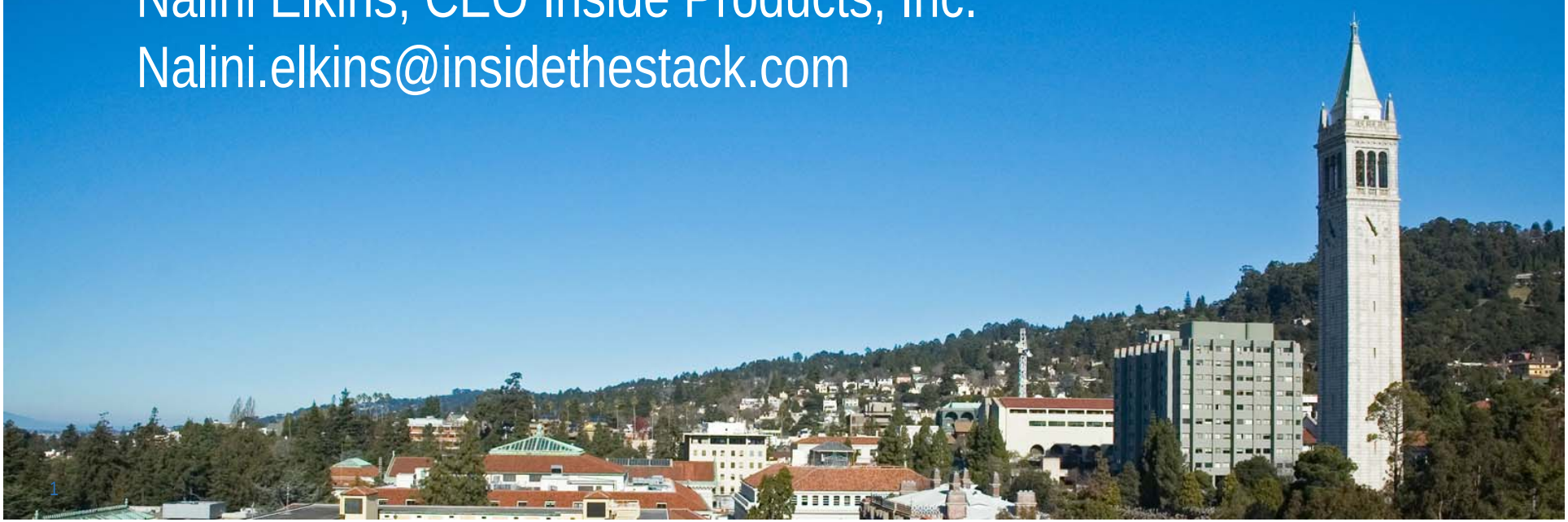
SHARKFEST '13

Wireshark Developer and User Conference

IPv6 Trace Analysis using Wireshark

Nalini Elkins, CEO Inside Products, Inc.
Nalini.elkins@insidethestack.com



Agenda

- What has not changed between IPv4 and IPv6 traces
- What <u>has</u> changed between IPv4 and IPv6 traces
- IPv6 extension headers
- Flow label
- Who sent it and who received it? (Global Unicast, Multicast, Link Local)
- Packets, packets, packets!
- Tunneling (Teredo, 6to4)
- DNSv6 / DHCPv6

What has not changed

- Packets trace the network flow
- Upper layer protocols (mostly)

What has changed

- The IP layer protocol (extensions, etc.)
- Address resolution
- Source and destination addresses (and meaning)
- ICMP
- Understanding of network analyst

Common IPv6 Extension Headers

Next Header (Hex)	Next Header (Decimal)	Header Name	Description
0	0	Hop-by-Hop Options	For all devices on the path
2B	43	Routing	0 – Source Routing (deprecated) 2 – Mobile IPv6
2C	44	Fragment	Only when packet is fragmented
32	50	Encapsulated Security Payload (ESP)	IPSec encrypted data
33	51	Authentication Header (AH)	IPSec authentication
3C	60	Destination Options	http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml (Mobile IP, etc)

IPv6 Hop-by-Hop Header

Size (bits)	Field Name	Description
8	Next Header	Contains the protocol number of the next header
8	Length	Length of this header in octets (bytes)
Variable	Options	8 bits for type, length in bytes, and then the option itself http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml

Remember: this has to be read by every device!

No.	Time	Source	Destination	Pro
1693	46.130640	::	ff02::2	IC

```
⊞ Frame 1693 (86 bytes on wire, 86 bytes captured)
⊟ Ethernet II, Src: 192.168.1.1 (00:14:bf:ba:45:f9), Dst: I
    Destination: IPv6-Neighbor-Discovery_00:00:00:02 (33:33
    Source: 192.168.1.1 (00:14:bf:ba:45:f9)
    Type: IPv6 (0x86dd)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: IPv6 hop-by-hop option (0x00)
    Hop limit: 1
    Source address: ::
    Destination address: ff02::2
⊟ Hop-by-hop Option Header
    Next header: ICMPv6 (0x3a)
    Length: 0 (8 bytes)
    Router alert: MLD (4 bytes)
    PadN: 2 bytes
⊟ Internet Control Message Protocol v6
    Type: 131 (Multicast listener report)
    Code: 0
    Checksum: 0x7ea3 [correct]
    Maximum response delay: 0
    Multicast Address: ff02::2
```

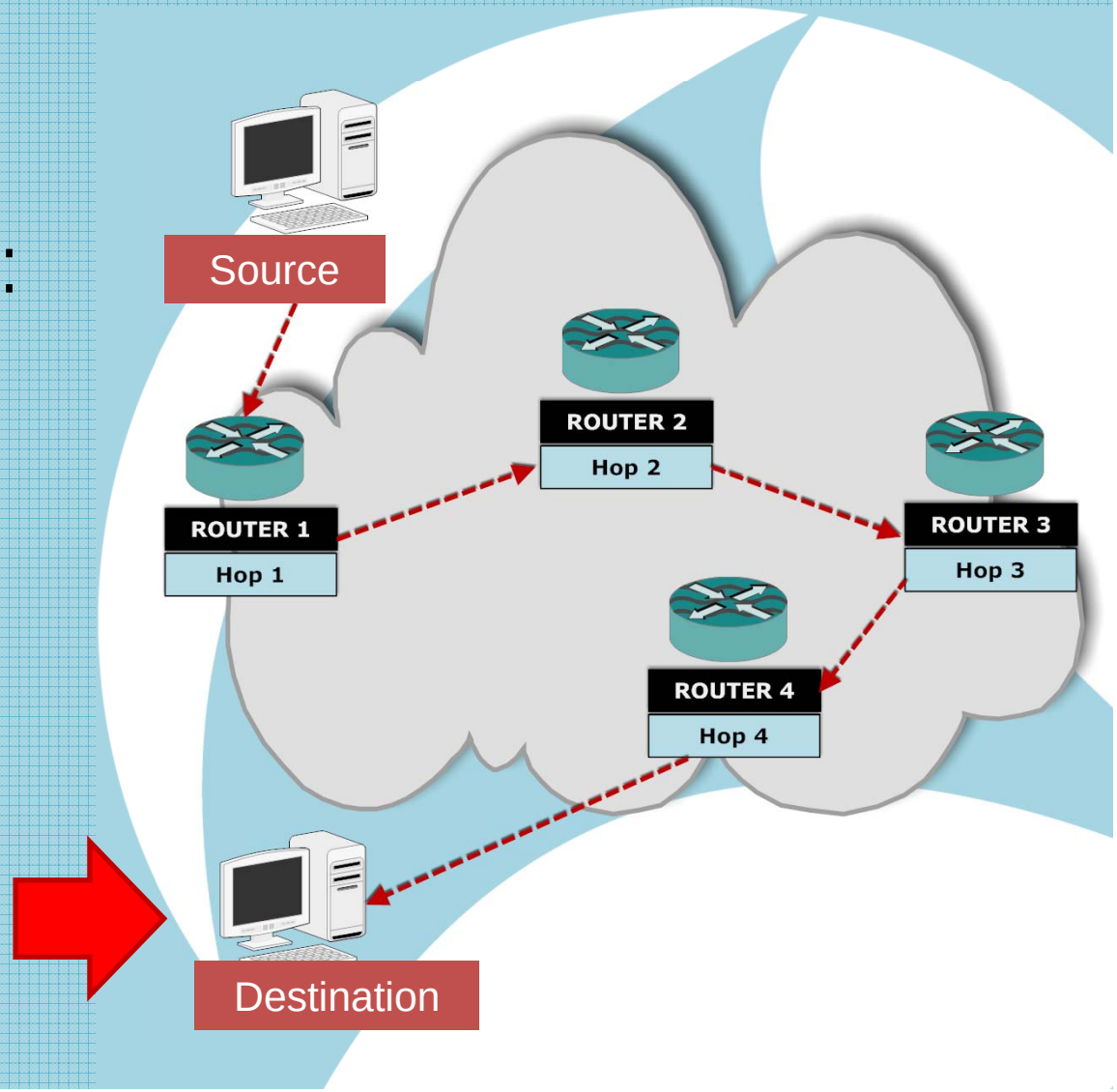
Sample Fragment Header

No.	Time	Source	Destination
5762	80.385670	2001:4998:0:6::15	2607:f740:0:3f:216:3eff:fe68:72c0

```
⊞ Frame 5762: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits)
⊞ Ethernet II, Src: Cisco_ae:30:0a (00:0c:cf:ae:30:0a), Dst: Xensourc_68:72:c0 (
⊟ Internet Protocol Version 6, Src: 2001:4998:0:6::15 (2001:4998:0:6::15), Dst:
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0101 0100 0001 0000 1100 = Flowlabel: 0x0005410c
    Payload length: 1440
    Next header: IPv6 fragment (0x2c)
    Hop limit: 56
    Source: 2001:4998:0:6::15 (2001:4998:0:6::15)
    Destination: 2607:f740:0:3f:216:3eff:fe68:72c0 (2607:f740:0:3f:216:3eff:fe68
    [Destination SA MAC: Xensourc_68:72:c0 (00:16:3e:68:72:c0)]
  ⊟ Fragmentation Header
      Next header: TCP (0x06)
      0000 0000 0000 0... = Offset: 0 (0x0000)
      .... .... .... ...1 = More Fragment: Yes
      Identification: 0xa262a3bc
    Reassembled IPv6 in frame: 5763
⊞ Data (1432 bytes)
```

