Managing an IPv6 Network: Deep Dive into ICMPv6

Laura Knapp
WW Business Consultant
Laurak@aesclever.com
Items to Be Discussed

- Error Messages
- Informational Messages
- Neighbor Discovery Protocol
- Multicast Listener Discovery Protocol
- Packet MTU Size
- Fragmentation
- Other ICMPv6 functions
IPv6: Auto configuration

Combination

ARP : ICMP router discovery : ICMP redirect

Neighbor discovery

Multicast and unicast datagrams
Establishes MAC address on same network
ICMPv6 router solicitation
ICMPv6 router advertisement
ICMPv6 neighbor solicitation
ICMPv6 redirect
ICMPv6 includes IGMP protocol for Multicast IP
Reduces impact of finding hosts

Stateless: router configures a host with IPv6 address
Stateful: DHCP for IPv6
Link Local Address: IPv6 connectivity on isolated LANs
ICMPv6 is more complicated than ICMPv4

Protocol consolidation occurred in IPv6

Additional messages have been added
ICMPv6

- ICMPv6 is used by IPv6 nodes to report errors encountered in processing packets, and to perform other internet-layer functions, such as diagnostics (ICMPv6 "ping")
- ICMPv6 is an integral part of IPv6 and MUST be fully implemented by every IPv6 node
- ICMPv6 messages are grouped into two classes:
  - error messages - Types 0-127
  - informational messages - Types 128-255
- IPv6 next ‘header’ value for ICMPv6 is 58
ICMPv6 Functions

Reports:

- packet processing errors
- intranetwork communications path diagnosis
- multicast membership

New functions:

- Neighbor Discovery
  - allows nodes on the same link to discover each other
  - allows nodes to discover each other’s addresses
  - finds routers for paths to other networks
  - determines the fully qualified name of a node
  - path MTU discovery determines the maximum path size along a path
ICMPv6 Header

Three Fields

**Type (8 bits)**
- Indicates the type of the message.
- If the high order bit = 0 (0 - 127) → error message
- If the high-order bit = 1 (128 – 255) → information message.

**Code ( 8 bits)**
- Content depends on the message type, and it is used to create an additional level of message granularity.

**Checksum (16 bits)**
- Used to detect errors in the ICMP message and in part of the IPv6 message.
ICMPv6 Messages

ICMPv6 messages are grouped into two classes:

• **Error messages**
  – To provide feedback to a source device about an error that has occurred.
  – Generated specifically in response to some sort of action, usually the transmission of a datagram.
  – Identified as such by having a zero in the high-order bit of their message.
  – Type field values 0 to 127

• **Informational messages**
  – Used to let devices exchange information, implement certain IP-related features, and perform testing.
  – Message Types from 128 to 255

Many of these ICMP types have a "code" field.
ICMPv6 Error Messages

<table>
<thead>
<tr>
<th>Type Value</th>
<th>Message Name</th>
<th>Summary Description of Message Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Destination Unreachable</td>
<td>Indicates that a datagram could not be delivered to its destination. <em>Code</em> value provides more information on the nature of the error.</td>
</tr>
<tr>
<td>2</td>
<td>Packet Too Big</td>
<td>Sent when a datagram cannot be forwarded because it’s too big for the MTU of the next hop in the route. This message is only needed in IPv6 because routers cannot fragment oversized messages in IPv6, but they can in IPv4.</td>
</tr>
<tr>
<td>3</td>
<td>Time Exceeded</td>
<td>Sent when a datagram has been discarded prior to delivery because the <em>Hop Limit</em> field was reduced to zero.</td>
</tr>
<tr>
<td>4</td>
<td>Parameter Problem</td>
<td>Indicates a miscellaneous problem (specified by the <em>Code</em> value) in delivering a datagram.</td>
</tr>
</tbody>
</table>
ICMPv6 Error Messages

ICMPv6 error messages:
1. Destination unreachable
   - code=0 no route to destination
   - code=1 communication with destination prohibited
   - code=2 (not assigned)
   - code=3 address unreachable
   - code=4 port unreachable
   - code=5 source address failed
   - code=6 reject route to destination

As much of received datagram as possible without exceeding the maximum IPv6 MTU

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: 1</td>
<td>Code: 0 to 6</td>
<td>Checksum</td>
<td>Unused (All 0s)</td>
</tr>
</tbody>
</table>

