IPv6 access security

IPv6 is in the core. How do you get it to the edge?

Jussi Peltola
Dynaco Oy

2011-09-16

Requirements for access

- Client isolation: no DoS, eavesdropping or other unwanted interactions
- Non-repudiation (blame) - Traffic originated must be traceable to the client (uRPF, ip source-guard, DHCP logs)
- End-user host autoconfiguration (DHCP, SLAAC) - often desired for servers, too.

Essential IPv6

ARP	NDP
CIDR	Classless addressing in the protocol, classful address policies
DHCP	DHCPv6 and Router Announces
	Link-local addresses

NDP DoS - the weakness

Not a new issue in itself - bloated IPv4 subnets are known to be problematic.

A /64 is immense compared to a /24 or /16 (or the whole IPv4 space.)

A /16 may fit in a modern router's ARP cache. A /64 will never* fit in any ND cache.

A single /64 interface on a router will make it vulnerable to NDP DoS.

* Not any time soon, anyway

NDP DoS - the weakness

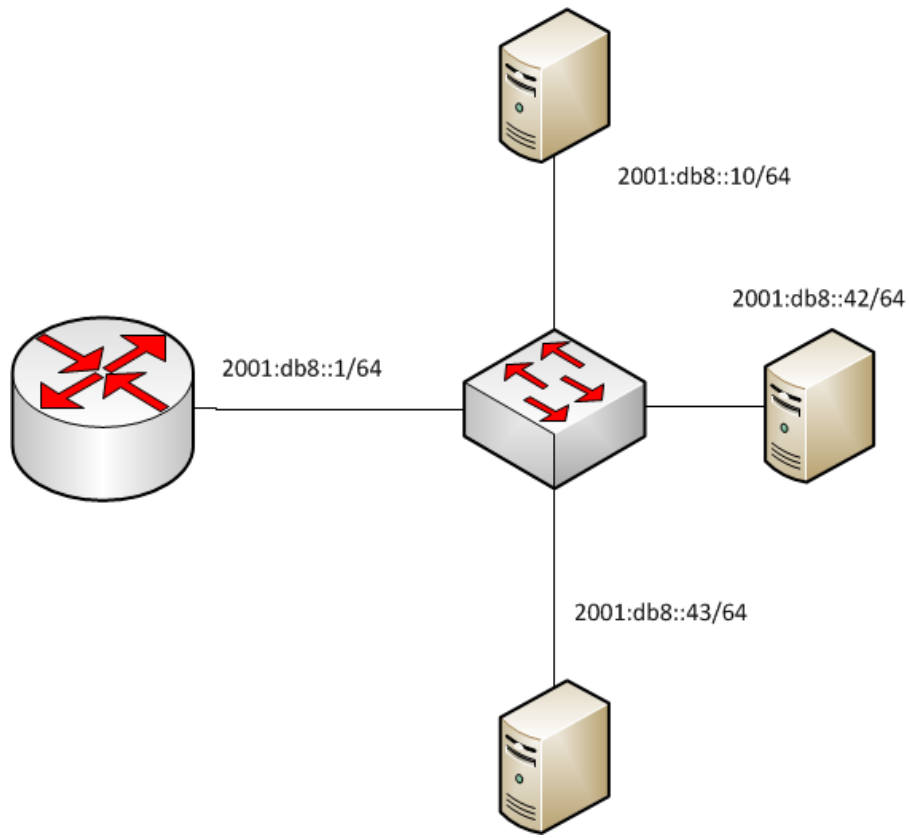
Routers process NDP in the control plane CPU, which needs to be rate limited - otherwise the whole CPU is susceptible to DoS. This global rate limit is usually rather high, in the thousands of pps.

Routers also have limited resources to store ND entries - with IPv4 these limits are usually not reached. Not so with /64s.

On some routers the ND resolver and table are shared with ARP - the whole router, including IPv4, can come crashing down because of a DoS against a single /64 interface.

