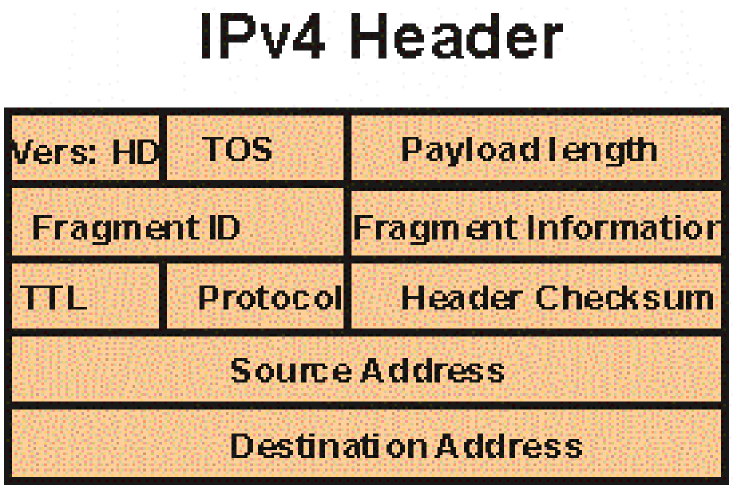
IPv6 : Deep Dive
Share Session 11164

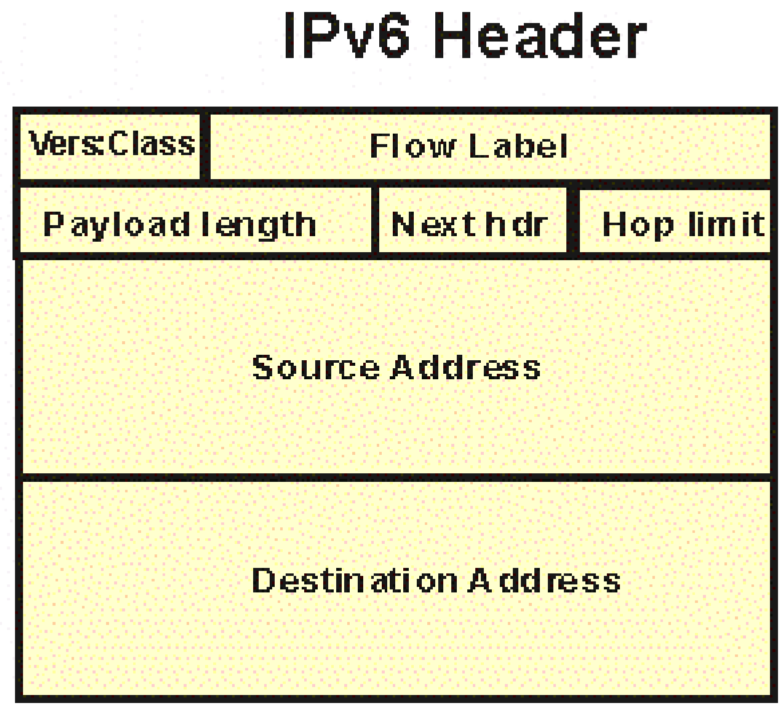
Laura Knapp
WW Business Consultant
Laurak@aesclever.com

What is IPv6

Addressing	128 bits addresses hierarchically assigned
Routing	Strongly hierarchical (route aggregation)
Performance	Simple datagram
Extensibility	New flexible option header format
	Improved support for extensions and options
Multimedia	Better support for QoS
Multicast	Compulsory-better scope control
Security	Built in security (IPSEC)
Auto-configuration	Stateless and state-full address configuration
Mobility	Better efficiency and security

IPv6 Header





IPv4 header is 20 bytes : IPv6 header is 40 bytes
Address increased from 32 to 128 bits
Fragmentation fields moved out of base header
Header checksum
Time to Live replaced with 'Hop Limit'
Protocol replaced with 'Next Header'
TOS replaced with 'Flow Label'
Alignment changed from 32 to 64 bits

