Mastering IPv6 Neighbor Discovery

Nick Russo
NETWORK ENGINEER

@nickrusso42518 www.njrusmc.net

Agenda

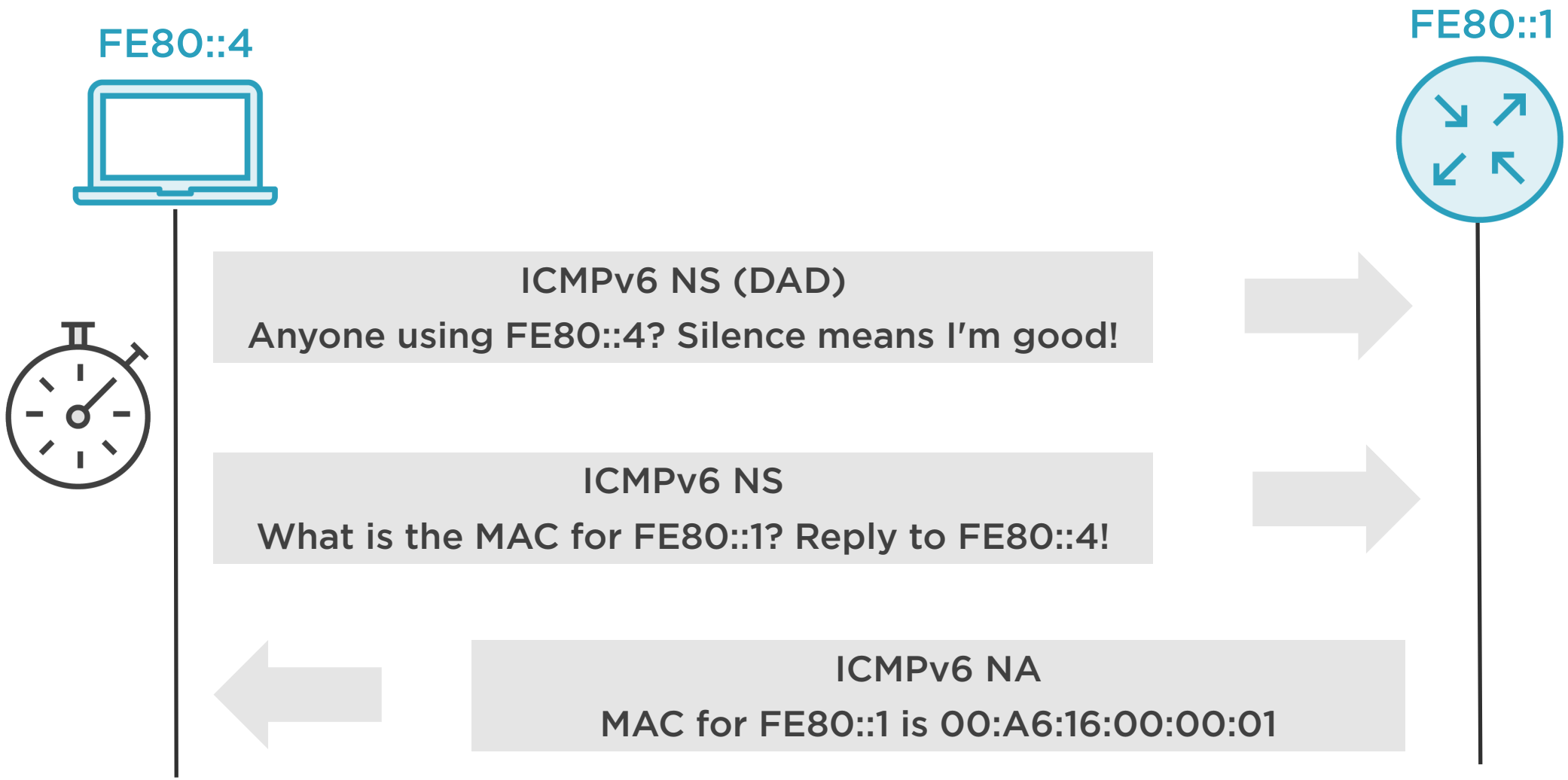
Understanding ND operations

- IPv4 ARP and IPv6 basics needed!