IPv6 Destination Options

- Destination Options: for end host



IPv6 Destination Options

```
⊞ Frame 1: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits)
⊞ Prism capture header
⊞ IEEE 802.11 Data, Flags: .......T
⊞ Logical-Link Control
⊟ Internet Protocol Version 6, Src: 2001:720:810:1212:209:b7ff:fe3c:902c (2001:720:810:1212:2
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 40
    Next header: IPv6 destination option (60)
    Hop limit: 255
    Source: 2001:720:810:1212:209:b7ff:fe3c:902c (2001:720:810:1212:209:b7ff:fe3c:902c)
    [Source SA MAC: Cisco_3c:90:2c (00:09:b7:3c:90:2c)]
    Destination: 2001:720:810:1213::1 (2001:720:810:1213::1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ Destination Option
      Next header: Mobile IPv6 [illegible] (62)
      Length: 2 (24 bytes)
    ⊟ IPv6 Option (PadN)
        Type: PadN (1)
        Length: 2
        PadN: 0000
    ⊟ IPv6 Option (Home Address)
        Type: Home Address (201)
        Length: 16
        Home Address: 2001:720:810:1213::2 (2001:720:810:1213::2)
⊟ Mobile IPv6 / Network Mobility
```

Use of Destination Options in Mobile IPv6

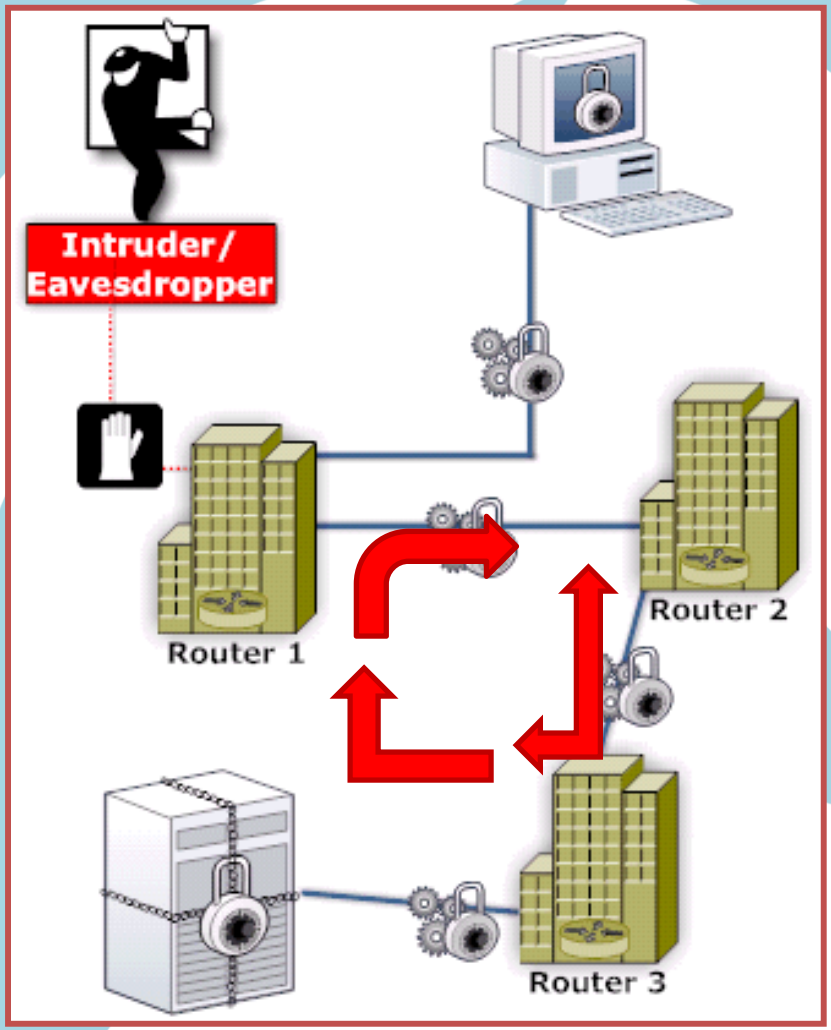
No.	Time	Source	Destination	Protocol
1	0.000000	2a01:e35:8bd9:8bb0:	2001:4b98:dc0:41:21	UDP
2	0.050763	2001:4b98:dc0:41:21	2a01:e35:8bd9:8bb0:	ICMPv6

```
⊞ Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
⊞ Ethernet II, Src: AsustekC_76:29:b6 (00:1e:8c:76:29:b6), Dst: FreeboxS_4d:1f:41 (f
⊟ Internet Protocol Version 6, Src: 2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397 (2a01:e35
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 26
    Next header: IPv6 destination option (60)
    Hop limit: 64
    Source: 2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397 (2a01:e35:8bd9:8bb0:a0a7:ea9c:74e
    Destination: 2001:4b98:dc0:41:216:3eff:fece:1902 (2001:4b98:dc0:41:216:3eff:fece
    [Destination SA MAC: Xensourc_ce:19:02 (00:16:3e:ce:19:02)]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ Destination Option
      Next header: UDP (17)
      Length: 0 (8 bytes)
    ⊟ IPv6 Option (Unknown 11)
        Type: Unknown (11)
        Length: 1
        Unknown Option Payload: 09
    ⊟ IPv6 Option (PadN)
        Type: PadN (1)
        Length: 1
        PadN: 00
⊟ User Datagram Protocol, Src Port: 42513 (42513), Dst Port: name (42)
    Source port: 42513 (42513)
```

From RFC2460: Option 11: discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

RFC5095 (Deprecation of Type 0 Routing Headers in IPv6)

- RH0 : can create routing loops.
- Deprecated
- Segments Left = zero, ignore
- Segments Left > zero, send ICMPv6 error message



No.	Time	Source	Destination
1	0.000000	3001::200:10ff:fe10:1181	3000::200:10ff:fe10:1060

```
⊞ Frame 1: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
⊞ Ethernet II, Src: Hughes_10:10:60 (00:00:10:10:10:60), Dst: IntelCor_16:c7:fe (00:15:17:16:c7
⊟ Internet Protocol Version 6, Src: 3001::200:10ff:fe10:1181 (3001::200:10ff:fe10:1181), Dst: 3
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 65
    Next header: IPv6 routing (43)
    Hop limit: 255
    Source: 3001::200:10ff:fe10:1181 (3001::200:10ff:fe10:1181)
    [Source SA MAC: Hughes_10:11:81 (00:00:10:10:11:81)]
    Destination: 3000::215:17ff:fe16:c7fe (3000::215:17ff:fe16:c7fe)
    [Destination SA MAC: IntelCor_16:c7:fe (00:15:17:16:c7:fe)]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ Routing Header, Type : IPv6 Source Routing (0)
      Next header: ICMPv6 (58)
      Length: 6 (56 bytes)
      Type: IPv6 Source Routing (0)
      Segments Left: 1
      Address: 3002::200:10ff:fe10:1262 (3002::200:10ff:fe10:1262)
      Address: 3003::200:10ff:fe10:1363 (3003::200:10ff:fe10:1363)
      Address: 3000::200:10ff:fe10:1060 (3000::200:10ff:fe10:1060)
⊟ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
  ⊞ Checksum: 0x1d00 [incorrect, should be 0xdbb9]
    [Bad Checksum: True]
    Identifier: 0x0000
    Sequence: 0
  ⊞ Data (1 byte)
```

Malformed Packets

- Manipulate headers
  - IPv6 incorrect or partial header
  - Violate header order
  - Violate header option restrictions

IPv6 Main Header (40 Bytes)

Version	Traffic Class	Flow Label	
Payload Length		Next Hdr	Hop Limit
Source Address			
Destination Address			

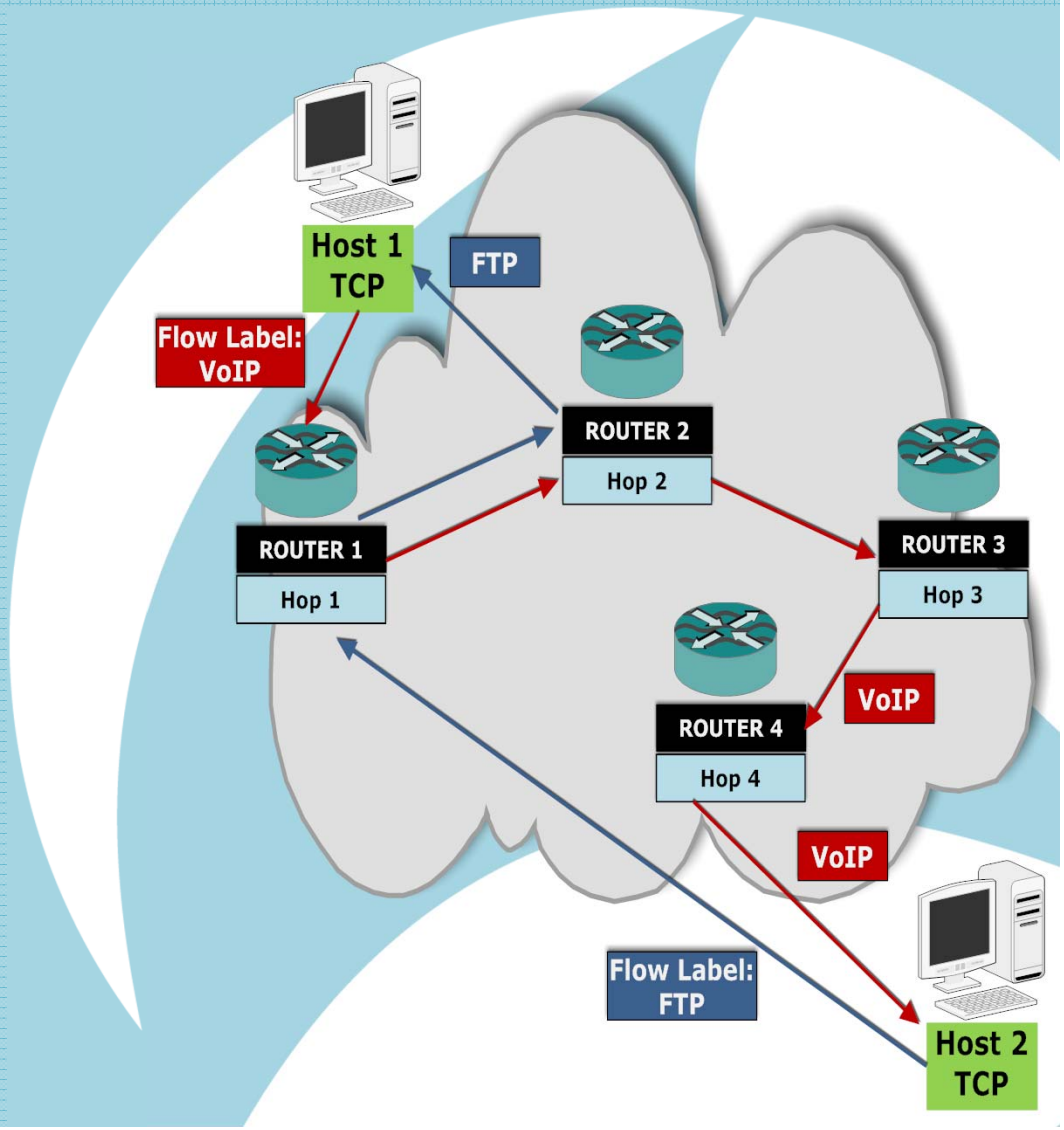
Crafted Packet

```
⊞ Frame 9 (182 bytes on wire, 182 bytes captured)
⊞ Ethernet II, Src: 3com_03:04:05 (00:01:02:03:04:05),
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 43008
    Next header: IPv6 fragment (0x2c)
    Hop limit: 255
    Source address: ::
    Destination address: ::
⊟ Fragmentation Header
    Next header: IPv6 routing (0x2b)
    Offset: 48
    More fragments: Yes
    Identification: 0x00370037
⊟ Routing Header, Type 0
    Next header: IPv6 fragment (0x2c)
    Length: 9 (80 bytes)
    Type: 0
    Segments left: 0
    address 0: ::
    address 1: ::
    address 2: ::
    address 3: ::
    address 4: ::7005:917c:ffff:ffff
⊟ Fragmentation Header
    Next header: IPv6 hop-by-hop option (0x00)
    Offset: 0
    More fragments: No
    Identification: 0x00000000
⊟ Hop-by-hop Option Header
```