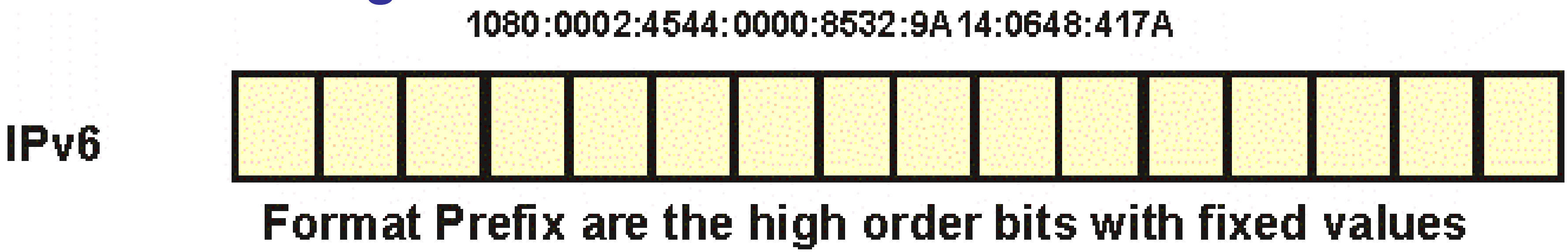
Items to Be Discussed

IP Addressing

ICMPv6

- **Error Messages**
- **Informational Messages**
- **Neighbor Discovery Protocol**
- **Multicast Listener Discovery Protocol**
- **Packet MTU Size**
- **Fragmentation**
- **Other ICMPv6 functions**

Addressing Format



Defined in RFC 3513

40,282,366,920,938,463,374,607,431,768,211,456 addresses

40 trillion trillion trillion addresses

Addresses are assigned to interfaces

Multiple address can be defined to a single interface

Address structure

Ipv6 address = Prefix + Interface id

Separation of ‘who you are’ from ‘where you are connected’

Assignments by ARIN, APNIC, RIPE

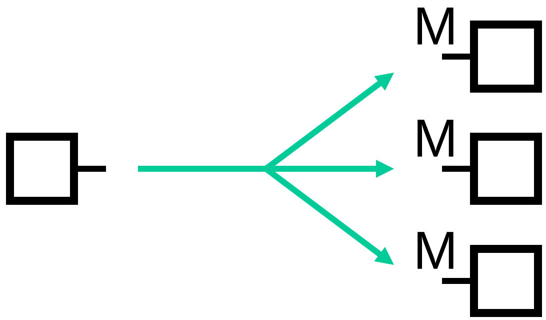
IPv6 Address Types

unicast:

for one-to-one communication

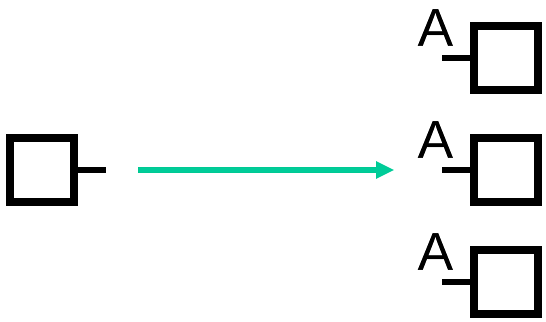
multicast:

for one-to-many communication

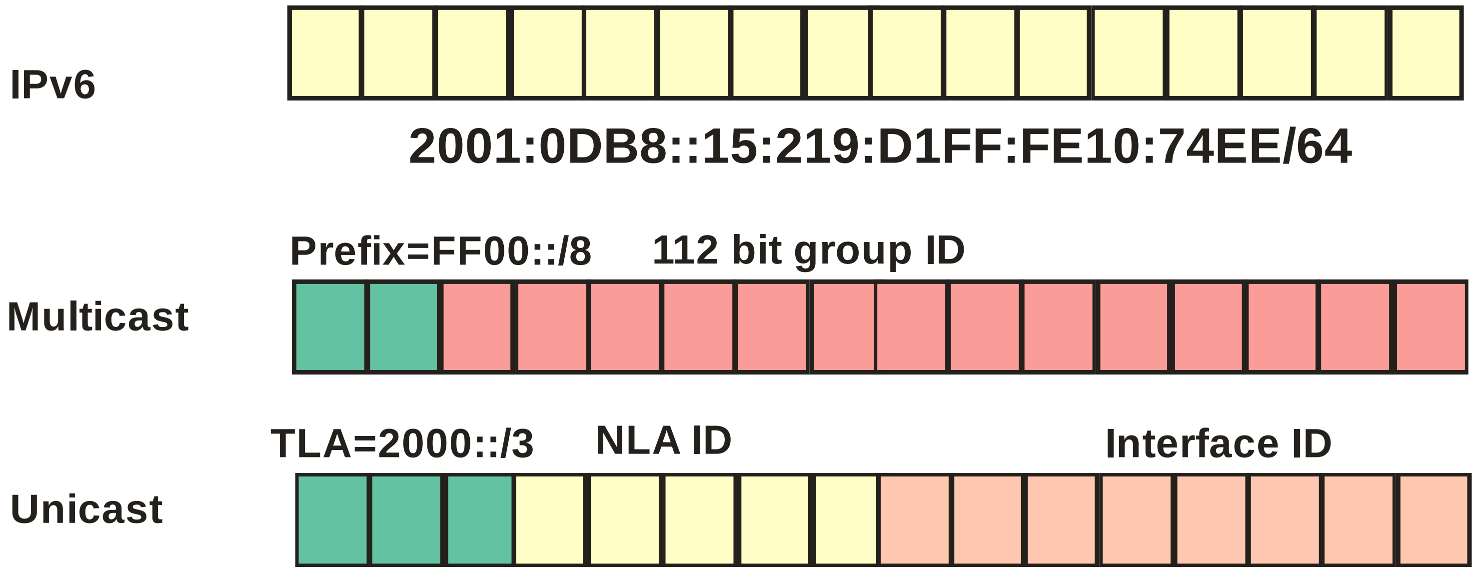


anycast:

for one-to-nearest communication



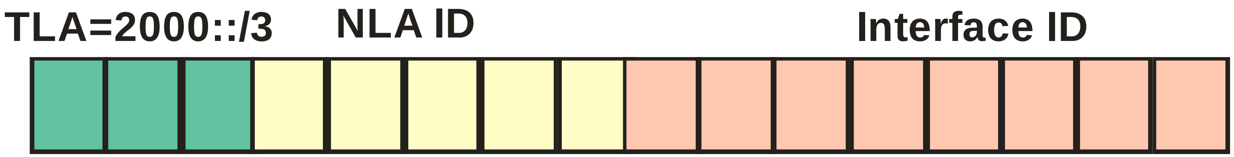
IPv6 Address: Site and Link



2001:0408/32 ATT
2001:0506:0000/48 Verizon Business
2001:4840/32 Earthlink
2001:49C0/32 IBM
2001:0200--039F 12 ISPs in Korea

FC00::/7 Unique Local – Internet router will discard
FE80::/10 Link Local – Non-routeable

Global Unicast Address



TLA : Top Level Aggregation - 3 bytes (21 bits; First three bits of byte 1 are 001)
IANA allocates address blocks to the regional Internet registries
They allocate portions of their block to national registries or to ISPs

NLA : Next Level Aggregation - 5 bytes
High order part assigned to smaller or regional ISPs, large companies
Holders of an NLA block assign partsof their block to their customers
They assign middle chunks to locations
Low order numbers identify subnets

Interface ID : host interface (64 bits)
Assigned by the owning organization
IEEE has defined a 64 bit NIC address known as EUI-64
NIC driver for IPv6 will convert 48 bit NIC to 64 bit NIC

Structure greatly reduces the entries in the routing table....only one entry needed in a US router to define all the networks in a region or country

Address Type Prefixes

- Unspecified
  - used when there is no address
- Loopback
- Link Local Unicast
- Multicast
- Unicast + Anycast
  - hierarchical
  - /13 - /32 to LIR's (ISP's)
  - /48 or /56 to endusers / sites

  - “Site Local” used to exist (fec0::/10) but this has been deprecated in favor of ULA

http://www.iana.org/assignments/ipv6-address-space

0000 .... 0000 (::/128)

0000 .... 0001 (::1/128)

1111 1110 1000 0000 .... (fe80::/16)

1111 1111 .... (ffxx::/8)

The rest, 2000::/3, which is 1/8th of total IPv6 space

2001::/16 = RIRs

2001::/32 = Teredo

2002::/16 = 6to4

3ffe::/16 = 6bone*

fd00::/8 = ULA

* = 6bone shut down on 6/6/6

Items to Be Discussed

IP Addressing

ICMPv6

- **Error Messages**
- **Informational Messages**
- **Neighbor Discovery Protocol**
- **Multicast Listener Discovery Protocol**
- **Packet MTU Size**
- **Fragmentation**
- **Other ICMPv6 functions**