NDP DoS - "scan" attack

```
IP6 2001:db8:42::dead:beef > 2001:
db8::3dcc:727e:32fc: ICMP6, echo
request, seq 670, length 64
IP6 2001:db8:42::dead:beef > 2001:
db8::bb93:ee63:78bc: ICMP6, echo
request, seq 621, length 64
IP6 2001:db8:42::dead:beef > 2001:
db8::67ff:f3fa:0b77: ICMP6, echo
request, seq 195, length 64
IP6 2001:db8:42::dead:beef > 2001:
db8::b1fa:abc0:d04d: ICMP6, echo
request, seq 208, length 64
IP6 2001:db8:42::dead:beef > 2001:
db8::be61:5805:1a63: ICMP6, echo
request, seq 432, length 64
```



NDP DoS - "scan" attack

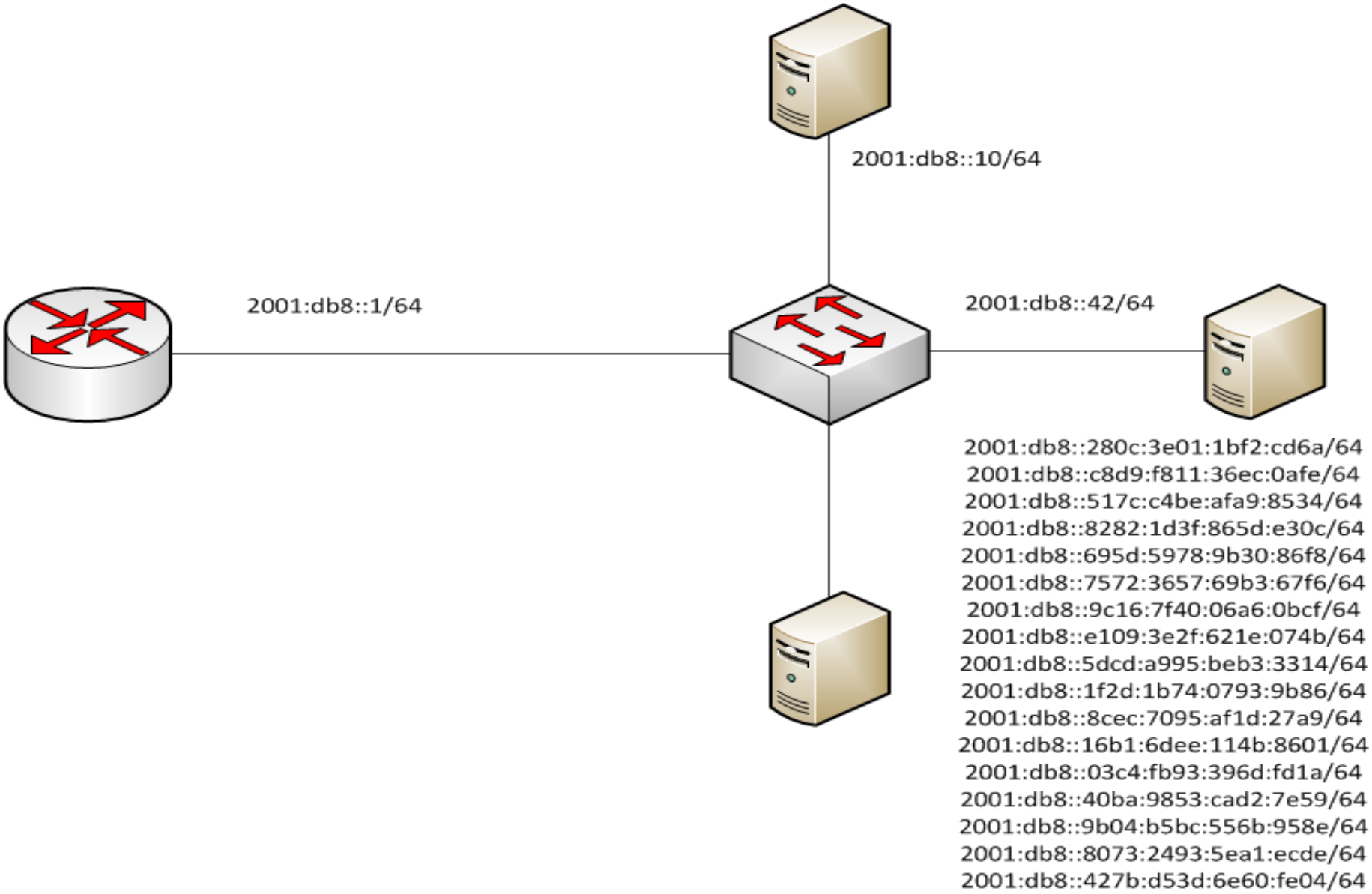
Even if ND resolving was implemented in hardware at line-rate, talking to nonexistent hosts would create a multicast flood.

The router has to queue packets to non-resolved nexthops - this queue always has some limit.