- Crafted IPv6 packet
- Multiple headers
- Deprecated headers
- Headers out of order

Flow Label

- Quality of Service
- What is a flow?
- All routers on the path
- SNA CoS



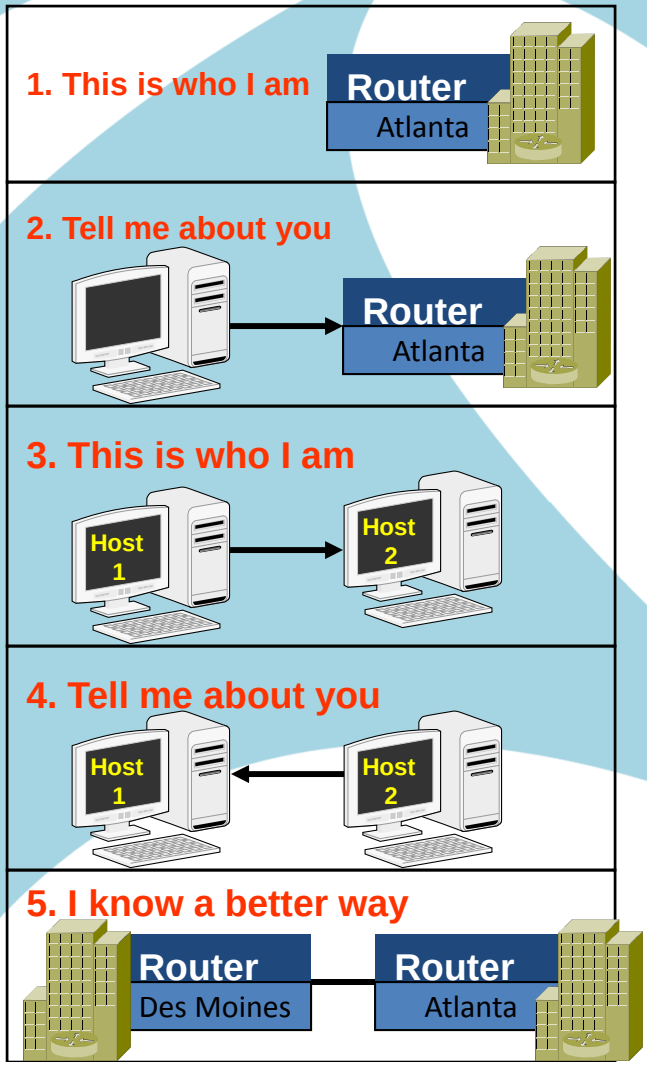
Trace Packet With Flow Label

No.	Time	Source	Destination
3406	64.672910	2607:f4e8:130:202:225:90ff:fe01:a610	2607:f740:0:3f:216:3eff:fe68:72c0

```
⊞ Frame 3406: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
⊞ Ethernet II, Src: Cisco_ae:30:0a (00:0c:cf:ae:30:0a), Dst: Xensourc_68:72:c0 (00:16:3e:68:72:c0)
⊟ Internet Protocol Version 6, Src: 2607:f4e8:130:202:225:90ff:fe01:a610 (2607:f4e8:130:202:225:90ff
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 1001 0011 1001 0010 1110 = Flowlabel: 0x0009392e
    Payload length: 40
    Next header: TCP (0x06)
    Hop limit: 56
    Source: 2607:f4e8:130:202:225:90ff:fe01:a610 (2607:f4e8:130:202:225:90ff:fe01:a610)
    [Source SA MAC: SuperMic_01:a6:10 (00:25:90:01:a6:10)]
    Destination: 2607:f740:0:3f:216:3eff:fe68:72c0 (2607:f740:0:3f:216:3eff:fe68:72c0)
    [Destination SA MAC: Xensourc_68:72:c0 (00:16:3e:68:72:c0)]
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 41991 (41991), Seq: 0, Ack: 1, Len:
    Source port: http (80)
    Destination port: 41991 (41991)
    [Stream index: 43]
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 40 bytes
  ⊞ Flags: 0x012 (SYN, ACK)
    Window size value: 65535
    [Calculated window size: 65535]
  ⊞ Checksum: 0xff36 [validation disabled]
  ⊞ Options: (20 bytes)
  ⊞ [SEQ/ACK analysis]
```

Neighbor Discovery

- Neighbor Discovery (ND) replaces ARP
- RFC4861: Neighbor Discovery for IP version 6 (IPv6)
- Used in SLAAC
- Five ICMPv6 message types:
  1. *Router Advertisement*
  2. *Router Solicitation*
  3. *Neighbor Advertisement*
  4. *Neighbor Solicitation*
  5. *Redirect*



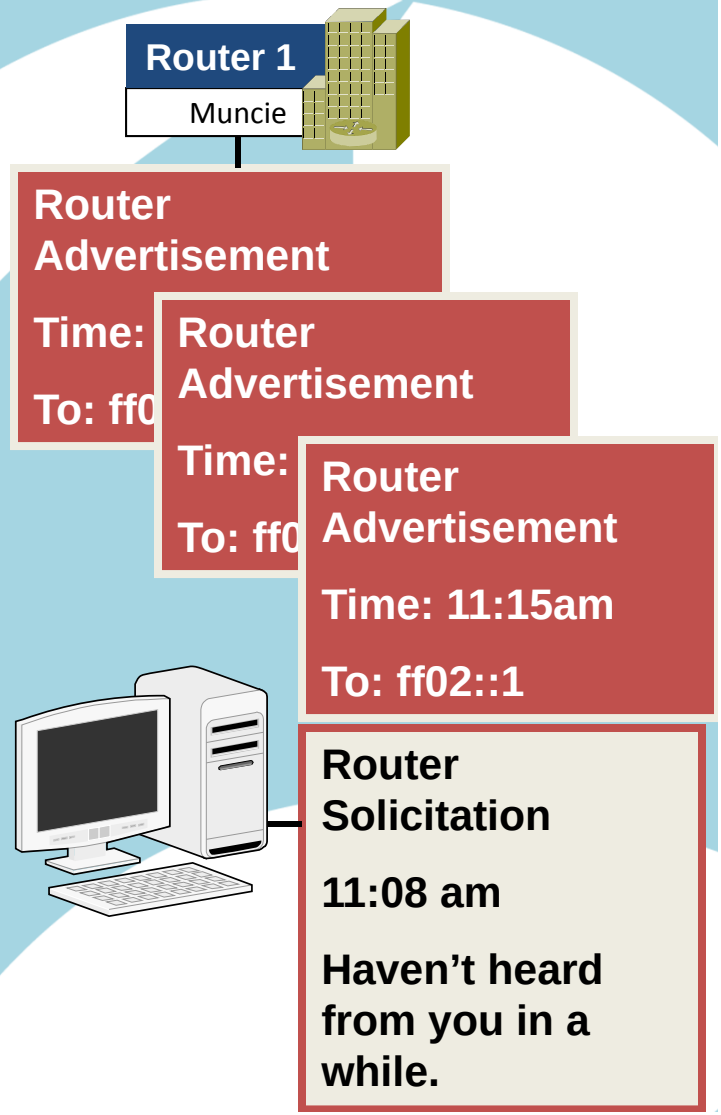
Neighbor Discovery

No.	Time	Source	Destination	Protocol	Info
23	13.642801	::	ff02::1:ff39:292b	ICMPv6	Multicast listener report
24	13.642826	::	ff02::2	ICMPv6	Router solicitation
25	13.642847	::	ff02::1:ff39:292b	ICMPv6	Neighbor solicitation
31	17.642731	fe80::211:d8ff:fe39:292b	ff02::2	ICMPv6	Router solicitation
46	21.642662	fe80::211:d8ff:fe39:292b	ff02::2	ICMPv6	Router solicitation
47	22.642644	fe80::211:d8ff:fe39:292b	ff02::1:ff39:292b	ICMPv6	Multicast listener report

```
⊞ Frame 25 (78 bytes on wire, 78 bytes captured)
⊟ Ethernet II, Src: AsustekC_39:29:2b (00:11:d8:39:29:2b), Dst: IPv6-Neighbor-Discovery_ff:39:29:2b
    Destination: IPv6-Neighbor-Discovery_ff:39:29:2b (33:33:ff:39:29:2b)
    Source: AsustekC_39:29:2b (00:11:d8:39:29:2b)
    Type: IPv6 (0x86dd)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 24
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: ::
    Destination address: ff02::1:ff39:292b
⊟ Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0x504d [correct]
    Target: fe80::211:d8ff:fe39:292b
```