04/09/2013
## ICMPv6 Error Messages

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Message</th>
</tr>
</thead>
</table>
| 2    | 0    | Packet too big  
  code=0 next byte contains the maximum transmission MTU of the next hop |
| 3    | 0 or 1 | Time exceeded |
| 4    | 0, 1, 2 | Parameter problem  
  code=0 erroneous header field encountered  
  code=1 unrecognized next header type encountered  
  code=2 unrecognized IPv6 option encountered |

As much of received datagram as possible without exceeding the maximum IPv6 MTU
## ICMPv6 Informational Messages

<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td><em>Echo Request</em></td>
<td>Sent by a device to test connectivity to another device on the internetwork.</td>
<td>2463</td>
</tr>
<tr>
<td>129</td>
<td><em>Echo Reply</em></td>
<td>Sent in reply to an <em>Echo (Request)</em> message; used for testing connectivity.</td>
<td>2463</td>
</tr>
<tr>
<td>133</td>
<td><em>Router Solicitation</em></td>
<td>Prompts a router to send a <em>Router Advertisement</em>.</td>
<td>2461</td>
</tr>
<tr>
<td>134</td>
<td><em>Router Advertisement</em></td>
<td>Sent by routers to tell hosts on the local network the router exists and describe its capabilities.</td>
<td>2461</td>
</tr>
<tr>
<td>135</td>
<td><em>Neighbor Solicitation</em></td>
<td>Sent by a device to request the layer two address of another device while providing its own as well.</td>
<td>2461</td>
</tr>
<tr>
<td>136</td>
<td><em>Neighbor Advertisement</em></td>
<td>Provides information about a host to other devices on the network.</td>
<td>2461</td>
</tr>
<tr>
<td>137</td>
<td><em>Redirect</em></td>
<td>Redirects transmissions from a host to either an immediate neighbor on the network or a router.</td>
<td>2461</td>
</tr>
<tr>
<td>138</td>
<td><em>Router Renumbering</em></td>
<td>Conveys renumbering information for router renumbering.</td>
<td>2894</td>
</tr>
</tbody>
</table>
### ICMPv6 Informational Messages

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: 128</td>
<td>Code: 0</td>
<td>Checksum</td>
<td></td>
</tr>
<tr>
<td>Identifier</td>
<td>Sequence number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Optional data**
Sent by the request message; repeated by the reply message

**128 Echo request**
- code=0 and Identifier and sequence number carried

**129 Echo reply**
- code=0 and identifier and sequence number carried
ICMPv6 Neighbor Discovery Protocol (NDP)

Defined in RFC 2461

- Combines prior IPV4 functions
  - ARP (RFC 826)
  - Router Discovery (RFC 1256)
  - Redirect Message (RFC 792)

Mechanisms to:

- Discover routers
- Prefix discovery for on-link
- Parameter discovery (i.e. link MTU)
- Address auto-configuration
- Address resolution
- Next hop determination
- Neighbor unreachable
- Duplicate address
- Redirect
Main three functions:

1. Host-Router Functions
2. Host-Host Communication Functions
3. Redirect Function
NDP Functional Groups

Host-Router Discovery Functions

- Router Discovery
  - Core function of this group: the method by which hosts locate routers on their local network

- Prefix Discovery
  - Closely related to the process of router discovery
  - Determines what network they are on, which tells them how to differentiate between local and distant destinations and whether to attempt direct or indirect delivery of datagrams

- Parameter Discovery
  - A host learns important parameters about the local network and/or routers, such as the MTU of the local link.

- Address Auto-configuration
  - Hosts in IPv6 are designed to be able to automatically configure themselves, but this requires information that is normally provided by a router

Host-Host communications

- Address Resolution
  - The process by which a device determines the layer two address of another device on the local network from that device's layer three (IP) address
  - Performed by ARP in IP version 4.

- Next-Hop Determination
  - Looking at an IP datagram's destination address and determining where it should next be sent.

- Neighbour Unreachability Detection
  - Determining whether or not a neighbour device can be directly contacted

- Duplicate Address Detection (DAD)
  - Determining if an address that a device wishes to use already exists on the network

Redirect Function
- The technique whereby a router informs a host of a better next-hop node to use for a particular destination
ICMPv6 Router Solicitation/Advertisement

Router Solicitation (ICMPv6 Type 133)
Sent by hosts to request that any local routers send a Router Advertisement message so they don't have to wait for the next regular advertisement message.