IPv6: Autoconfiguration

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

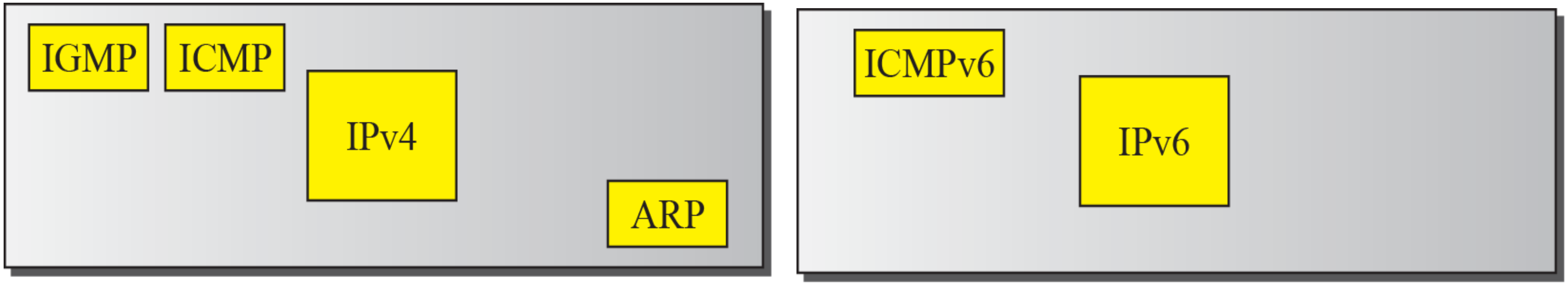
Reduces impact of finding hosts

Stateless: router configures a host with IPv6 address

Stateful: DHCP for IPv6

Link Local Address: IPv6 connectivity on isolated LANs

ICMPv4 and ICMPv6 Quick View



Network layer in version 4

Network layer in version 6

ICMPv6 is more complicated than ICMPv4

Protocol consolidation occurred in IPv6

Additional messages have been added

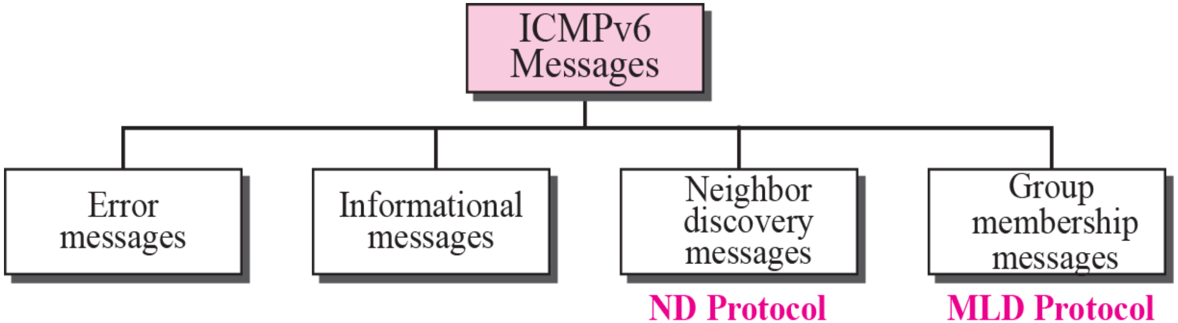
ICMPv6

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

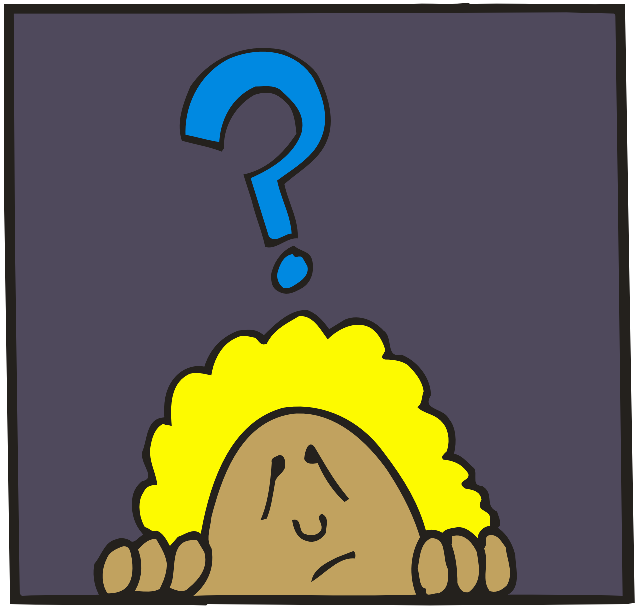
ICMPv6 messages are grouped into two classes:
error messages - Types 0-127
informational messages - Types 128-255

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 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.

MAC header	IPv6 header	ICMPv6 header	ICMPv6 message

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Type</td><td colspan="8">Code</td><td colspan="16">Checksum</td></tr>
<tr><td colspan="32">ICMPv6 message
...</td></tr>
</table>

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.