Because of this the control plane has a per-destination policer. It works well - until you have a subnet so large that you can't keep state for every address.

Routers have different failure modes when this happens. All degrade in some way.

NDP DoS - "proxy ND" attack



NDP DoS - "proxy ND" attack

If there is a naive proxy ND responder, or a malicious attacker, in a /64, the ND table fills up. The entries will stick for the ND timeout, which is usually quite long.

Routers age out valid ND entries after a timeout. Some have a race condition that allows the ND entry slot to be used up by a new entry before the live one has been refreshed.

With time, it's highly probable that "real" ND entries will be evicted and replaced with the bogus ones.

NDP DoS - solutions

A very obvious solution is to not use /64 - this is common practice especially on point-to-point links.

Typically a /64 is allocated, but only the least significant bits are used - this allows unlimited growing of the subnet if more hosts are needed, and gives convenient addresses.

The downside is that this breaks stateless autoconfig, which requires a /64 subnet. This is OK for datacenter access, but can be problematic for end-user access - static addressing will not work for coffee shops and consumer ISPs.

NDP DoS - solutions

Stateful firewalls that only allow inbound traffic to a limited number of addresses will protect against outside DoS.

- Helps routed CPEs and private networks
- Will not help against a "proxy ND" attack from the inside.

Stateful DHCPv6 with DHCPv6 snooping will prevent the "proxy ND" attack by limiting hosts to some reasonable number of addresses.

NDP DoS - solutions

The DoS can be mitigated (but not perfectly) with router behavior:

- Per interface ND rate limit ("scan" containment)
- Per interface ND entry limit ("proxy ND" containment)
- Per interface ND entry reservation (preferably default!)
  - Useful to keep some ND space for core-facing links
- Per MAC ND entry limit (proxy ND containment)
  - combine with port security.
- Priority to preexisting and static ND entries when table is full
- Priority to nexthops / routing protocol neighbors

Rogue RAs

DHCPv6 has no provision for giving clients a default route, and an ICMPv6 message of type Router Advertisement is used instead. The only other option is static configuration.

RAs have no authentication, so rogue RAs pose a similar problem as rogue DHCP.

Rogue RAs are worse: a single RA packet will immediately point all the machines in the LAN to the new router, and install a new IPv6 address on their stacks.

Rogue RAs

Some consumer devices send RAs by default:

- Windows machines with Internet Connection Sharing
- Some Apple AirPorts, etc.

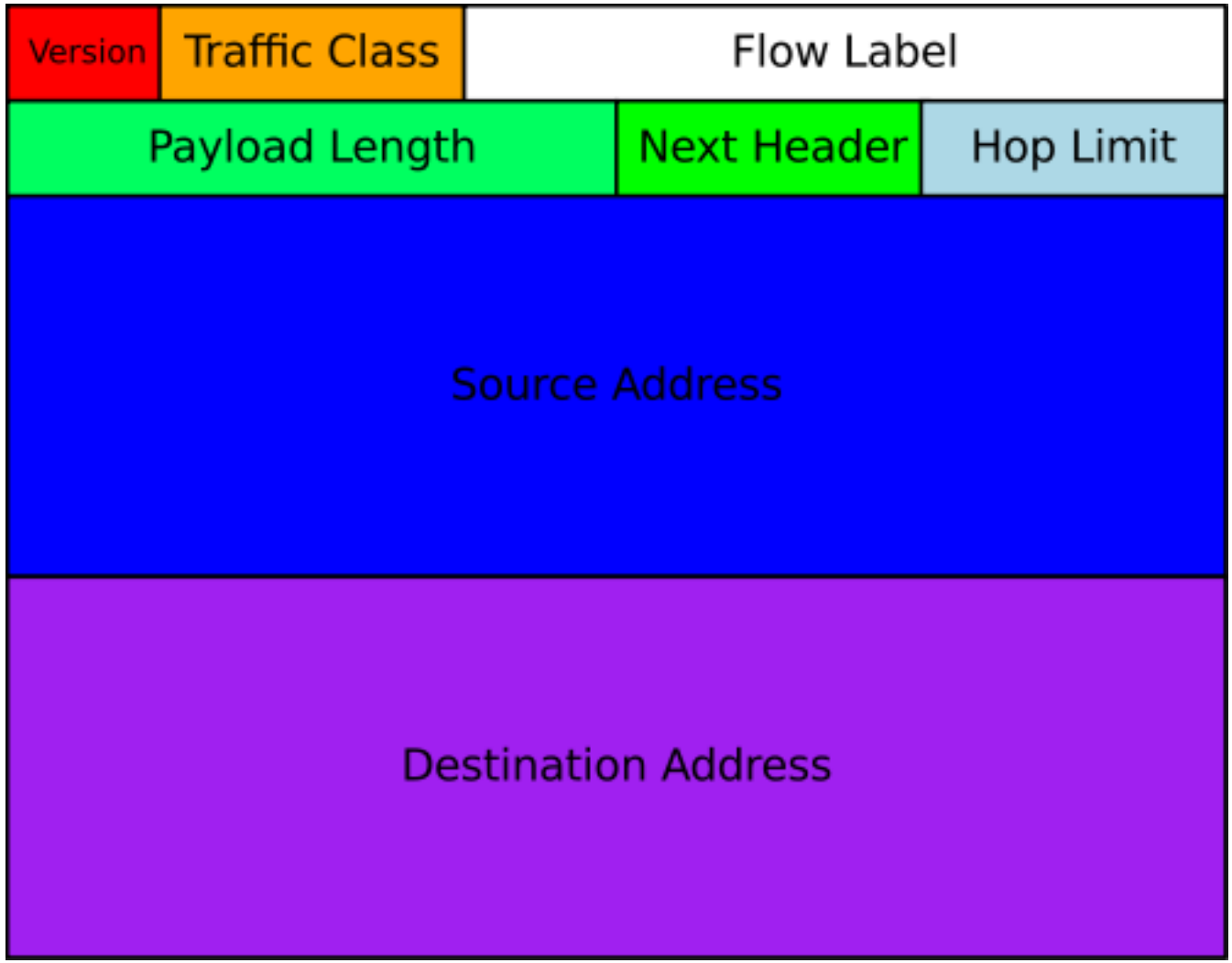
Accidental rogue DHCP is rarer, except consumer routers.

