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 has 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
<table>
<thead>
<tr>
<th>Next Header (Hex)</th>
<th>Next Header (Decimal)</th>
<th>Header Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Hop-by-Hop Options</td>
<td>For all devices on the path</td>
</tr>
<tr>
<td>2B</td>
<td>43</td>
<td>Routing</td>
<td>0 – Source Routing (deprecated) 2 – Mobile IPv6</td>
</tr>
<tr>
<td>2C</td>
<td>44</td>
<td>Fragment</td>
<td>Only when packet is fragmented</td>
</tr>
<tr>
<td>32</td>
<td>50</td>
<td>Encapsulated Security Payload (ESP)</td>
<td>IPSec encrypted data</td>
</tr>
<tr>
<td>33</td>
<td>51</td>
<td>Authentication Header (AH)</td>
<td>IPSec authentication</td>
</tr>
<tr>
<td>3C</td>
<td>60</td>
<td>Destination Options</td>
<td><a href="http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml">http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml</a> (Mobile IP, etc)</td>
</tr>
<tr>
<td>Size (bits)</td>
<td>Field Name</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Next Header</td>
<td>Contains the protocol number of the next header</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Length</td>
<td>Length of this header in octets (bytes)</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Options</td>
<td>8 bits for type, length in bytes, and then the option itself <a href="http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml">http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml</a></td>
<td></td>
</tr>
</tbody>
</table>

Remember: this has to be read by every device!
Frame 1693 (86 bytes on wire, 86 bytes captured)

- Ethernet II, Src: 192.168.1.1 (00:14:bf:ba:45:f9), Dst: ff02::2
  - 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: 0x000000
- 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
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>5762</td>
<td>80.385670</td>
<td>2001:4998:0:6::15</td>
<td>2607:f740:0:3f:216:3eff:fe68:72c0</td>
</tr>
</tbody>
</table>

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 (00:16:3e:68:72:c0)

  + 0110 .... = Version: 6  
  + .... 0000 0000 .... 0000 = Traffic class: 0x00000000  
  .... 0000 0000 0000 0000 1100 = Flowlabel: 0x0005410c

  **Payload length:** 1440
  **Next header:** IPv6 fragment (0x2c)
  **Hop limit:** 56

  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)]

- **Fragmentation Header**
  - **Next header:** TCP (0x06)
  - 0000 0000 0000 0... = offset: 0 (0x0000)
  - 0000 0000 0000 0... = 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
  - 0110 .... = Version: 6
  - .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  - .... .... 0000 0000 0000 0000 0000 = Flow label: 0x00000000
- Payload length: 40
- Next header: IPv6 destination option (60)
- Hop limit: 255
- Source SA MAC: Cisco_3c:90:2c (00:09:b7:3c:90:2c)]
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Destination Option
  - Next header: Mobile IPv6 (58) (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
- Mobile IPv6 / Network Mobility
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
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

- 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

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>3406</td>
<td>64.672910</td>
<td>2607:f4e8:130:202:225:90ff:fe01:a610</td>
<td>2607:f740:0:3f:216:3eff:fe68:72c0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2607:f4e8:130:202:225:90ff:fe01:a610</td>
<td></td>
</tr>
</tbody>
</table>

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)


- 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 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)
[PSHO/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

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

**Frame 25 (78 bytes on wire, 78 bytes captured)**

  - Source: AsustekC_39:29:2b (00:11:d8:39:29:2b)
  - Type: IPV6 (0x86dd)

**Internet Protocol Version 6**
- Version: 6
- Traffic class: 0x00
- Flowlabel: 0x000000
- 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

Muncie

Router Advertisement
Time: 10:45am To: ff02::1

Router Advertisement
Time: 11:00am To: ff02::1

Router Advertisement
Time: 11:15am To: ff02::1

Router Solicitation
11:08 am Haven’t heard from you in a while.
Router Advertisements contain:

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

Router Advertisement
Time: 10:45am
To: ff02::1
• Use AutoConfiguration
• Stateless
• Network Prefix: 2001:: /64
• I am default router
• For 200 seconds
• Hop limit: 126
• MTU: 4096
Router Advertisement Packet
- Source address
- Destination address
- ICMP type
- Hop limit
- Prefix length
- Prefix

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: 0x000000
  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

ICMPv6 options
  Type: 1 (Source link-layer address)
  Length: 8 bytes (1)
  Link-layer address: 00:14:bf:ba:45:f9
Router Solicitation (RS)

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

Router Solicitation
I need an address.
Please send a router advertisement

Router 1
Muncie
Router Solicitation Packet

- Source address
- Destination address
- ICMPv6 type
Neighbor Advertisements sent:

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>9.865886</td>
<td>fe80::2ff:8cffe:fe10:3976</td>
<td>2001:5c0:8fff:fffe:3f52</td>
<td>ICMPv6 Neighbor solicitation</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>9.865895</td>
<td>2001:5c0:8fff:fffe:3f52</td>
<td>fe80::2ff:8cffe:fe10:3976</td>
<td>ICMPv6 Neighbor advertisement</td>
<td></td>
</tr>
</tbody>
</table>