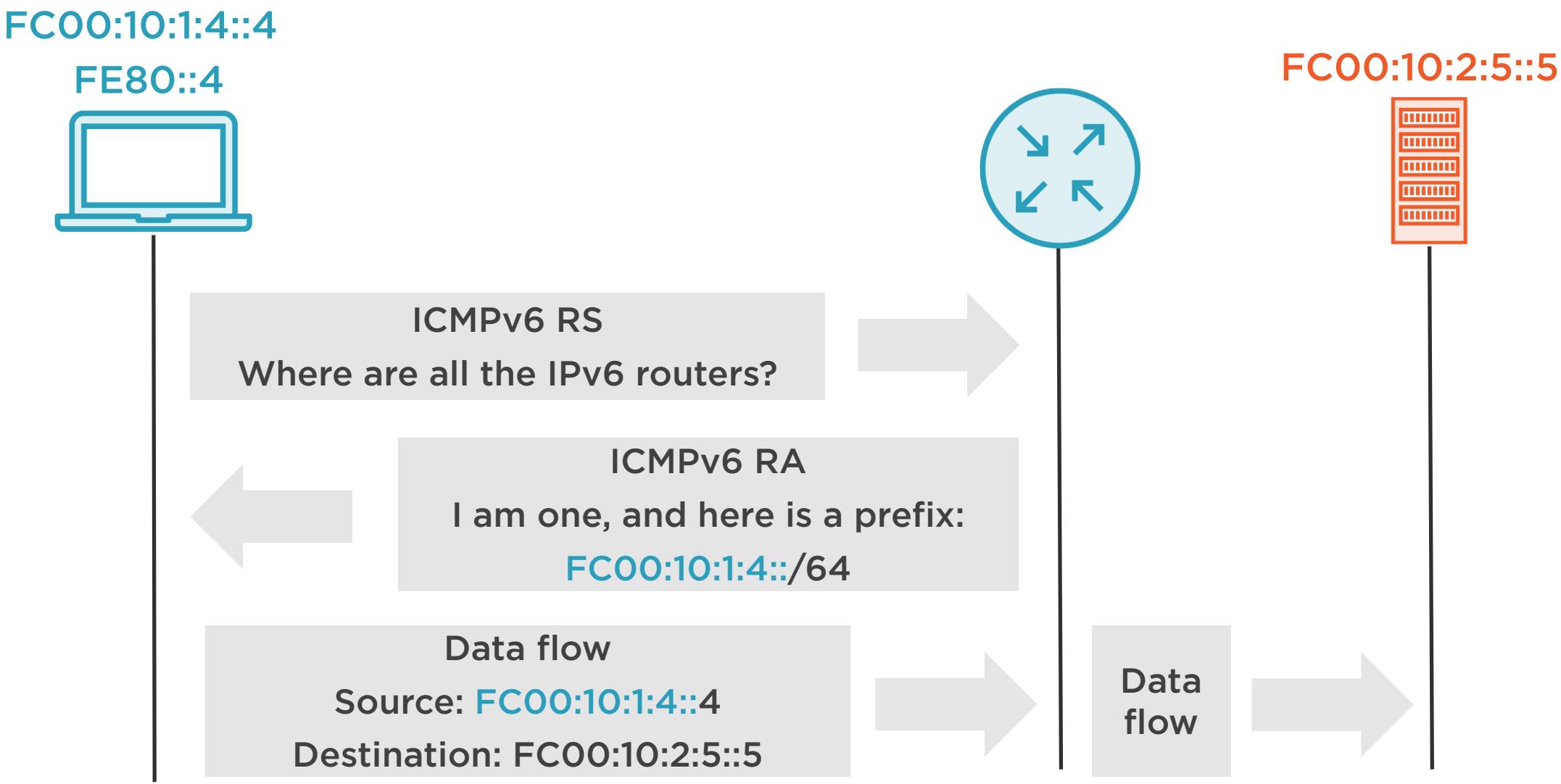
IPv6 ND in action, by the numbers

Packet analysis

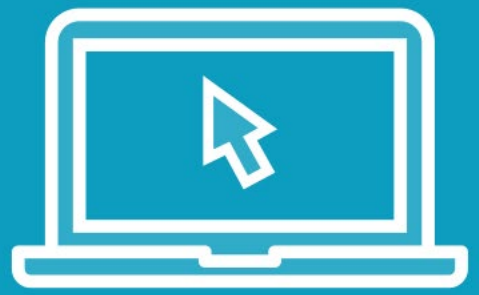
How IPv6 ND Works



Non Link-local Communication



Demo



IPv6 ND: The NS and NA

IPv6 Neighbor Solicitation – DAD

No.	Time	Source	Destination	Protocol	Info
1	0.000000	::	ff02::1:ff00:4	ICMPv6	Neighbor Solicitation for fe80::4
2	8.376527	fe80::4	ff02::1:ff00:1	ICMPv6	Neighbor Solicitation for fe80::1 from 00:00:a6:16:00:04
3	8.387692	fe80::1	fe80::4	ICMPv6	Neighbor Advertisement fe80::1 (rtr, sol, ovr) is at 00:00:a6:16:00:01

```
▶ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:04, Dst: 33:33:ff:00:00:04
▶ Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff00:4
▼ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0x06ab [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: fe80::4
  ▼ ICMPv6 Option (Nonce)
      Type: Nonce (14)
      Length: 1 (8 bytes)
      Nonce: e6bb87dff8cf
```

Type 135 means NS
No codes

Sender's desired address

Prevent looped-back NS (RFC 7527)

IPv6 Neighbor Solicitation – ND

No.	Time	Source	Destination	Protocol	Info