Mitigation:

- Provide native IPv6 with RA priority to the max
- RA guard (L2 switch filter)
- Private VLANs and other L2 containment techniques.

Coffee shops with a cheap WLAN access point seem to be out of luck. Large campus and university LANs are also in trouble, needing to replace all their switches to support RA guard.

Header chain ACL evasion



Header chain ACL evasion

IPv6 has an extensible header chaining mechanism with the Next Header field.

HW router platforms only look at the beginning of a packet. End hosts don't have such limits.
By chaining sufficiently many extra headers before the TCP, UDP or other header, stateless ACLs can be bypassed.

Expect many exciting discoveries with different end hosts and ACL implementations.

Access topologies - L3 per customer

- VLAN / L3 interface and subnet per customer
- Works. Provides separation, blame and the most flexibility with autoconfiguring end hosts. Watch out for NDP DoS.

```
ipv6 route 2001:db8:1000::/48 2001:db8:1:42::2

interface FastEthernet 1/1
  ipv6 address 2001:db8:1:42::1/126
  ipv6 verify unicast reverse-path
  ip address ?.?.?.? !.!.!.!
  ip helper address 192.0.2.1
  ip verify unicast reverse-path
  no ip proxy-arp
```

Access topologies - L3 per customer

Problems:

- Invasive surgery on existing networks
- Administrative overhead
- Router resource consumption
- VLAN count limits in intermediate switches
- Difficulties with dual-stacking: IPv6 is vlan per customer, preexisting IPv4 is shared subnet.
  - Unnumbered subinterfaces work for this if supported
  - Protocol based VLANs are also a possibility

Benefits:

- VLAN per customer allows for cheap & cheerful L2 access switches - or at least postpones replacement of the existing ones.

Access topologies - shared L2

- The way it's commonly done in IPv4
- Requires support from L2 devices: DHCP snooping, IP source guard and private VLANs are satisfactory when all three are combined. RA guard is also needed unless private VLANs are used.
- These features need hardware support for IPv6 and are scarce even in new equipment. Some devices may be flexible enough for implementation with a software upgrade - will the vendors want that?
- If you want to allow your residential customers the joy of routed allocations, the L2 devices' filters and relay agents should understand DHCP prefix delegation.

Access topologies - shared L2

- In practice, L2 devices that support RA guard are not too common, and DHCPv6 snooping is implemented by just a few vendors.
- If we want IPv6 any time soon, asking everyone to replace their whole access network is not going to help.
- Rogue RAs are pushing some people to upgrade for RA guard - but will they need to upgrade again to get the rest of the features they need?

?

plz@plz.fi