Router Advertisement (RA)

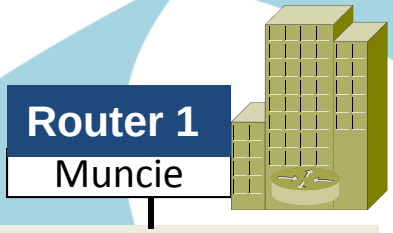
- *Router Advertisement* (RA) important for SLAAC.
- Sent at intervals
- Unsolicited RA sent to FF02::1
- Receiving hosts update configuration
- RA also responds to *Router Solicitation* (RS)
- Solicited RA sent to address of RS sender



Router Advertisement Contents

Router Advertisements contain:

- Stateless / stateful (DHCPv6)
- Network prefix
- Default router
- Hop limit
- MTU



Router Advertisement

Time: 10:45am

To: ff02::1

•Use AutoConfiguration

•Statelss

•Network Prefix: 2001:: /64

•I am default router

•For 200 seconds

•Hop limit: 126

•MTU: 4096

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::214:bfff:feba:45f9	ff02::1	ICMPv6	Router advertisement

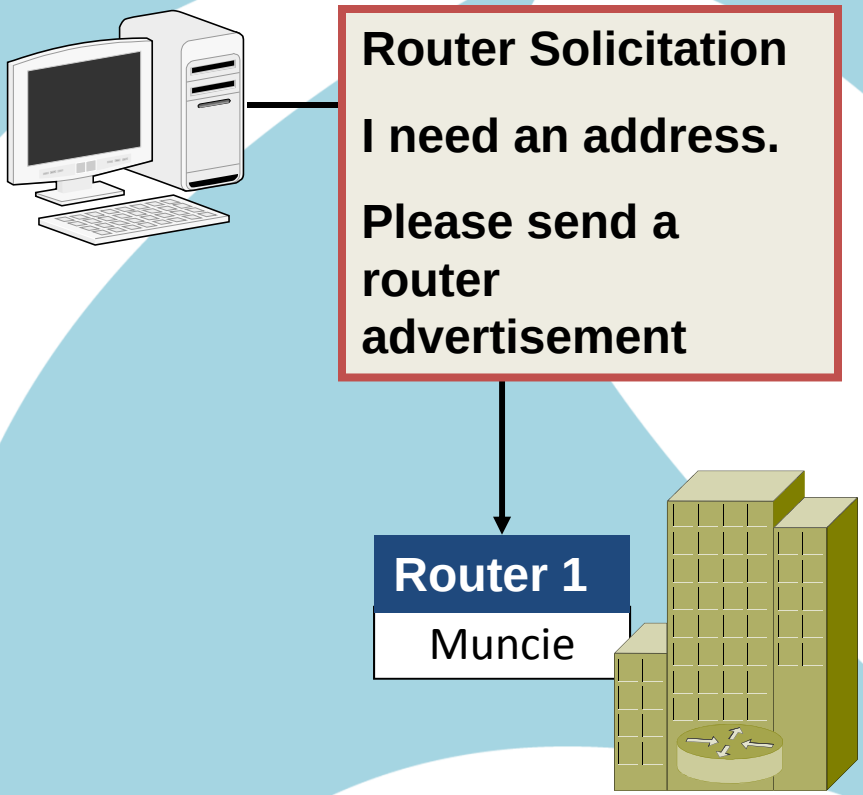
```
⊞ Frame 1 (110 bytes on wire, 110 bytes captured)
⊟ Ethernet II, Src: 192.168.1.1 (00:14:bf:ba:45:f9), Dst: IPv6-Neighbor-Discovery_00:00:00:01 (33:33:00:00:00:01)
    Destination: IPv6-Neighbor-Discovery_00:00:00:01 (33:33:00:00:00:01)
    Source: 192.168.1.1 (00:14:bf:ba:45:f9)
    Type: IPv6 (0x86dd)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 56
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::214:bfff:feba:45f9
    Destination address: ff02::1
⊟ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0xecdd [correct]
    Cur hop limit: 64
  ⊟ Flags: 0x00
      0... .... = Not managed
      .0.. .... = Not other
      ..0. .... = Not Home Agent
      ...0 0... = Router preference: Medium
    Router lifetime: 1800
    Reachable time: 0
    Retrans time: 0
  ⊟ ICMPv6 options
      Type: 3 (Prefix information)
      Length: 32 bytes (4)
      Prefix length: 64
    ⊟ Flags: 0xc0
        1... .... = Onlink
        .1.. .... = Auto
        ..0. .... = Not router address
        ...0 .... = Not site prefix
      Valid lifetime: 0x00278d00
      Preferred lifetime: 0x00093a80
      Prefix: 2001:4840:ffff:c012:214:bfff:feba:45f9
  ⊟ ICMPv6 options
      Type: 1 (Source link-layer address)
      Length: 8 bytes (1)
      Link-layer address: 00:14:bf:ba:45:f9
```

Router Advertisement Packet

- Source address
- Destination address
- ICMP type
- Hop limit
- Prefix length
- Prefix

Router Solicitation (RS)

- Sent during SLAAC
- Immediate response needed
- Sent 3 times total if no response



Router Solicitation Packet

```
⊞ Frame 2206 (70 bytes on wire, 70 bytes captured)
⊟ Ethernet II, Src: 192.168.1.100 (00:11:d8:39:29:2b),
    Destination: IPv6-Neighbor-Discovery_00:00:00:02 (
    Source: 192.168.1.100 (00:11:d8:39:29:2b)
    Type: IPv6 (0x86dd)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 16
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::211:d8ff:fe39:292b
    Destination address: ff02::2
⊟ Internet Control Message Protocol v6
    Type: 133 (Router solicitation)
    Code: 0
    Checksum: 0x7842 [correct]
  ⊟ ICMPv6 options
      Type: 1 (Source link-layer address)
      Length: 8 bytes (1)
      Link-layer address: 00:11:d8:39:29:2b
```

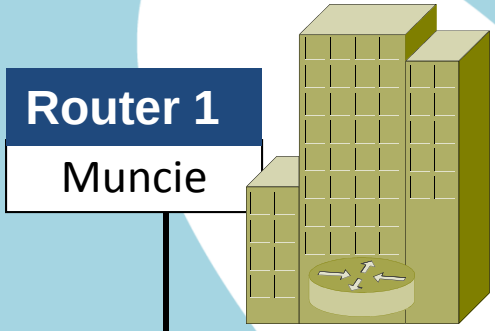
Router Solicitation Packet

- Source address
- Destination address
- ICMPv6 type

Neighbor Advertisement (NA)

Neighbor Advertisements sent:

- In response to *Neighbor Solicitation*
- Or if own NIC changes
- Contain link-layer address



Neighbor Advertisement

To: fe80::1:2:3:4

•My link-local address is: fe80::5:6:7:8

Neighbor Advertisement Packet

No.	Time	Source	Destination	Protocol	Info
6	9.865886	fe80::2ff:8cff:fe10:3976	2001:5c0:8fff:fffe	ICMPv6	Neighbor solicitation
7	9.865895	2001:5c0:8fff:fffe::3f52	fe80::2ff:8cff:fe1	ICMPv6	Neighbor advertisement

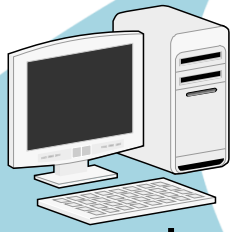
```
⊞ Frame 7 (86 bytes on wire, 86 bytes captured)
⊞ Ethernet II, Src: 00:ff:8d:10:39:76 (00:ff:8d:10:39:76), Dst: 00:ff:8c:10:39:76 (00:ff:8c:10:39:76)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: 2001:5c0:8fff:fffe::3f52
    Destination address: fe80::2ff:8cff:fe10:3976
⊟ Internet Control Message Protocol v6
    Type: 136 (Neighbor advertisement)
    Code: 0
    Checksum: 0xbdf3 [correct]
  ⊟ Flags: 0x40000000
      0... .... .... .... .... .... .... .... = Not router
      .1.. .... .... .... .... .... .... .... = Solicited
      ..0. .... .... .... .... .... .... .... = Not override
    Target: 2001:5c0:8fff:fffe::3f52
  ⊟ ICMPv6 options
      Type: 2 (Target link-layer address)
      Length: 8 bytes (1)
      Link-layer address: 00:ff:8d:10:39:76
```

Neighbor Advertisement

- ICMP type 136

Neighbor Solicitation (NS)

- *Neighbor Solicitations* request information
- *Neighbor Advertisement* response
- Sent during SLAAC (DAD)
- Sent to verify reachability



Neighbor Solicitation

To: ff02::1

Are you using:

fe80::1:2:3:4?