1	0.000000	::	ff02::1:ff00:4	ICMPv6	Neighbor Solicitation for fe80::4
2	8.376527	fe80::4	ff02::1:ff00:1	ICMPv6	Neighbor Solicitation for fe80::1 from 00:00:a6:16:00:04
3	8.387692	fe80::1	fe80::4	ICMPv6	Neighbor Advertisement fe80::1 (rtr, sol, ovr) is at 00:00:a6:16:00:01

```
▶ Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:04, Dst: 33:33:ff:00:00:01
▶ Internet Protocol Version 6, Src: fe80::4, Dst: ff02::1:ff00:1
▼ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0xd67c [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: fe80::1
  ▼ ICMPv6 Option (Source link-layer address : 00:00:a6:16:00:04)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: 00:00:a6:16:00:04
```

Type 135 means NS (again)
No codes

Remote address to resolve

Sender's MAC address

IPv6 Neighbor Advertisement

No.	Time	Source	Destination	Protocol	Info
1	0.000000	::	ff02::1:ff00:4	ICMPv6	Neighbor Solicitation for fe80::4
2	8.376527	fe80::4	ff02::1:ff00:1	ICMPv6	Neighbor Solicitation for fe80::1 from 00:00:a6:16:00:04
3	8.387692	fe80::1	fe80::4	ICMPv6	Neighbor Advertisement fe80::1 (rtr, sol, ovr) is at 00:00:a6:16:00:01