Router Advertisement (ICMPv6 Type 134)
Sent regularly by routers to tell hosts that they exist and to provide them with important prefix and parameter Information.

Sent on periodic basis from router to the ‘all nodes address’
Hop limit should be 255
Could include security header
   M=1 use DHCP for address configuration
   O=1 use stateful protocol for address configuration
IPv6 Router Discovery

To forward packets to off-link destinations, Host A must discover the presence of Router 1

Host A sends a multicast Router Solicitation to the address FF02::2
Router Discovery Response

Router 1, having registered the multicast address of 33-33-00-00-00-02 with its Ethernet adapter, receives and processes the Router Solicitation. Router 1 responds with a unicast Router Advertisement message containing configuration parameters and local link prefixes.
ICMPv6 Neighbor Messages

Neighbor Solicitation (ICMPv6 Type 135)
- Nodes ask for link layer address of a target while providing their own link layer address to the target.
- Multicast to resolve an address in the range FF02::...:001:FF00:000 to FF02::...:001:FFF:FFF
- Take low order 32 bits of address and append to the following prefix: FF02::...:001.
- Unicast to verify the reachability of a neighbor.

Neighbor Advertisement (ICMPv6 Type 136)
- Sent by nodes in response to Neighbor solicitation message.
- Can be sent unsolicited to quickly ask for information
- Identify sender as router, destination address, or over-ride existing cache
To send a packet to Host B, Host A must use address resolution to resolve Host B’s link-layer address.
Host B, having registered the solicited-node multicast address of 33-33-FF-22-22-22 with its Ethernet adapter, receives and processes the Neighbour Solicitation. Host B responds with a unicast Neighbour Advertisement message.
Neighbor Solicitation and Advertisement

<table>
<thead>
<tr>
<th>ID</th>
<th>Timestamp</th>
<th>Datagram Size</th>
<th>Local IP</th>
<th>Rmt IP</th>
<th>Protocol</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>320</td>
<td>06:14:34:0405</td>
<td>72</td>
<td>2001:428:3604:0</td>
<td>FF02::1 FF00::1</td>
<td>ICMPv6</td>
<td></td>
</tr>
<tr>
<td>321</td>
<td>06:14:34:0460</td>
<td>161</td>
<td>10.2.0.236</td>
<td>239.255.256.250</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>322</td>
<td>06:14:34:0596</td>
<td>72</td>
<td>FE80::1</td>
<td>2001:428:3604:0</td>
<td>ICMPv6</td>
<td></td>
</tr>
</tbody>
</table>

Packet Details:

Packet ID: 322
Time: 4/10/2012 06:14:34:0596 HAT
IP Version 6
Source: 2001:428:3804:0:D78:D8B:886D:8A5A
Destination: FF02::FF00::1
Traffic Class: 0x000
Flow Label: 0x000
Payload Length: 32
Next Header (Protocol): ICMPv6
Hop Limit: 255

ICMPv6 Informational Message:
Type: Neighbor Solicitation (135)
Code: 0
Checksum: 0x98E8
Target Address: FE80::1

ICMPv6 Option:
   Type: Source Link_layer Address (1)
   Length: 8 bytes
   Link-layer address: EC:55:F9:C1:E1:51

ICMPv6 Option:
   Type: Target Link_layer Address (2)
   Length: 8 bytes
   Link-layer address: 00:08:E2:60:18:1A
Neighbor Discovery Table

Adding a Static Entry in the Neighbour Discovery Table (Cisco Feature)
IPv6 Auto-configuration

- Host 1 comes on line and generates a link local address.
- Host 1 sends out a query called neighbor discovery to the same address to verify uniqueness. If there is a positive response, a random number generator is used to generate a new address.
- Host 1 multicasts a router solicitation message to all routers.
- Routers respond with a router advertisement that contains the IPv6 Address prefix and other information.
- Host 1 automatically configures its global address by appending its interface ID to the AGA
- Host 1 can now communicate
Prefix Advertisement

Packet Summary

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>132</td>
<td>06:13:39:2874</td>
<td>104</td>
<td>FE80::1</td>
<td>FF02::1</td>
<td>ICMPv6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Packet Details

Packet ID: 132
Time: 4/10/2012 06:13:39:2874 HAT

IP Version 6
Source: FE80::1
Destination: FF02::1
Traffic Class: 0x0000
Flow Label: 0x0000
Payload Length: 64
Next Header (Protocol): ICMPv6
Hop Limit: 255

