Duplicate Address Detection

- Used before assigning an address
  - Check see if any other node has the same address
- Send NS for address desired
  - But from what address?
    - node might have none
    - Send from unspecified address 0::0
      - Also allows recognition of DAD
- Reply multicast to all nodes (on link)
  - No link layer address permitted
    - in NS from unsolicited address
  - No IPv6 address to send to

DAD Example

```
12:57:53.850579 0:6:5b:da:45:ad 33:33:ff:ad:be:ef 86dd 78:
   0::0 > ff02::1:ffad:beef:
        icmp6: neighbor sol: who has fe80::dead:beef
12:57:57.590521 0:6:5b:da:45:ad 33:33:ff:ad:be:ef 86dd 86:
   fe80::206:5bff:feda:45ad > ff02::1:ffad:beef:
   HBH (padn)(rtalert: 0x0000)
        icmp6: multicast listener report
                 max resp delay: 0
                 addr: ff02::1:ffad:beef [hlim 1]
12:58:13.624130 0:10:5a:76:e9:b4 33:33:ff:ad:be:ef 86dd 86:
   fe80::210:5aff:fe76:e9b4 > ff02::1:ffad:beef:
        icmp6: neighbor sol: who has fe80::dead:beef
        (src lladdr: 00:10:5a:76:e9:b4)
12:58:13.624215 0:6:5b:da:45:ad 0:10:5a:76:e9:b4 86dd 86:
   fe80::206:5bff:feda:45ad > fe80::210:5aff:fe76:e9b4:
        icmp6: neighbor adv: tgt is fe80::dead:beef(SO)
        (tgt lladdr: 00:06:5b:da:45:ad)
12:58:13.624338 0:10:5a:76:e9:b4 0:6:5b:da:45:ad 86dd 70:
   fe80::210:5aff:fe76:e9b4 > fe80::dead:beef:
        icmp6: echo request
12:58:13.624371 0:6:5b:da:45:ad 0:10:5a:76:e9:b4 86dd 70:
   fe80::dead:beef > fe80::210:5aff:fe76:e9b4:
        icmp6: echo reply
```

DAD Example (2)

```
13:15:01.869708 0:10:5a:76:e9:b4 33:33:ff:ad:be:ef 86dd 78:
   0::0 > ff02::1:ffad:beef:
         icmp6: neighbor sol:
                who has fe80::dead:beef
                                (len 24, hlim 255)


13:15:01.869761 0:6:5b:da:45:ad 33:33:0:0:0:1 86dd 86:
   fe80::dead:beef > ff02::1:
         icmp6: neighbor adv:
                tgt is fe80::dead:beef(O)
                (tgt lladdr: 00:06:5b:da:45:ad)
                                (len 32, hlim 255)
```

Neighbour Unreach Detection

- Used to discover if router being used is functioning
  - Router gives no feedback
  - Simply forwards packet
- If upper layer says all is OK
  - Then router must be working
    - eg: TCP is receiving ACK
- Otherwise
  - Occasionally unicast NS to router
  - Expect NA in reply
    - With R flag set
  - If no reply, or no R flag
    - router no longer functional
    - Pick a different one

ND Security Issues

- Send NS
  - request link addr for IPv6 address
  - someone replies
    - "That is me, my link addr is ..."
  - How do we know that is not fake?
- Receive RA
  - Contains list of prefixes
    - Used to configure addresses
  - Sender is Router
  - Can we trust that message?
    - How?

NS/NA Security

- Need to prove
  - seystem sending NS/NA
  - owns the address it claims
- Address
  - Prefix relatively easy
    - if not appropriate NS/NA irrelevant
  - Local part can be anything
    - RFC3041 random identifier
    - Any node might choose any value
      - Which owns which?
- Could add configuration
  - But might as well configure link address
    - abandon NA/NS completely

NS/NA Security (2)

- Information Available
  - The address
    - We know that, want to communicate
  - The NA/NS packet
    - and anything it contains
  - That's all...
- The NS/NA is being validated
  - Nothing in it can be trusted without proof
- Only the address remains
  - Can we use the address to prove ownership?

NS/NA Security (3)

- Local part can be anything
  - Use EUI-84
    - almost guarantees uniqueness
  - Use random number
    - in 64 bit space
      - almost guarantees uniqueness
  - Human configured
    - human guarantees uniqueness
      - we hope...
- Nothing cares which is chosen
  - Or some other method

CGA

Cryptographically Generated Addresses RFC3972

- Hash generated address
  - Hash defined data
    - Result -> local part
  - Include data with NS/NA
    - Other nodes can verify calculation
- Defined data
  - Could be anything
    - ... network prefix
  - If data constant
    - hash stable
    - same result every time
  - If data variable
    - result will vary
- Of itself not very useful
  - Anyone can copy data