	
3c.	Optional. Specify a value for the Preferred Lifetime field, which is the length of time (in seconds) that the IPv6 address generated from an IPv6 prefix remains preferred.	*preferred-lifetime*	
3d.	Optional. Enable the SmartEdge router to send a request to bring down the IPv6 stack of the subscriber circuit in which a DAD failure is detected.	*proto-down-on-dad*	
3e.	Optional. Configure options and settings for RA messages.	*ra-interval* *ra-lifetime* *ra-managed-config* *ra-on-link* *ra-other-config*	You can enter this command multiple times to configure different parameters.
3f.	Optional. Specify a value for the Valid Lifetime field, which is the length of time that an IPV6 prefix is valid for on-link determination.	*valid-lifetime*	

2.1.2 Assigning an ND Profile and an IPv6 Prefix to an IPv6 Subscriber Record

By default, a default ND profile is assigned to an IPv6 subscriber. If you want to assign an ND profile other than the default to an IPv6 subscriber, perform the tasks described in Table 2. An ND profile must exist before you can assign it to a record.

Table 2 Assigning an ND Profile and an IPv6 Prefix to an IPv6 Subscriber Record

Step	Task	Root Command	Notes
1.	Create or select the context for the ND router.	*context*	Enter this command in global configuration mode.
2.	Create a named subscriber record to be associated with the IPv6 subscriber.	*subscriber*	Enter this command in context configuration mode. Use the `name` keyword with the `subscriber` command.
3.	Configure the IPv6 framed prefix to be used by the subscriber. ND advertises this prefix in an RA message.	*ipv6 framed-prefix*	Enter this command in subscriber configuration mode. Replace the ***ipv6-prefix*** argument with a unique prefix, which is not assigned to any another subscriber or is not part of the interface ipv6 address.
4.	Assign an ND profile to the subscriber using the subscriber record.	*ipv6 nd profile*	Enter this command in subscriber configuration mode.

2.1.3 Configuring Router to Limit the Effect of ND Packet DoS Attacks

To configure the router to limit the effect of ND packet Denial of Service (DoS) attacks on a circuit, enter the **`rate limit circuit nd`** command as described in Table 3.

Table 3 Configure Router to Prevent DoS Attacks

Task	Root Command	Notes
Optional. Enable rate limiting ND packets on the circuit to prevent DoS attacks. Specify the number of packets allowed on each circuit, the interval during which the system counts the packets, and the drop-interval during which during which packets are dropped, if the allowed number of messages was exceeded in the previous interval.	*rate-limit circuit nd*	Enter the command in global configuration mode. Rate limiting is performed on ND packets coming on every circuit (virtual circuit in the case of PPPoE) even though it is configured on the parent circuit at the card level. It supports access link groups but not Ethernet or 802.1Q link groups.

2.1.4 Configuring a Traffic Card to Limit the Effect of ND Packet DoS Attacks

To configure a traffic card to limit the effect of ND packet DoS attacks, enter the **`rate-limit nd`** command as described in Table 4.

Table 4 Configure a Traffic Card to Prevent DoS Attacks

Task	Root Command	Notes
Enable rate limiting and specify the rate and burst limits for ND packets.	*rate-limit nd*	Enter this command in card configuration mode.

2.1.5 ND Operations Tasks for IPv6 Subscriber Circuits

To monitor and troubleshoot ND features for IPv6 subscriber circuits, perform the ND operations tasks described in Table 5. Enter the **`debug`** command in exec mode; enter the **`show`** commands in any mode.

Table 5 ND Operations Tasks for IPv6 Subscriber Circuits

Task	Root Command	Notes
Enable the generation of debug messages for ND events.	*debug nd*	
Enable the generation of debug messages for IPv6 subscribers.	*debug nd*	Use the **`subscriber`** keyword with this command to enable debug messages for IPv6 subscribers.
Display ND circuit information for one or more ND circuits.	*show nd circuit*	
Display ND interface information for one or more ND routers.	*show nd interface*	
Display ND profile information for a context.	*show nd profile*	
Display ND packet statistics on a specified interface.	*show nd statistics*	Use the **`interface`** ***`if-name`*** construct to specify an interface.

2.2 Configuration and Operations Tasks for Nonsubscriber Circuits

Table 6 and Table 7 provide information on how to configure ND-related features for IPv6 nonsubscriber circuits. Table 8 provides information on how to monitor and troubleshoot ND features for IPv6 nonsubscriber circuits. Perform the configuration and operations tasks in the order presented.

To configure an ND router, perform the tasks described in Table 6; enter all commands in ND router configuration mode, unless otherwise noted.