Neighbor Solicitation Packet

```
⊞ Frame 25 (78 bytes on wire, 78 bytes captured)
⊟ Ethernet II, Src: AsustekC_39:29:2b (00:11:d8:39:29:2b), Dst: IPv6-Neig
    Destination: IPv6-Neighbor-Discovery_ff:39:29:2b (33:33:ff:39:29:2b)
    Source: AsustekC_39:29:2b (00:11:d8:39:29:2b)
    Type: IPv6 (0x86dd)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 24
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: ::
    Destination address: ff02::1:ff39:292b
⊟ Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0x504d [correct]
    Target: fe80::211:d8ff:fe39:292b
```

NS Packet (Reachability)

No.	Time	Source	Destination	Protocol	Info
6	9.865886	fe80::2ff:8cff:fe10:3976	2001:5c0:8fff:fffe	ICMPv6	Neighbor solicitation
7	9.865895	2001:5c0:8fff:fffe::3f52	fe80::2ff:8cff:fe1	ICMPv6	Neighbor advertisement

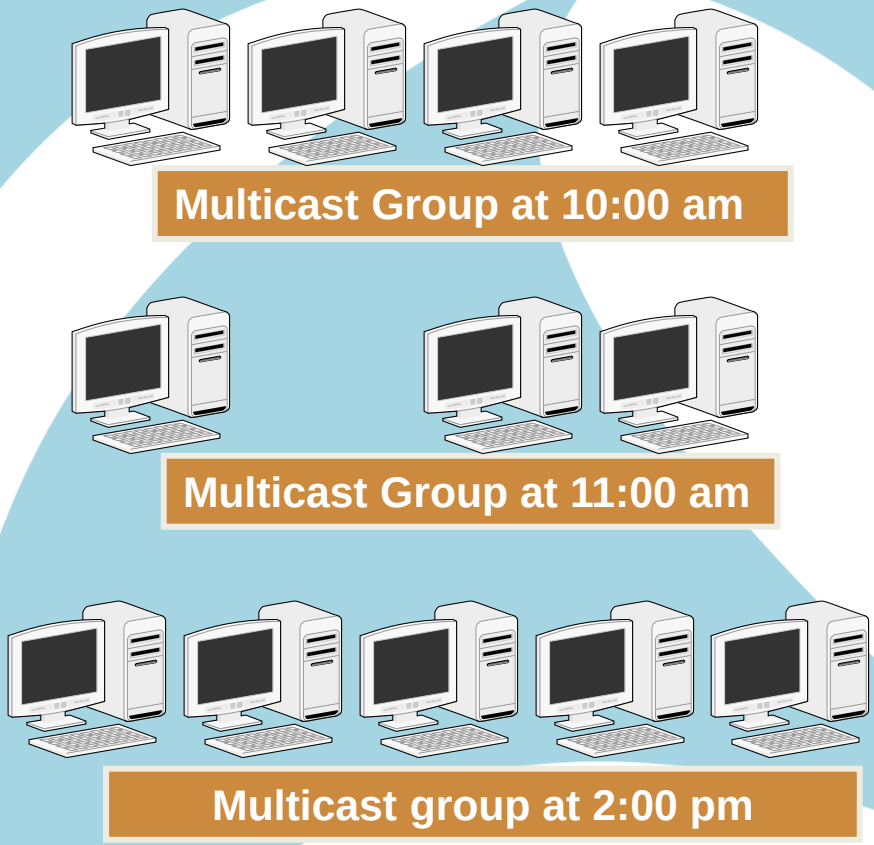
```
⊞ Frame 6 (86 bytes on wire, 86 bytes captured)
⊞ Ethernet II, Src: 00:ff:8c:10:39:76 (00:ff:8c:10:39:76), Dst: 00:ff:8d:10:39:76 (00:ff:8d:10:39:76)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::2ff:8cff:fe10:3976
    Destination address: 2001:5c0:8fff:fffe::3f52
⊟ Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0x00f4 [correct]
    Target: 2001:5c0:8fff:fffe::3f52
  ⊟ ICMPv6 options
      Type: 1 (Source link-layer address)
      Length: 8 bytes (1)
      Link-layer address: 00:ff:8c:10:39:76
```

Neighbor Solicitation Packet

To a specific unicast address.

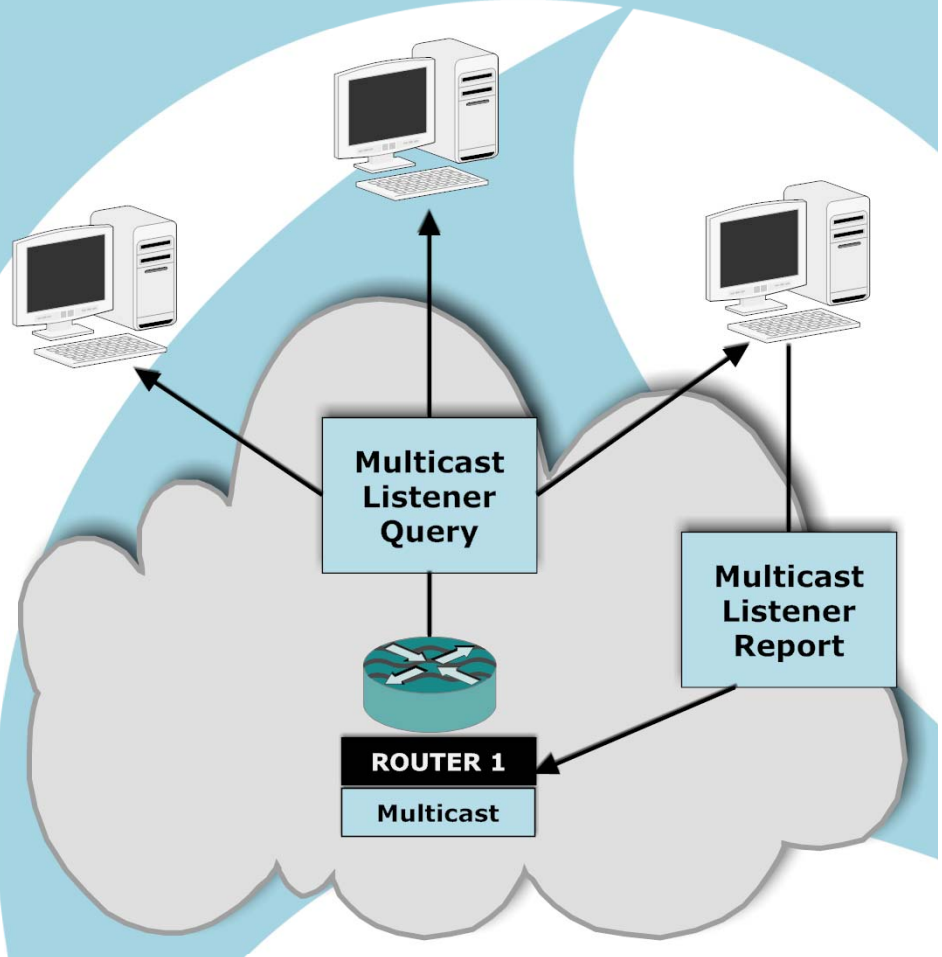
Multicast Groups

- Multicast: frequently used
  - All-nodes
  - All-routers
  - All-OSPF-routers
- Dynamic membership
- Multicast Listener Discovery (MLD) protocol used



Multicast Listener Discovery

- RFC2710: Multicast Listener Discovery (MLD) for IPv6
- RFC3590: Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
- RFC3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6



MLD Message Types

MLD message type	Description
Multicast Listener Query	General Query, used to learn which multicast addresses have listeners on an attached link. Multicast-Address-Specific Query, used to learn if a particular multicast address has any listeners on an attached link.
Multicast Listener Report	Sent by a host when it joins a multicast group, or in response to a Multicast Listener Query sent by a router.
Multicast Listener Done	Sent by a host when it leaves a host group and might be the last member of that group on the network segment.

Multicast Listener Report

No.	Time	Source	Destination	Protocol	Info
1693	46.130640	::	ff02::2	ICMPv6	Multicast listener report

```
⊞ Frame 1693 (86 bytes on wire, 86 bytes captured)
⊟ Ethernet II, Src: 192.168.1.1 (00:14:bf:ba:45:f9), Dst: IPv6-Neighbor-Discovery_00:00:00:02
    Destination: IPv6-Neighbor-Discovery_00:00:00:02 (33:33:00:00:00:02)
    Source: 192.168.1.1 (00:14:bf:ba:45:f9)
    Type: IPv6 (0x86dd)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: IPv6 hop-by-hop option (0x00)
    Hop limit: 1
    Source address: ::
    Destination address: ff02::2
⊟ Hop-by-hop Option Header
    Next header: ICMPv6 (0x3a)
    Length: 0 (8 bytes)
    Router alert: MLD (4 bytes)
    PadN: 2 bytes
⊟ Internet Control Message Protocol v6
    Type: 131 (Multicast listener report)
    Code: 0
    Checksum: 0x7ea3 [correct]
    Maximum response delay: 0
    Multicast Address: ff02::2
```

New Resource Record Type

- **DNS *A*** resource record: 32-bit IPv4 address
- **DNS *AAAA*** resource record: 128-bit IPv6 address
- Structure similar, but much larger!
- Other RRs: CNAME, MX, etc.

AAAA Record

AAAA (or quad A) record : defines an IPv6 address that matches to a host name.

- Can have more than one IPv6 address per host name
- Can have more than one host name per IPv6 address

AAAA record format:

Host.domain.name. *IN* *AAAA* *nnnn::nnnn*

Example:

from db.local

@ IN AAAA ::1

from NAMED.CONF

zone "localhost"

{ type master;

file "/etc/bind/db.local"; };

DNS Query – IPv6

```
⊞ Frame 1 (72 bytes on wire, 72 bytes captured)
⊞ Ethernet II, Src: Intel_4c:b3:ed (00:02:b3:4c:b3:ed), Dst: 00:1c:10:11:c7:09 (00:1c:10:11:c7
⊞ Internet Protocol, Src: 192.168.1.110 (192.168.1.110), Dst: 192.168.1.1 (192.168.1.1)
⊞ User Datagram Protocol, Src Port: 32777 (32777), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x846e
  ⊟ Flags: 0x0100 (Standard query)
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.kame.net: type AAAA, class IN
        Name: www.kame.net
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
```

Query to resolve IPv6 address for www.kame.net.

