31. IPv6 on Hosts

NEIGHBOR DISCOVERY PROTOCOL (NDP)

NDP uses ICMPv6 messages to define several functions:

- SLAAC (StateLess Address Auto-Configuration)—Tells a host its network prefix and the prefix length. *We'll talk about this last.*
- Router Discovery—Tells a host the addresses of IPv6 routers on the LAN.
- DAD (Duplicate Address Detection)—Tells a host that their new IPv6 address is not already in use.
- Neighbor MAC Discovery—replaces ARP for learning MAC addresses within the LAN.

Neighbor—any device on the same LAN (VLAN), also called a "link."

ROUTER DISCOVERY

A pair of ICMPV6 messages allow hosts to learn the addresses of any local routers. This is a good example of how IPv6 uses multicasts to achieve the LAN-wide distribution of a broadcast without impacting every device on the LAN. In the case of an RS, non-routers aren't bothered.

Message	Destination	Description
RS (Router Solicitation)	FF02::2 (All IPv6 Routers)	FF02::2 is local-scope, so the host is asking all routers on its own LAN to identify themselves
RA (Router Advertisement)	Unicast to Requestor or FF02::1 (All IPv6 Hosts)	All routers periodically describe themselves to all hosts on the local LAN. Plus, if they hear an RS, they'll identify themselves directly to the sender.

Following a successful router discovery, the host knows (at least) three things:

- The router address
- The router address prefix-length
- The network prefix and prefix-length of its own LAN—calculated from the above two items and the knowledge that the router must be in the same LAN to have answered.

NEIGHBOR MAC DISCOVERY

A similar pair of ICMPV6 messages replace IPv4 ARP, allowing hosts on a LAN to learn each other's OSI L2 (MAC) addresses.

Message	Destination	Description
NS (Neighbor Solicitation)	Solicited-Node Multicast address corresponding to target	All interfaces whose IPv6 address matches the last 24 bits (6 hex digits) will receive the message
NA (Neighbor Advertisement)	Unicast to Requestor (NS) or FF02::1 (All IPv6 Hosts) possible for an unsolicited announcement	The message will include • Target address—the full IPv6 of the responder • The MAC address of the responder

DAD (Duplicate Address Detection)—Before using an IPv6 address (including when an interface comes up), a host will send an NS for that address. If there's an NA reply with an exactly matching target address, then the address won't be used until the problem is fixed. Even link-local addresses are checked this way.

DHCP WITH NDP

Stateful DHCPv6—like IPv4, tracks client leases; stateless doesn't.

DHCPv6 doesn't supply default-router info to the client (client uses NDP for that).

Messages—The names have changed (DORA to SARR) and so has some addressing

MESSAGE	FROM	SOURCE ADDRESS	DESTINATION ADDRESS
Solicit	Client	Host's link-local address In IPv4 this was 0.0.0.0	FF02::1:2 (All DHCP Agents) This is link-local scope; in IPv4 the broadcast address was used.
Advertise	Server		
Request	Client		
Reply	Server		

A relay agent changes the solicitation to a unicast

- The Destination address becomes the global-unicast address of the DHCPv6 server
- The Source address becomes that of the relay router's outgoing interface (by default)—this differs from DHCPv4

```
R5(config)# interface gi0/1
R5(config-if)# ipv6 dhcp relay destination 2001:db8:56::6

R5# show ipv6 interface gi0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::21E:13FF:FE21:E3A9
  No Virtual link-local address(es):
  Description: TO S5
  Global unicast address(es):
    2001:DB8:5::5, subnet is 2001:DB8:5::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:2
```

Shows that the interface is now listening to the address FF02::1:2 (all DHCP agents)

```
    FF02::1:FF00:5
    FF02::1:FF21:E3A9
  MTU is 1500 bytes
```

SLAAC

SLAAC (StateLess Address Auto-Configuration)—An alternative way to assign IPv6 addresses that doesn't require a DHCP server to babysit addresses and a human to babysit it.

The Address—After a host learns its prefix and prefix-length from NDP RS & RA messages, it can make up the host part, using either EUI-64 or a random number. As always, the host will use DAD to guarantee uniqueness before using the address.

DNS Server Addresses can come from a stateless DHCP server. The DHCP server is considered stateless because it doesn't have to remember anything about the hosts on the net—it's just answering a question, not assigning addresses.

Recap—Information Sources for host self-configuration

NDP (Router discovery)	SLAAC	Stateless DHCPv6
Default Router (gateway)	Unicast Address (EUI-64 or random)	DNS Server
Network Prefix Length		
Network Prefix (combine above two)		

Host Commands

IOS	Windows	Linux / MAC

`show ipv6 neighbors`
`show ipv6 routers`
	`netsh interface ipv6 show neighbors`	`(Linux) ip -6 neighbor show`
		`(Mac) ndp -an`
		Routers flagged with an "R"

`ping`
`(or) ping ipv6`
	`ping`	`ping6`

`traceroute`	`tracert`	`traceroute6`
`show ipv6 interface`	`ipconfig`	`ifconfig`

One way to see if another host is even responsive to IPv6 at all is to flush the neighbor table and ping it. Even if the ping didn't work, the neighbor table should show an entry resulting from the NDP message your router sent to learn its MAC address (like ARP).

```
R5# clear ipv6 neighbors
R5# show ipv6 neighbors
R5# ping 2001:db8:56::6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:56::6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/8 ms
R5# show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
FE80::21B:D4FF:FE76:6058                    0 001b.d476.6058  DELAY Gi0/0
2001:DB8:56::6                              0 001b.d476.6058  REACH Gi0/0
```

In IOS, if you make enough of a mistake with the IPv6 address that it no longer looks like an IPv6 address, you could get the following message:

```
R5# ping 2001:db8:56:6
% Unrecognized host or address, or protocol not running.
```

The address should have ended with ::6 (double-colon)