ICMPv6 Informational Message:
Type: Router Advertisement (134)
Code: 0
Checksum: 0xC673
Cur hop limit: 64
Flags:
1... .... = Managed address configuration: Set
.0... .... = Other configuration: Not Set
.0... .... = Home Agent: Not Set
...0 0... = Default Router Preference: Medium
..... 0... = Proxy: Not Set
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0

ICMPv6 Option
Type: Source Link Layer Address (1)
Length: 8 bytes
Link-layer address: 00:06:E2:60:18:1A

ICMPv6 Option
Type: MTU (5)
Length: 8 bytes
MTU: 1500

ICMPv6 Option
Type: Prefix Information (3)
Length: 32 bytes
Prefix Length: 64
Flags:
1... = On-link flag (L): Set
.1... = Autonomous address-configuration flag (A): Set
Valid Lifetime: 2592000
Preferred Lifetime: 604800
Prefix (IPv6 address): 2001:428:3804::
### ICMPv6 Redirect

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: 137</td>
<td>Range: 0-255, Indicates a redirect is needed</td>
</tr>
<tr>
<td>Code: 0</td>
<td>Range: 0-255, Indicates a redirect is needed</td>
</tr>
<tr>
<td>Checksum</td>
<td>Range: 0-65535, Entropy check for message</td>
</tr>
<tr>
<td>Reserved</td>
<td>Range: 0-65535, Not used for this protocol</td>
</tr>
<tr>
<td>Target</td>
<td>Range: 0-65535, Physical address of target</td>
</tr>
<tr>
<td>Destination</td>
<td>Range: 0-65535, IP address of destination</td>
</tr>
<tr>
<td>Options</td>
<td>Range: 0-65535, Additional information</td>
</tr>
</tbody>
</table>

An option is added to let the host know the target router’s physical address.
1. A router informs an originating host of the IP address of a router available on the local link that is “closer” to the destination.

“Closer” is routing metric function used to reach the destination network segment. This condition can occur when there are multiple routers on a network segment and the originating host chooses a default router and it is not the best one to use to reach the destination.

2. A router informs an originating host that the destination is a neighbour (it is on the same link as the originating host).

This condition can occur when the prefix list of a host does not include the prefix of the destination. Because the destination does not match a prefix in the list, the originating host forwards the packet to its default router.
To inform Host A that subsequent packets to the destination of FEC0::2:2AA:EE:FE99:9999 should be sent to Router 2, Router 1 sends a Redirect message to Host A
ICMPv6 Multicast Listener (MLD)

Took pieces from IGMP (Internet Group Management Protocol) (RFC 1112 and RFC 2236) and merged into new protocol

Defined in RFC 2710.

MLD is a sub-protocol of ICMPv6.

Allows routers to discover nodes that wish to receive multicast packets on all the routers links

Query can be general or specific:

- Tell me all nodes with multicast address x
- Tell me all nodes and their multicast addresses

Maximum response delay only is used with the Query message
### Trace Multicast Listener Query

<table>
<thead>
<tr>
<th>ID</th>
<th>Timestamp</th>
<th>Datagram Size</th>
<th>Loc</th>
<th>Query Builder</th>
<th>Packet Summary</th>
<th>Session Summary</th>
<th>Packet Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>380</td>
<td>06:14:42:4013</td>
<td>72</td>
<td>FE60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>381</td>
<td>06:14:42:5287</td>
<td>78</td>
<td>10.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Packet Details

<table>
<thead>
<tr>
<th>Hex Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet ID : 380</td>
</tr>
<tr>
<td>CTRACE Header</td>
</tr>
<tr>
<td>IPv6 Header</td>
</tr>
<tr>
<td>ICMPv6 Header</td>
</tr>
<tr>
<td>RU Data</td>
</tr>
</tbody>
</table>

- **Type – 3A (ICMPv6)**
- **Code – 00**
- **Checksum -0502**
- **82=130=MLQ**
- **Maximum Response Delay= 27 10 hex= 10000ms**

**Multicast Listener Report**

<table>
<thead>
<tr>
<th>ID</th>
<th>Timestamp</th>
<th>Datagram Size</th>
<th>Local IP</th>
<th>Rmt. IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>380</td>
<td>06:14:42:4013</td>
<td>72</td>
<td>FE80::D2D0:FD1</td>
<td>FF02::1</td>
</tr>
<tr>
<td>381</td>
<td>06:14:42:5237</td>
<td>78</td>
<td>10.2.0.123</td>
<td>10.2.255.255</td>
</tr>
<tr>
<td>382</td>
<td>06:14:42:7249</td>
<td>72</td>
<td>FE80::E488:BE1</td>
<td>FF02::1:3</td>
</tr>
</tbody>
</table>