Command entered: host –t AAAA www.kame.net

DNS Response – IPv6

```
⊞ Frame 2 (100 bytes on wire, 100 bytes captured)
⊞ Ethernet II, Src: 00:1c:10:11:c7:09 (00:1c:10:11:c7:09), Dst: Intel_4c:b3:ed (00:02:b3:4c:b3:ed)
⊞ Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.110 (192.168.1.110)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 32777 (32777)
⊟ Domain Name System (response)
    Transaction ID: 0x846e
  ⊟ Flags: 0x8180 (Standard query response, No error)
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.kame.net: type AAAA, class IN
        Name: www.kame.net
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ www.kame.net: type AAAA, class IN, addr 2001:200:0:8002:203:47ff:fea5:3085
        Name: www.kame.net
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
        Time to live: 21 hours, 12 minutes, 26 seconds
        Data length: 16
        Addr: 2001:200:0:8002:203:47ff:fea5:3085
```

Commands to Query DNS

- DIG : name/address resolution, DNS server addresses, mail exchanges, name servers, and related information
- HOST : name/address resolution
- NSLOOKUP : name/address resolution (deprecated)

DIG Command Samples

- # get the IPv4 address(es) for yahoo.com
  dig yahoo.com A
- # get the IPv6 address(es) for yahoo.com
  dig yahoo.com AAAA
- # get the name for an IPv4 address
  dig -x 209.131.36.158
- # get a list of yahoo's mail servers
  dig yahoo.com MX
- # get a list of DNS servers authoritative for yahoo.com
  dig yahoo.com NS
- # get all of the above
  dig yahoo.com ANY

DNS Query – DIG AAAA

```
⊞ Frame 2 (74 bytes on wire, 74 bytes captured)
⊞ Linux cooked capture
⊞ Internet Protocol, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
⊞ User Datagram Protocol, Src Port: 32770 (32770), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0xfb48
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.kame.net: type AAAA, class IN
        Name: www.kame.net
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
```

Query packet generated by :

dig www.kame.net AAAA

```
⊞ Frame 3 (183 bytes on wire, 183 bytes captured)
⊞ Linux cooked capture
⊞ Internet Protocol, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 32770 (32770)
⊟ Domain Name System (response)
    Transaction ID: 0xfb48
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ⊟ Queries
    ⊟ www.kame.net: type AAAA, class IN
        Name: www.kame.net
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ www.kame.net: type AAAA, class IN, addr 2001:200:0:8002:203:47ff:fea5:3085
        Name: www.kame.net
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
        Time to live: 23 hours, 49 minutes, 40 seconds
        Data length: 16
        Addr: 2001:200:0:8002:203:47ff:fea5:3085
  ⊟ Authoritative nameservers
    ⊟ kame.net: type NS, class IN, ns orange.kame.net
        Name: kame.net
        Type: NS (Authoritative name server)
        Class: IN (0x0001)
        Time to live: 23 hours, 49 minutes, 40 seconds
        Data length: 9
        Name server: orange.kame.net
    ⊞ kame.net: type NS, class IN, ns ns1.itojun.org
  ⊟ Additional records
    ⊞ ns1.itojun.org: type A, class IN, addr 202.232.15.92
    ⊞ ns1.itojun.org: type A, class IN, addr 221.249.121.227
```

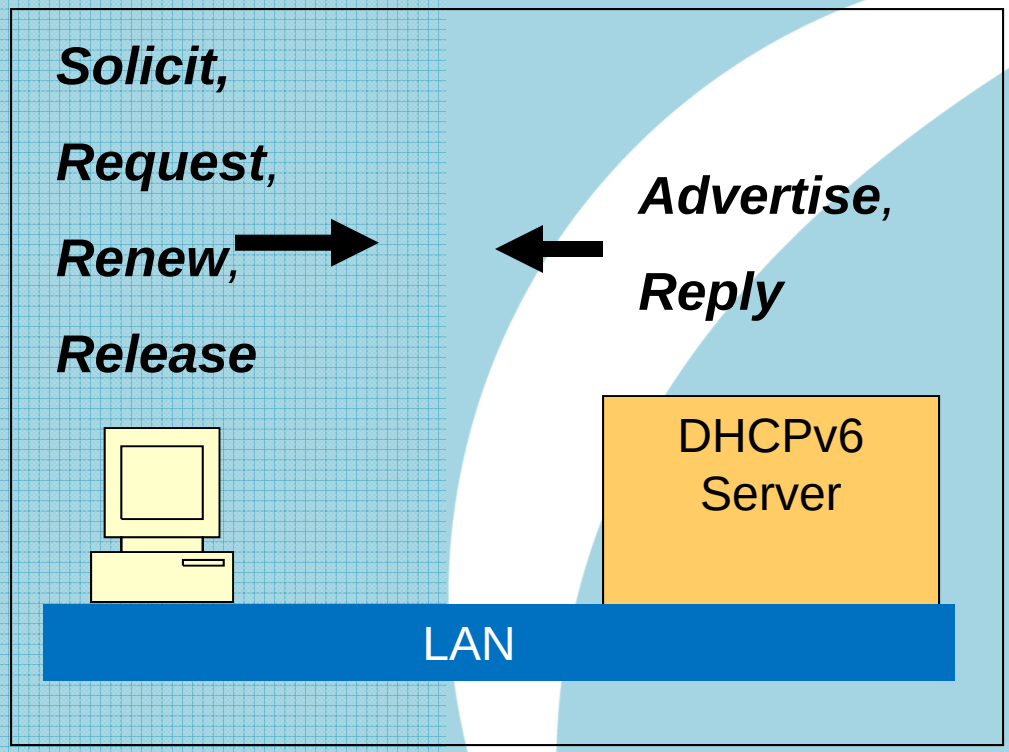
Query response packet generated by :

dig www.kame.net AAAA

No.	Time	Source	Destination	Protocol	Info
687	45.265137	192.168.1.100	Broadcast	ARP	Who has 192.168.1.1? Tell 0.0.0.0
3	5.495586	192.168.1.110	208.185.132.166	DNS	Standard query A www.yahoo-ht3.akadns.net
4	5.511737	208.185.132.166	192.168.1.110	DNS	Standard query response A 209.131.36.158
5	5.761619	192.168.1.110	128.9.0.107	DNS	Standard query PTR 166.132.185.208.in-addr.arpa
6	7.760591	192.168.1.110	128.9.0.107	DNS	Standard query PTR 107.0.9.128.in-addr.arpa
7	7.779552	192.168.1.110	192.203.230.10	DNS	Standard query PTR 166.132.185.208.in-addr.arpa
8	7.807188	192.203.230.10	192.168.1.110	DNS	Standard query response
9	7.807608	192.168.1.110	192.42.93.32	DNS	Standard query PTR 166.132.185.208.in-addr.arpa
10	7.824882	192.42.93.32	192.168.1.110	DNS	Standard query response
11	7.825340	192.168.1.110	192.26.92.30	DNS	Standard query A NS.ABOVE.NET
12	7.825444	192.168.1.110	192.26.92.30	DNS	Standard query A NS3.ABOVE.NET
13	7.909654	192.26.92.30	192.168.1.110	DNS	Standard query response A 207.126.96.162
14	7.909924	192.26.92.30	192.168.1.110	DNS	Standard query response A 207.126.105.146
15	7.910047	192.168.1.110	207.126.96.162	DNS	Standard query PTR 166.132.185.208.in-addr.arpa
16	7.926091	207.126.96.162	192.168.1.110	DNS	Standard query response PTR reserved.above.net.132.185.208.in-add
17	9.779463	192.168.1.110	192.203.230.10	DNS	Standard query PTR 1
18	9.802489	192.203.230.10	192.168.1.110	DNS	Standard query respo
19	9.802935	192.168.1.110	192.35.51.32	DNS	Standard query PTR 1
20	9.828373	192.35.51.32	192.168.1.110	DNS	Standard query respo
21	9.829057	192.168.1.110	65.114.168.20	DNS	Standard query A dns
22	9.829141	192.168.1.110	65.114.168.20	DNS	Standard query A bor
23	9.829205	192.168.1.110	65.114.168.20	DNS	Standard query A darkstar.isi.edu
24	9.919192	65.114.168.20	192.168.1.110	DNS	Standard query response A 128.9.64.64
25	9.919742	192.168.1.110	128.9.64.64	DNS	Standard query PTR 107.0.9.128.in-addr.arpa
26	9.920497	65.114.168.20	192.168.1.110	DNS	Standard query response A 128.9.160.161
27	9.921168	65.114.168.20	192.168.1.110	DNS	Standard query response A 128.9.128.127
28	9.959063	128.9.64.64	192.168.1.110	DNS	Standard query response PTR ns1.isi.edu
29	9.961158	192.168.1.110	192.31.80.32	DNS	Standard query PTR 10.230.203.192.in-addr.arpa
30	10.035037	192.31.80.32	192.168.1.110	DNS	Standard query response
31	10.035776	192.168.1.110	128.9.0.107	DNS	Standard query A ns.arc.nasa.gov
32	10.035885	192.168.1.110	128.9.0.107	DNS	Standard query A nasans1.nasa.gov
33	10.035976	192.168.1.110	128.9.0.107	DNS	Standard query A nasans4.nasa.gov
36	12.049499	192.168.1.110	198.32.64.12	DNS	Standard query A ns.arc.nasa.gov
37	12.049563	192.168.1.110	198.32.64.12	DNS	Standard query A nasans1.nasa.gov
38	12.049609	192.168.1.110	198.32.64.12	DNS	Standard query A nasans4.nasa.gov
39	12.080109	198.32.64.12	192.168.1.110	DNS	Standard query response
40	12.080744	192.168.1.110	66.135.32.100	DNS	Standard query A ns.arc.nasa.gov
41	12.089521	198.32.64.12	192.168.1.110	DNS	Standard query response
42	12.089638	198.32.64.12	192.168.1.110	DNS	Standard query response
43	12.089878	192.168.1.110	66.135.32.100	DNS	Standard query A nasans1.nasa.gov
44	12.090179	192.168.1.110	66.135.32.100	DNS	Standard query A nasans4.nasa.gov
45	12.150933	66.135.32.100	192.168.1.110	DNS	Standard query response
46	12.151338	192.168.1.110	198.116.144.49	DNS	Standard query A ns.arc.nasa.gov
47	12.152227	66.135.32.100	192.168.1.110	DNS	Standard query response
48	12.152345	66.135.32.100	192.168.1.110	DNS	Standard query response
49	12.152479	192.168.1.110	198.116.144.49	DNS	Standard query A nasans1.nasa.gov
50	12.152679	192.168.1.110	198.116.144.49	DNS	Standard query A nasans4.nasa.gov
51	12.248789	198.116.144.49	192.168.1.110	DNS	Standard query response A 128.102.16.2
52	12.249126	192.168.1.110	128.102.16.2	DNS	Standard query PTR 10.230.203.192.in-addr.arpa
53	12.253196	198.116.144.49	192.168.1.110	DNS	Standard query response A 192.77.84.32
54	12.253456	198.116.144.49	192.168.1.110	DNS	Standard query response A 198.116.144.33
55	12.266297	128.102.16.2	192.168.1.110	DNS	Standard query response PTR E.ROOT-SERVERS.NET
56	12.267671	192.168.1.110	192.26.92.32	DNS	Standard query PTR 32.93.42.192.in-addr.arpa