**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:8cffe: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)

  Source: AsustekC_39:29:2b (00:11:d8:39:29:2b)
  Type: IPV6 (0x86dd)

Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x000000
  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
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

<table>
<thead>
<tr>
<th>MLD message type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Listener Query</td>
<td>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.</td>
</tr>
<tr>
<td>Multicast Listener Report</td>
<td>Sent by a host when it joins a multicast group, or in response to a Multicast Listener Query sent by a router.</td>
</tr>
<tr>
<td>Multicast Listener Done</td>
<td>Sent by a host when it leaves a host group and might be the last member of that group on the network segment.</td>
</tr>
</tbody>
</table>
**Multicast Listener Report**

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1693</td>
<td>46.130640</td>
<td>::</td>
<td>ff02::2</td>
<td>ICMPv6</td>
<td>Multicast listener report</td>
</tr>
</tbody>
</table>

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:** 0x000000
  - **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 (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";
};
```
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)
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
  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
    Name: www.kame.net
    Type: AAAA (IPv6 address)
    Class: IN (0x0001)
    Time to live: 21 hours, 12 minutes, 26 seconds
    Data length: 16
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

<table>
<thead>
<tr>
<th>Frame 2 (74 bytes on wire, 74 bytes captured)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux cooked capture</td>
</tr>
<tr>
<td>Internet Protocol, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)</td>
</tr>
<tr>
<td>User Datagram Protocol, Src Port: 32770 (32770), Dst Port: domain (53)</td>
</tr>
<tr>
<td>Domain Name System (query)</td>
</tr>
<tr>
<td>Transaction ID: 0xfb48</td>
</tr>
<tr>
<td>Flags: 0x0100 (Standard query)</td>
</tr>
<tr>
<td>Questions: 1</td>
</tr>
<tr>
<td>Answer RRs: 0</td>
</tr>
<tr>
<td>Authority RRs: 0</td>
</tr>
<tr>
<td>Additional RRs: 0</td>
</tr>
<tr>
<td>Queries</td>
</tr>
<tr>
<td><a href="http://www.kame.net">www.kame.net</a>: type AAAA, class IN</td>
</tr>
<tr>
<td>Name: <a href="http://www.kame.net">www.kame.net</a></td>
</tr>
<tr>
<td>Type: AAAA (IPv6 address)</td>
</tr>
<tr>
<td>Class: IN (0x0001)</td>
</tr>
</tbody>
</table>

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
    Name: www.kame.net
    Type: AAAA (IPv6 address)
    Class: IN (0x0001)
    Time to live: 23 hours, 49 minutes, 40 seconds
    Data length: 16
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
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query A <a href="http://www.yahoo.com">www.yahoo.com</a></td>
</tr>
<tr>
<td>04/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response A 209.131.36.158</td>
</tr>
<tr>
<td>05/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query PTR 166.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>06/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query PTR 166.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>07/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response A 207.126.96.162</td>
</tr>
<tr>
<td>08/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response A 207.126.105.146</td>
</tr>
<tr>
<td>09/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR reserved.above.net.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>10/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR 192.123.203.192.in-addr.arpa</td>
</tr>
<tr>
<td>11/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR above.net.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>12/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR 192.123.203.192.in-addr.arpa</td>
</tr>
<tr>
<td>13/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR above.net.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>14/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR 192.123.203.192.in-addr.arpa</td>
</tr>
<tr>
<td>15/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR above.net.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>16/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR 192.123.203.192.in-addr.arpa</td>
</tr>
<tr>
<td>17/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR above.net.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>18/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR 192.123.203.192.in-addr.arpa</td>
</tr>
<tr>
<td>19/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR above.net.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>20/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR 192.123.203.192.in-addr.arpa</td>
</tr>
<tr>
<td>21/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR above.net.132.185.208.in-addr.arpa</td>
</tr>
<tr>
<td>22/</td>
<td>19.2.1.100</td>
<td>192.168.1.100</td>
<td>208.18.132.206</td>
<td>DNS</td>
<td>Standard query response PTR 192.123.203.192.in-addr.arpa</td>
</tr>
</tbody>
</table>
DHCPv6 Basic Commands

Solicit, Request, Renew, Release

LAN

DHCPv6 Server

Advertise, Reply
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.
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

- 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
Solicit message from client

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)
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>7.748051</td>
<td>fe80::211:d8ff:fe39:292b</td>
<td>fe80::21d:9ff:febb:e960</td>
</tr>
</tbody>
</table>

**Frame 23** (208 bytes on wire, 208 bytes captured)

- **Internet Protocol Version 6**
- **User Datagram Protocol**, Src Port: 547 (547), Dst Port: 546 (546)

**DHCPv6**

- **Message type**: Advertise (2)
- **Transaction-ID**: 0x0000041f8
- **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*
DHCPv6 Request

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 showing Server Identifier.
Frame 28 (216 bytes on wire, 216 bytes captured)
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:ee: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.
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
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
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