---

83 = 131 decimal = MLR

Maximum Response Delay = 00 00 hex = 0ms

Multicast Address FF02::1:3
ICMPv6 Path MTU Discovery

RFC 1981

To enable hosts to discover the min. MTU on a path to a particular destination

Fragmentation in IPv6 is not performed by intermediary routers

The source node may fragment packets by itself only when the path MTU is smaller than the packets to deliver

PMTUD for IPv6 uses ICMPv6 error message
  • Type 2 Packet Too Big

MTU Size Error Feedback
  • If a router is forced to try sending a datagram that is too large over a physical link, it must drop the datagrams, since it cannot fragment them
  • A feedback process has been defined using ICMPv6 that lets routers tell source devices when the datagrams they are using are too large for the route
How Does a Node know what MTU size to Use?

1. **Use Default MTU**
   Use the default MTU of **1280**, which all physical networks must be able to handle.

2. **Use Path MTU Discovery feature**
   A node sends messages over a route to determine the overall minimum MTU.
For purposes of fragmentation, IPv6 datagrams are broken into two pieces:

- **Un-fragment-able Part**
  Includes the main header of the original datagram + any extension headers that need to be present in each fragment - *Hop-By-Hop Options, Destination Options* (for those options to be processed by devices along a route) and *Routing*.

- **Fragment-able Part**
  Data portion of the datagram + other extension headers if present - *authentication Header, Encapsulating Security Payload* and/or *Destination Options* (for options to be processed only by the final destination).

The **Un-fragment-able Part** must be present in each fragment, while the **Fragment-able Part** is split up amongst the fragments.
Suppose we need to send this over a link with an MTU of only 230 bytes. Three fragments are created. This is due to the need to put the two 30-byte un-fragment-able extension headers in each fragment and the requirement that each fragment be a length that is a multiple of 8.

Fragmentation Example

Fragment #1: The first fragment would consist of the 100-byte *Un-fragment-able Part*, followed by an 8-byte *Fragment* header and the first 120 bytes of the *Fragment-able Part* of the original datagram. This would contain the two fragment-able extension headers and the first 60 bytes of data.

Fragment #2: This would also contain the 100-byte *Un-fragment-able Part*, followed by a *Fragment* header and 120 bytes of data (bytes 60 to 179).

Second Fragment: This would also contain the 100-byte *Un-fragment-able Part*, followed by a *Fragment* header and 120 bytes of data (bytes 60 to 179).
ICMPv6 Model Host

Each host is to maintain the following:

- Neighbor Cache
- Destination Cache
- Prefix List
- Default Router List
- LinkMTU
- CurHopLimit
- BaseReachable Time
- Reachable Time
- Retransmit Timer
Changes Needed to Implement IPv6

Hosts
- Implement IPv6 code in operating system
- TCP/UDP aware of IPv6
- Sockets/Winsock library updates for IPv6
- Domain Name Server updates for IPv6

Domain Name Server (DNS)
- Many products already support 128 bit addresses
- Uses ‘AAAA’ records for IPv6
- IP6.INT (in_addr_arpa in IPv4)

Routers
- IPv6 forwarding protocols
- Routing protocols updated to support IPv6
- Management needs to support ICMPv6
- Implement transition mechanisms

IPv6 Protocol Status
- RIPv6 - Same as RIPv2
- OSPFv6 - Updated for IPv6
- EIGRP - Extensions implemented
- IDRP - Recommended for exterior protocol over BGP4
- BGP4+ - Preferred implementation in IPv6 today
Gracias

laurak@aesclever.com
www.aesclever.com
650-617-2400
IPv6 References

IPv6 Home Page

http://www.ietf.org/
http://www.getipv6.info/
http://www.ipv6forum.com
http://arin.net
http://www.internet2.edu
http://www.ipv6.org
http://test-ipv6.com/
http://www.ipv6.com/

Books
Internetworking IPv6 with Cisco Routers - ISBN 0-07-022831-1
IPv6 RFCs

View any IPv6 RFC

http://datatracker.ietf.org/doc/search/