Packets generated by:
dig www.yahoo.com

DHCPv6 Basic Commands



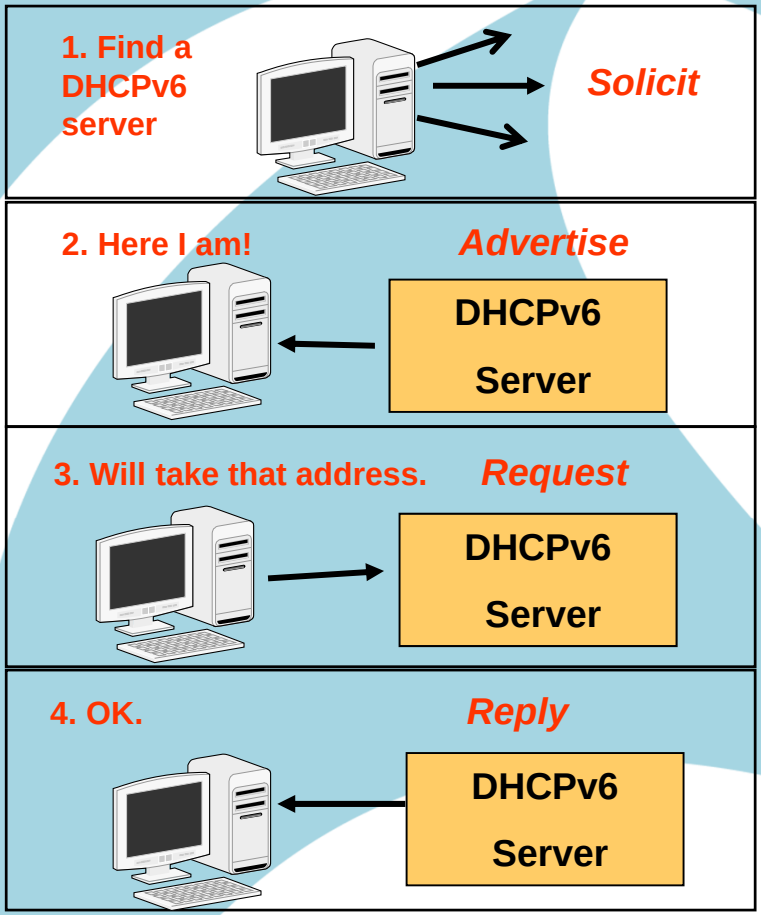
DHCPv6 Flow : Start

1. Client sends a ***Solicit*** message to All_DHCP_Relay_Agents_and_Servers (FF02::1:2)

2. DHCPv6 servers respond with ***Advertise*** messages.

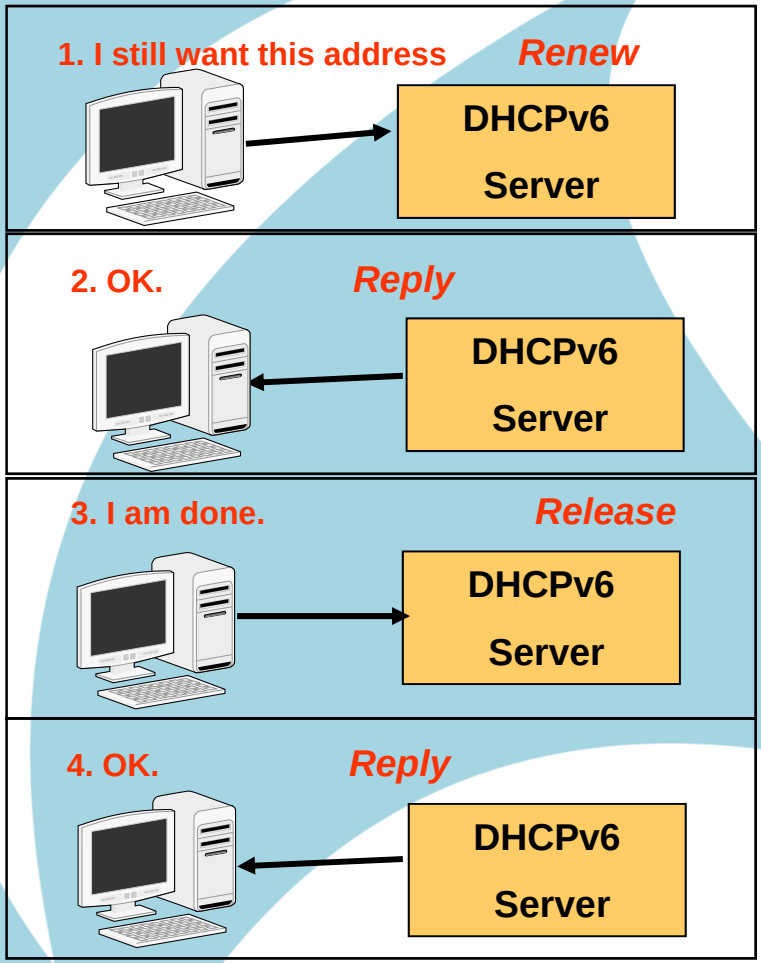
3. Client chooses a server and sends a ***Request*** message

4. DHCPv6 server responds with a ***Reply*** message



DHCPv6 Flow – Continue / End

1. Client sends a ***Renew*** message to DHCPv6 server
2. DHCPv6 server responds with ***Reply*** message.
3. Client sends a ***Release*** message to DHCPv6 server.
4. DHCPv6 server responds with a ***Reply*** message



Packets for Initialization

Generated for client getting address from DHCPv6 server

	Time	Source	Destination	Protocol	Info
22	7.703411	fe80::21d:9ff:febb:e960	ff02::1:2	DHCPv6	Solicit
23	7.748051	fe80::211:d8ff:fe39:292b	fe80::21d:9ff:febb:e960	DHCPv6	Advertise
27	9.750117	fe80::21d:9ff:febb:e960	ff02::1:2	DHCPv6	Request
28	9.776760	fe80::211:d8ff:fe39:292b	fe80::21d:9ff:febb:e960	DHCPv6	Reply

- Packet 22: ***Solicit*** from link-local of client to multicast All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
- Packet 23: ***Advertise*** from link-local of DHCPv6 server to link-local of client
- Packet 27: ***Request*** from link-local of client to multicast All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
- Packet 28: ***Reply*** from link-local of DHCPv6 server to link-local of client

No.	Time	Source	Destination
22	7.703411	fe80::21d:9ff:febb:e960	ff02::1:2

```
⊞ Frame 22 (112 bytes on wire, 112 bytes captured)
⊞ Ethernet II, Src: 00:1d:09:bb:e9:60 (00:1d:09:bb:e9:60), Dst: IPv6-Ne
⊞ Internet Protocol Version 6
⊞ User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547)
⊟ DHCPv6
    Message type: Solicit (1)
    Transaction-ID: 0x000041f8
  ⊟ Client Identifier
      option type: 1
      option length: 14
      DUID type: link-layer address plus time (1)
      Hardware type: IEEE 802 (6)
      Time: 266504608
      Link-layer address: 00:1d:09:bb:e9:60
  ⊟ Identity Association for Non-temporary Address
      option type: 3
      option length: 12
      IAID: 1
      T1: infinity
      T2: infinity
  ⊟ Elapsed time
      option type: 8
      option length: 2
      elapsed-time: 100 sec
  ⊟ Option Request
      option type: 6
      option length: 2
      Requested Option code: DNS recursive name server (23)
```

Solicit message from client

No.	Time	Source	Destination
23	7.748051	fe80::211:d8ff:fe39:292b	fe80::21d:9ff:febb:e960

```
⊞ Frame 23 (268 bytes on wire, 268 bytes captured)
⊞ Ethernet II, Src: AsustekC_39:29:2b (00:11:d8:39:29:2b), Dst: 00:1d:09:b
⊞ Internet Protocol Version 6
⊞ User Datagram Protocol, Src Port: 547 (547), Dst Port: 546 (546)
⊟ DHCPv6
    Message type: Advertise (2)
    Transaction-ID: 0x000041f8
  ⊟ Client Identifier
      option type: 1
      option length: 14
      DUID type: link-layer address plus time (1)
      Hardware type: IEEE 802 (6)
      Time: 266504608
      Link-layer address: 00:1d:09:bb:e9:60
  ⊟ Identity Association for Non-temporary Address
      option type: 3
      option length: 121
      IAID: 1
      T1: 2000
      T2: 3000
    ⊟ IA Address
        option type: 5
        option length: 24
        IPv6 address: 2000::3247:4cf3:37b1:a886
        Preferred lifetime: 3600
        Valid lifetime: 7200
```

Advertise message from server

```
⊟ Identity Association for Non-temporary Address
    option type: 3
    option length: 121
    IAID: 1
    T1: 2000
    T2: 3000
  ⊟ IA Address
      option type: 5
      option length: 24
      IPv6 address: 2000::3247:4cf3:37b1:a886
      Preferred lifetime: 3600
      Valid lifetime: 7200
  ⊟ Status code
      option type: 13
      option length: 77
      Status Code: Success (0)
      Status Message: 1 addr granted.
⊟ DNS recursive name server
    option type: 23
    option length: 32
    DNS servers address: 2000::ff
    DNS servers address: 2000::fe
```

2nd part of Advertise message from server

No.	Time	Source	Destination	Protocol	Info
27	9.750117	fe80::21d:9ff:febb	ff02::1:2	DHCPv6	Request

```
⊞ Frame 27 (158 bytes on wire, 158 bytes captured)
⊞ Ethernet II, Src: 00:1d:09:bb:e9:60 (00:1d:09:bb:e9:60), Dst: IPv6-Nei
⊞ Internet Protocol Version 6
⊞ User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547)
⊟ DHCPv6
    Message type: Request (3)
    Transaction-ID: 0x00005f89
  ⊟ Client Identifier
      option type: 1
      option length: 14
      DUID type: link-layer address plus time (1)
      Hardware type: IEEE 802 (6)
      Time: 266504608
      Link-layer address: 00:1d:09:bb:e9:60
  ⊟ Identity Association for Non-temporary Address
      option type: 3
      option length: 40
      IAID: 1
      T1: infinity
      T2: infinity
    ⊟ IA Address
        option type: 5
        option length: 24
        IPv6 address: 2000::3247:4cf3:37b1:a886
        Preferred lifetime: 3600
        Valid lifetime: 7200
  ⊟ Elapsed time
      option type: 8
      option length: 2
      elapsed-time: 300 sec
  ⊟ Option Request
      option type: 6
      option length: 2
      Requested Option code: DNS recursive name server (23)
```