Table 6 Configuring an ND Router

Step	Task	Root Command	Notes
1.	Create or select the context for the ND router.	*context*	Enter this command in global configuration mode.
2.	Create the interface for the ND router.	*interface*	Enter this command in context configuration mode.
3.	Specify an IPv6 IP address for the interface.	*ipv6 address*	Enter this command in interface configuration mode.
4.	Create the ND router and access ND router configuration mode.	*router nd*	Enter this command in context configuration mode.
5.	Optional. Configure global settings for the ND router by performing one or more of the following tasks, in any order:		
5a.	Optional. Configure the hop limit (the maximum number of routers that IPv6 traffic can traverse) advertised in ND RA messages sent by the router.	*hop-limit*	The range of values is 0 to 255. A value of 0 means no hop limit is specified.
5b.	Optional. Specify a value for the Retrans Timer field, which is the time between retransmitted NS messages.	*ns-retry-interval*	
5c.	Optional. Specify a value for the Preferred Lifetime field, which is the length of time (in seconds) that the IPv6 address generated from an IPv6 prefix remains preferred.	*preferred-lifetime*	
5d.	Optional. Configure options and settings for RA messages.	*ra*	You can enter this command multiple times to configure different parameters.

Table 6 Configuring an ND Router

Step	Task	Root Command	Notes
5e.	Optional. Specify a value for the Reachable Time field, which is the length of time this ND router or ND router interface assumes that a neighbor is reachable.	*reachable-time*	
5f.	Optional. Specify a value for the Valid Lifetime field, which is the length of time that an IPV6 prefix is valid for the purpose of on-link determination.	*valid-lifetime*	

To configure an interface for an ND router, perform the tasks described in Table 7; enter all commands in ND router interface configuration mode, unless otherwise noted.

Table 7 Configuring an ND Router Interface

Step	Task	Root Command	Notes
1.	Select the context for the ND router.	*context*	Enter this command in global configuration mode.
2.	Select the ND router and access ND router configuration mode.	*router nd*	Enter this command in context configuration mode.
3.	Select an existing interface and access ND router interface configuration mode.	*interface (ND)*	Enter this command in ND router configuration mode.
4.	Optional. Configure the settings for this interface by performing one or more of the following tasks, in any order:		Unspecified settings default to the ND router global settings.
4a.	Optional. Configure the hop limit (the maximum number of routers IPv6 traffic can traverse) advertised in ND RA messages sent by this interface.	*hop-limit*	The range of values is 0 to 255. A value of 0 means no hop limit is specified.

Table 7 Configuring an ND Router Interface

Step	Task	Root Command	Notes
4b.	Optional. Specify a value for the Preferred Lifetime field, which is the length of time (in seconds) that the IPv6 address generated from an IPv6 prefix remains preferred.	*preferred-lifetime*	
4c.	Optional. Configure options and settings for RA messages.	*ra*	You can enter this command multiple times to configure different parameters.
4d.	Optional. Specify the value for the Reachable Time field, which is the length of time this ND router or ND router interface assumes that a neighbor is reachable.	*reachable-time*	
4e.	Optional. Specify a value for the Valid Lifetime field, which is the length of time that an IPV6 prefix is valid for the purpose of on-link determination.	*valid-lifetime*	
5.	Specify a static neighbor for this interface.	*neighbor*	You can enter this command multiple times.
6.	Configure a prefix to be advertised for this interface.	*prefix*	You can enter this command multiple times.

To monitor and troubleshoot ND features for the ND router, perform the ND operations tasks described in Table 8. Enter the **`debug`** command in exec mode; enter the **`show`** commands in any mode.

Table 8 ND Router Operations Tasks

Task	Root Command
Enable the generation of debug messages for ND events.	*debug nd*
Display the current ND configuration.	*show nd interface*
Display neighbor information for one or more ND router interfaces.	*show nd neighbor*
Display prefix information for one or more ND router interfaces.	*show nd prefix*

Table 8 ND Router Operations Tasks

Task	Root Command
Display static-neighbor information for one or more ND router interfaces.	*show nd static-neighbor*
Display global statistics for one or more ND router interfaces.	*show nd statistics*
Display summary information for the ND router global settings.	*show nd summary*

3 Configuration Examples

The following example shows how to configure ND for IPv6 subscribers by configuring ND profiles, assigning these profiles to the subscriber records, and specifying IPv6 framed prefixes in the subscriber records that ND advertises in its RA messages:

Create or select the context; both IPv6 subscriber records and the ND profiles to be applied to these records must reside within the same context.

```
[local]Redback(config)#context local
```

The following four commands do not pertain specifically to ND and are provided here for completeness. ND uses part of the IPv6 address assigned to a multibind interface when it advertises RA messages. Create a multibind interface for the IPv6 subscriber sessions and assign an IPv6 address to this interface.

```
[local]Redback(config-ctx)#interface v6-intf-multi multibind
[local]Redback(config-if)#ip address 20.10.20.10/24
[local]Redback(config-if)#ipv6 address 2001:a:b::/48
[local]Redback(config-if)#exit
```