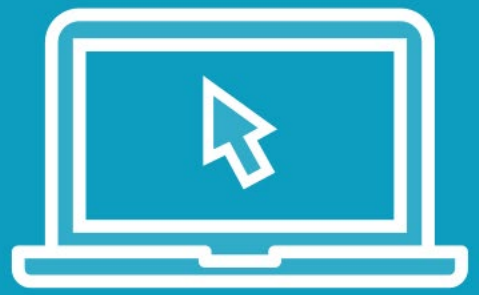
```
▶ Frame 3: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 6, Src: fe80::1, Dst: fe80::4
▼ Internet Control Message Protocol v6
    Type: Neighbor Advertisement (136)
    Code: 0
    Checksum: 0xf402 [correct]
    [Checksum Status: Good]
  ▼ Flags: 0xe0000000
      1... .... .... .... .... .... .... .... = Router: Set
      .1.. .... .... .... .... .... .... .... = Solicited: Set
      ..1. .... .... .... .... .... .... .... = Override: Set
      ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
    Target Address: fe80::1
  ▼ ICMPv6 Option (Target link-layer address : 00:00:a6:16:00:01)
      Type: Target link-layer address (2)
      Length: 1 (8 bytes)
      Link-layer address: 00:00:a6:16:00:01
```

Type 136 means NA
No codes

Remote address to resolve

MAC binding for FE80::1 !!!

Demo



IPv6 ND: The RS and RA

IPv6 Router Solicitation

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::4	ff02::2	ICMPv6	Router Solicitation from 00:00:a6:16:00:04
2	0.000662	fe80::1	fe80::4	ICMPv6	Router Advertisement from 00:00:a6:16:00:01

```
▶ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:04, Dst: 33:33:00:00:00:02
▶ Internet Protocol Version 6, Src: fe80::4, Dst: ff02::2
▼ Internet Control Message Protocol v6
    Type: Router Solicitation (133)
    Code: 0
    Checksum: 0xd60f [correct]
    [Checksum Status: Good]
    Reserved: 00000000
  ▼ ICMPv6 Option (Source link-layer address : 00:00:a6:16:00:04)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: 00:00:a6:16:00:04
```

Type 133 means RS
No codes

MAC of client

IPv6 Router Advertisement

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::4	ff02::2	ICMPv6	Router Solicitation from 00:00:a6:16:00:04
2	0.000662	fe80::1	fe80::4	ICMPv6	Router Advertisement from 00:00:a6:16:00:01

```
▶ Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
▶ Ethernet II, Src: 00:00:a6:16:00:01, Dst: 00:00:a6:16:00:04
▶ Internet Protocol Version 6, Src: fe80::1, Dst: fe80::4
▼ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x7bf5 [correct]
    [Checksum Status: Good]
    Cur hop limit: 64
  ▼ Flags: 0x00
      0... .... = Managed address configuration: Not set
      .0.. .... = Other configuration: Not set
      ..0. .... = Home Agent: Not set
      ...0 0... = Prf (Default Router Preference): Medium (0)
      .... .0.. = Proxy: Not set
      .... ..0. = Reserved: 0
    Router lifetime (s): 1800
    Reachable time (ms): 0
    Retrans timer (ms): 0
```

Type 134 means RA
No codes

Hop limit: new name for TTL

M Flag – RFC 4861
O Flag – RFC 4861
H Flag – RFC 3775
PRF – RFC 4191
P Flag – RFC 4389

IPv6 RA Options

```
▼ ICMPv6 Option (Source link-layer address : 00:00:a6:16:00:01)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: 00:00:a6:16:00:01
▼ ICMPv6 Option (MTU : 1500)
    Type: MTU (5)
    Length: 1 (8 bytes)
    Reserved
    MTU: 1500
▼ ICMPv6 Option (Prefix information : fc00:10:1:4::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
  ▶ Flag: 0xc0
    Valid Lifetime: 2592000
    Preferred Lifetime: 604800
    Reserved
    Prefix: fc00:10:1:4::
```

MAC of router

Helps prevent fragmentation

Dynamic and stateless addressing for clients!!!

IPv6 ND In Review

NS, NA, RS, RA

It is "polite"

It "just works"