Request message from client

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol
27	9.750117	fe80::21d:9ff:febb:e960	ff02::1:2	DHCPv6

```
⊞ Frame 27: 158 bytes on wire (1264 bits), 158 bytes capture
⊞ Ethernet II, Src: Dell_bb:e9:60 (00:1d:09:bb:e9:60), Dst:
⊞ Internet Protocol Version 6, Src: fe80::21d:9ff:febb:e960
⊞ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst
⊟ DHCPv6
    Message type: Request (3)
    Transaction ID: 0x005f89
  ⊞ Client Identifier: 000100060fe289a0001d09b
  ⊞ Identity Association for Non-temporary Address
  ⊞ Elapsed time
  ⊞ Option Request
  ⊟ Server Identifier: 000100060fd584940011d839292b
      Option: Server Identifier (2)
      Length: 14
      Value: 000100060fd584940011d839292b
      DUID type: link-layer address plus time (1)
      Hardware type: IEEE 802 (6)
```

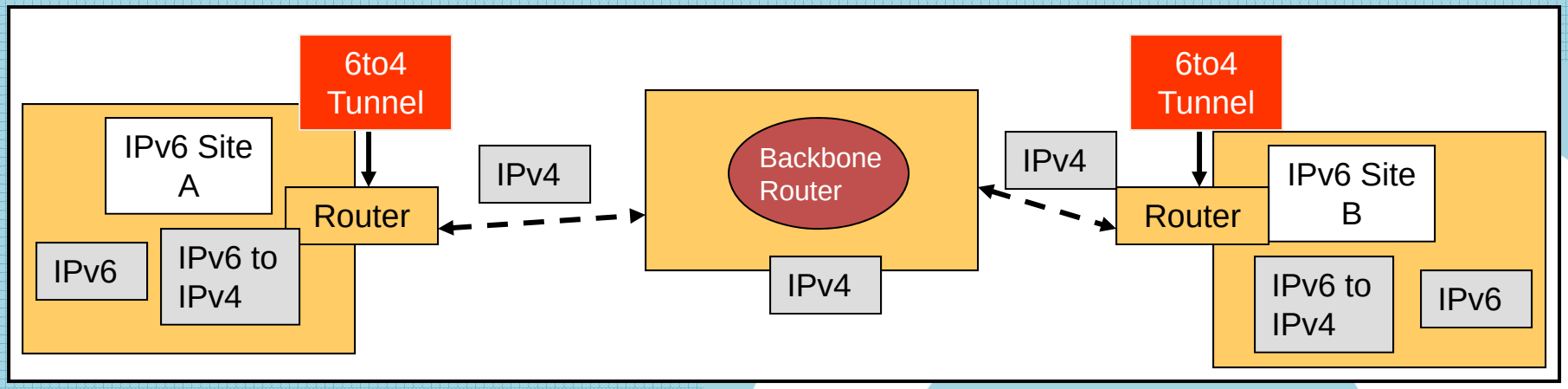
Request message from client showing Server Identifier

No.	Time	Source	Destination	Protocol	Info
28	9.776760	fe80::211:d8ff:fe3	fe80::21d:9ff:febb	DHCPv6	Reply

```
⊞ Frame 28 (216 bytes on wire, 216 bytes captured)
⊞ Ethernet II, Src: AsustekC_39:29:2b (00:11:d8:39:29:2b), Dst: 00:1d:09:bb
⊞ Internet Protocol Version 6
⊞ User Datagram Protocol, Src Port: 547 (547), Dst Port: 546 (546)
⊟ DHCPv6
    Message type: Reply (7)
    Transaction-ID: 0x00005f89
  ⊟ Client Identifier
      option type: 1
      option length: 14
      DUID type: link-layer address plus time (1)
      Hardware type: IEEE 802 (6)
      Time: 266504608
      Link-layer address: 00:1d:09:bb:e9:60
  ⊟ Identity Association for Non-temporary Address
      option type: 3
      option length: 74
      IAID: 1
      T1: 2000
      T2: 3000
    ⊟ IA Address
        option type: 5
        option length: 24
        IPv6 address: 2000::3247:4cf3:37b1:a886
        Preferred lifetime: 3600
        Valid lifetime: 7200
    ⊟ Status code
        option type: 13
        option length: 30
        Status Code: Success (0)
        Status Message: All addresses were assigned.
```

Reply message from server

6to4 Tunnels



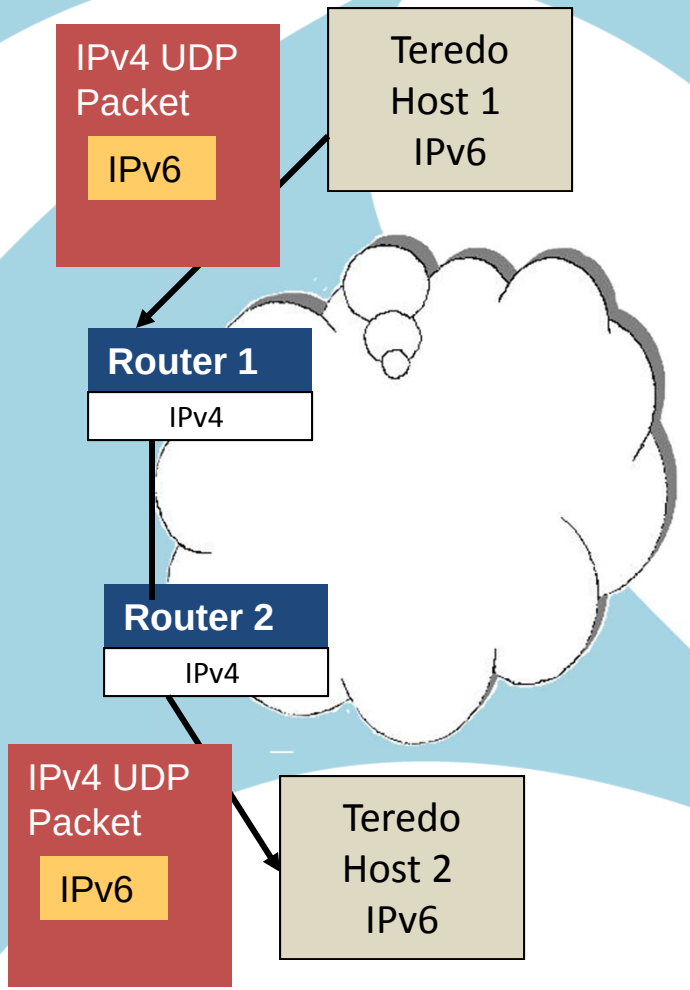
- **6to4** tunnels allow IPv6 packets over an IPv4 network.
- RFC 3056: Connection of IPv6 Domains via IPv4 Clouds.
- 6to4 is transition mechanism
- Operational differences
  - 6to4 interface automatically created in Windows XP and above
  - Most Unix implementations support 6to4
  - Cisco routers support 6to4 tunnels
  - z/OS Communications Server mainframe cannot be tunnel endpoint

```
⊞ Frame 154 (98 bytes on wire, 98 bytes captured)
⊞ Ethernet II, Src: 1a:43:20:00:01:00 (1a:43:20:00:01:00), Dst: 01:00:01:00:00:00 (01:00:0
⊟ Internet Protocol, Src: 139.18.25.33 (139.18.25.33), Dst: 81.131.67.131 (81.131.67.131)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 84
    Identification: 0x29fb (10747)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 16
    Protocol: IPv6 (0x29)
  ⊞ Header checksum: 0x474d [correct]
    Source: 139.18.25.33 (139.18.25.33)
    Destination: 81.131.67.131 (81.131.67.131)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 24
    Next header: TCP (0x06)
    Hop limit: 63
    Source address: 2001:638:902:1:201:2ff:fee2:7596
    Destination address: 2002:5183:4383::5183:4383
⊟ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1026 (1026), Seq: 0, Ack: 1
    Source port: ftp (21)
    Destination port: 1026 (1026)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 24 bytes
  ⊞ Flags: 0x0012 (SYN, ACK)
    Window size: 32768
    Checksum: 0x4194 [correct]
  ⊞ Options: (4 bytes)
  ⊞ [SEQ/ACK analysis]
```

IPv6 packet inside an IPv4 packet. Tunneling method is being used.

Why Teredo?

- Teredo does not need a router
- Tunneling issues with NAT
- NATs don't translate IPv6 packets in IPv4
- Teredo uses UDP encapsulation. (IPv6 packet becomes IPv4 UDP message
- UDP messages traverse multiple layers of NATs.
- Teredo is subject to the same security issues as any tunneled protocol



```
Frame 30: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: HonHaiPr_41:9c:20 (00:16:cf[illegible]:9c:20), Dst: 2wire_dc:
Internet Protocol Version 4, Src: 192.168.2.16 (192.168.2.16), Dst: 65.
User Datagram Protocol, Src Port: idps (3797), Dst Port: teredo (3544)
  Source port: idps (3797)
  Destination port: teredo (3544)
  Length: 60
  Checksum: 0xa6ad [validation disabled]
Teredo IPv6 over UDP tunneling
Internet Protocol Version 6, Src: 2001:0:4137:9e50:8000:f12a:b9c8:2815
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 12
  Next header: ICMPv6 (58)
  Hop limit: 21
  Source: 2001:0:4137:9e50:8000:f12a:b9c8:2815 (2001:0:4137:9e50:8000:f
  [Source Teredo Server IPv4: 65.55.158.80 (65.55.158.80)]
  [Source Teredo Port: 3797]
  [Source Teredo Client IPv4: 70.55.215.234 (70.55.215.234)]
  Destination: 2001:4860:0:2001::68 (2001:4860:0:2001::68)
```

IPv6 packet inside an IPv4 packet. Teredo tunneling method used.

Other IPv6 Sessions

- Sunday: 3:00 - Intro to IPv6 Addressing
- Tuesday: 4:45 - IPv6 Trace Analysis Using Wireshark
- Wednesday: 10:15 - IPv6 Security