Configure the ND profile and its parameters. This configuration is optional. In this example, three ND profiles are created, each with its own set of ND parameters to apply to the associated IPv6 subscriber circuits.

```
[local]Redback(config-ctx)#nd profile ndpro1
[local]Redback(config-nd-profile)#preferred-lifetime 3600
[local]Redback(config-nd-profile)#dad-transmits 3
!
[local]Redback(config-ctx)#nd profile ndpro2
[local]Redback(config-nd-profile)#ra-interval 120
!
[local]Redback(config-ctx)#nd profile ndpro3
[local]Redback(config-nd-profile)#proto-down-on-dad
!
[local]Redback(config-ctx)#nd profile ndpro4
[local]Redback(config-nd-profile)#preferred-lifetime 2400
[local]Redback(config-nd-profile)#dad-transmits 2
[local]Redback(config-nd-profile)#ra-managed-config
[local]Redback(config-nd-profile)#proto-down-on-dad
```

In the same context in which the multibind interface is configured, configure the subscriber records for the IPv6 subscribers, specifying the configured ND profile and assigning IPv6 prefixes.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#subscriber name subscriber1
[local]Redback(config-sub)#password test
[local]Redback(config-sub)#ip address 20.10.20.100
[local]Redback(config-sub)#ppp mtu 1000
```

Specify the IPv6 framed prefix to be used by the named IPv6 subscriber (in this case, subscriber1).

```
[local]Redback(config-sub)#ipv6 framed-prefix  2001:a:b:1::/64
```

Note: Each subscriber must have a unique prefix. ND advertises this prefix in the RA messages. This prefix in the subscriber record enables Stateless Address Autoconfiguration (SLAAC) for this subscriber

Specify the ND profile to be applied to the subscriber. (In this case, the ND profile ndpro1 is applied to subscriber1.) You can only apply one profile for each subscriber. This configuration is optional. By default, each subscriber is assigned a default ND profile to use for its IPv6 session.

```
[local]Redback(config-sub)#ipv6 nd-profile ndpro1
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#subscriber name subscriber2
[local]Redback(config-sub)#password test
[local]Redback(config-sub)#ip address 20.10.20.101
```

Configure the IPv6 framed-prefix to be used by the named subscriber (in this case, subscriber2).

```
[local]Redback(config-sub)#ipv6 framed-prefix 2001:a:b:2::/64
```

Specify the ND profile to be applied to the subscriber (in this case, the ND profile ndpro4 is to be applied to subscriber2).

```
[local]Redback(config-sub)#ipv6 nd-profile ndpro4
[local]Redback(config-sub)#exit
```

The following example shows how to configure an ND router in the **local** context and the **int1** interface for the ND router:

Create or select the context.

```
[local]Redback(config)#context local                                    //NOTE 1
```

Create the interface with an IPv6 IP address.

```
[local]Redback(config-ctx)#interface int1                               //NOTE 2
[local]Redback(config-if)#ipv6 address 2005::1/64
[local]Redback(config-if)#exit
```

Create the ND router; specify global parameters for all ND interfaces in this context. The global settings override the default settings.

```
[local]Redback(config-ctx)#router nd                                    //NOTE 3
[local]Redback(config-nd)#ns-retry-interval 100
[local]Redback(config-nd)#preferred-lifetime 43200
[local]Redback(config-nd)#ra interval 60
[local]Redback(config-nd)#ra lifetime 360
[local]Redback(config-nd)#reachable-time 1800
[local]Redback(config-nd)#valid-lifetime 43200
```

Select an interface.

```
[local]Redback(config-nd)#interface int1                                    //NOTE 4
```

Specify interface-specific parameters; the interface settings override the global settings.

```
[local]Redback(config-nd-if)#ns-retry-interval 20                           //NOTE 5
[local]Redback(config-nd-if)#preferred-lifetime 2880
[local]Redback(config-nd-if)#ra suppress
[local]Redback(config-nd-if)#valid-lifetime 2880
```

Specify one or more static neighbors for this interface.

```
[local]Redback(config-nd-if)#neighbor 2006::1/64 00:30:88:00:0a:3           //NOTE 6
```

Specify one or more prefixes and their parameters; the prefix settings override the interface settings.

```
                                                                            //NOTE 7
[local]Redback(config-nd-if)#prefix 2006::1/64 no-autoconfig no-onlink preferred-lifetime 360
valid-lifetime 360
[local]Redback(config-nd-if)#prefix 2007::/112
[local]Redback(config-ctx)#
```

Glossary

ARP
Address Resolution Protocol

DAD
Duplicate Address Detection

DoS
Denial of Service

ICMP
Internet Control Message Protocol

IPv4
IP version 4

IPv6
IP version 6

IRDP
(ICMP) Router Discovery Protocol

NA
Neighbor Advertisement

ND
Neighbor Discovery

NS
Neighbor solicitation

RA
Router Advertisement

RS
Router Solicitation

SLAAC
Stateless Address Autoconfiguration