Off-link prefixes vs. neighbor discovery protocol

Protocol or configuration issue?

Off-link prefixes

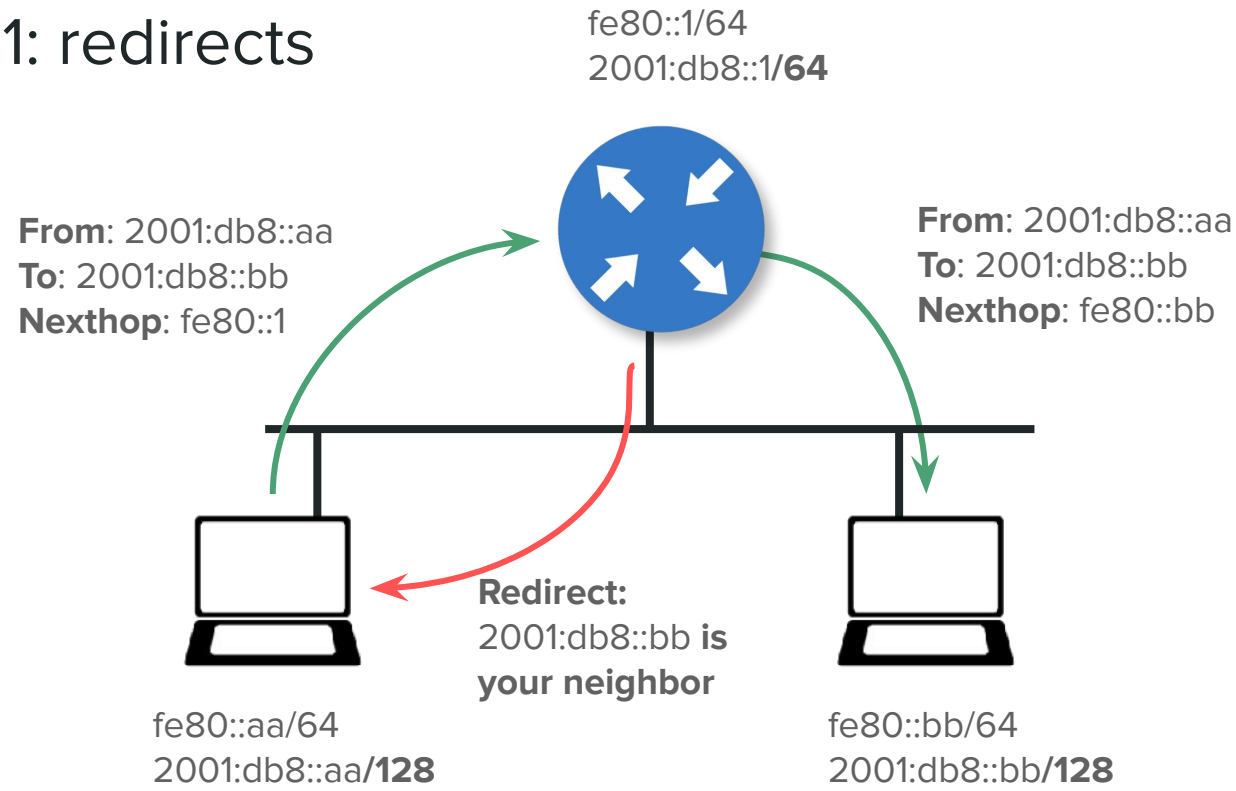
- Announced in RAs with **L=0**
- Do not create “**connected route**” of surrounding /64
- Everything is being **sent to the default gateway**
- Allows **controlled client-to-client communication** via the gateway even if direct communication is **blocked by L2 infrastructure**

RA:
Router: fe80::1
PIO: 2001:db8::/64 A=1 L=0

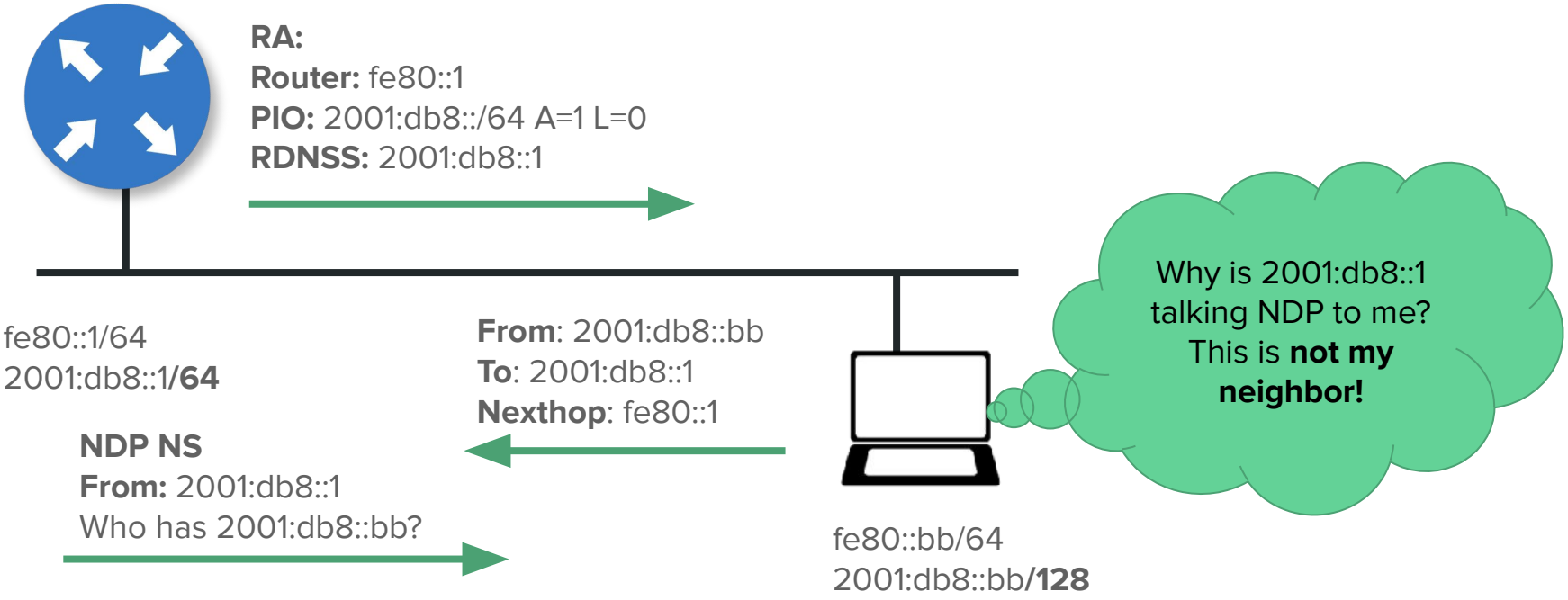
Interface:
2001:db8::1234:5678:9abc:def0**/128**

Routing table:
default via fe80::1 dev eth0

Issue 1: redirects



Issue 2: talking to the gateway



What RFC 4861 says

Section 8.2

A router **SHOULD** send a redirect message, whenever it forwards a packet that is not explicitly addressed to itself in which:

- the Source Address field of the packet **identifies a neighbor**, and
- better first-hop node **resides on the same link** as the sending node for the Destination Address of the packet being forwarded, and
- the Destination Address of the packet is not a multicast address.

Section 7.2.2

If the source address of the packet prompting the solicitation is the same as one of the addresses assigned to the outgoing interface, that address **SHOULD be placed in the IP Source Address** of the outgoing solicitation. Otherwise, any one of the addresses assigned to the interface should be used. Using the prompting packet's source address when possible ensures that the recipient of the Neighbor Solicitation **installs in its Neighbor Cache** the IP address that is highly likely to be used in **subsequent return traffic** belonging to the prompting packet's "connection".

Possible fixups in RFC 4861

- A router SHOULD provide means to prevent emitting Redirect messages on a particular interface
- A router SHOULD always use Link-local address for outgoing neighbor solicitation messages

Questions

- Should this be fixed in the protocol?
- Or is talking to vendors enough?
- Or maybe recommendation not to ever use router addresses in off-link segments?