Error messages

Type	Description	References
1	Destination unreachable:	RFC 2463
2	Packet too big.	RFC 2463
3	Time exceeded.	RFC 2463
4	Parameter problem.	RFC 2463

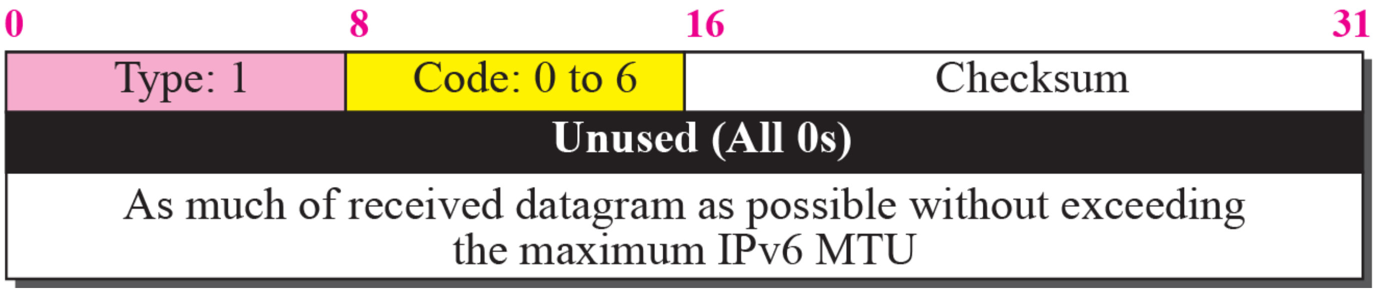
Informational messages

Type	Description	References
128	Echo request.	RFC 2463
129	Echo reply.	RFC 2463

ICMPv6 Error Messages

Type Value	Message Name	Summary Description of Message Type
1	Destination Unreachable	Indicates that a datagram could not be delivered to its destination. *Code* value provides more information on the nature of the error.
2	Packet Too Big	Sent when a datagram cannot be forwarded because it is too big for the MTU of the next hop in the route. This message is needed in IPv6 and not IPv4 because in IPv4, routers can fragment oversized messages, while in IPv6 they cannot.
3	Time Exceeded	Sent when a datagram has been discarded prior to delivery due to the *Hop Limit* field being reduced to zero.
4	Parameter Problem	Indicates a miscellaneous problem (specified by the *Code* value) in delivering a datagram.

ICMPv6 Error Messages

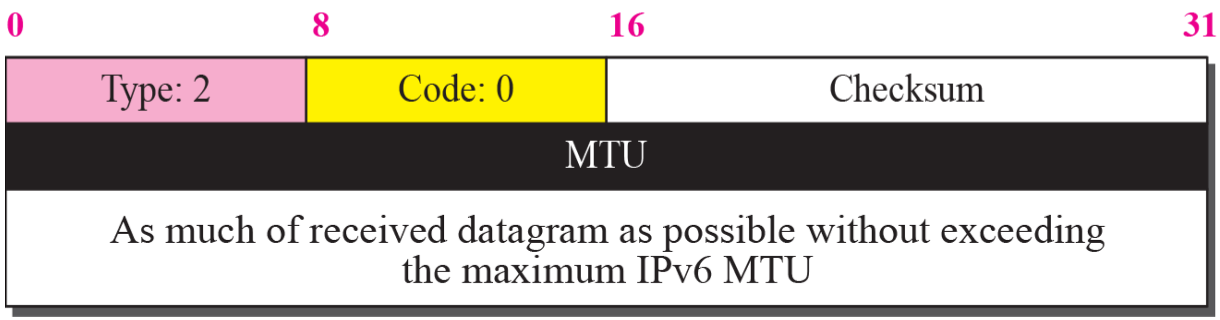


ICMPv6 error messages:

1 Destination unreachable

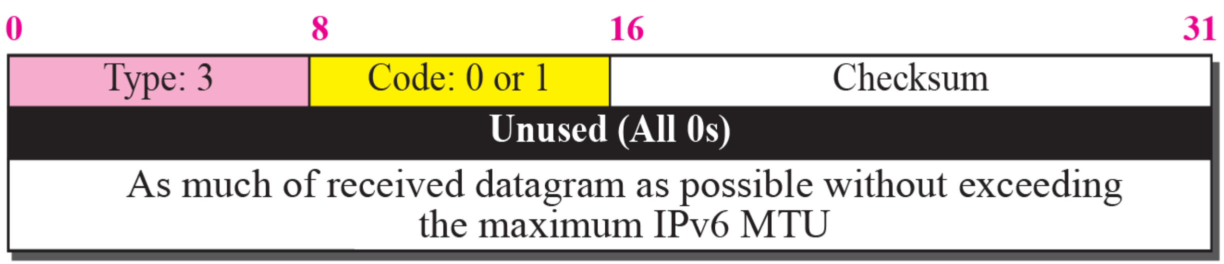
code=0 no route to destination
code=1 communication with destination prohibited
code=2 (not assigned)
code=3 address unreachable
code=4 port unreachable
code=5 source address failed
code=6 reject route to destination

ICMPv6 Error Messages

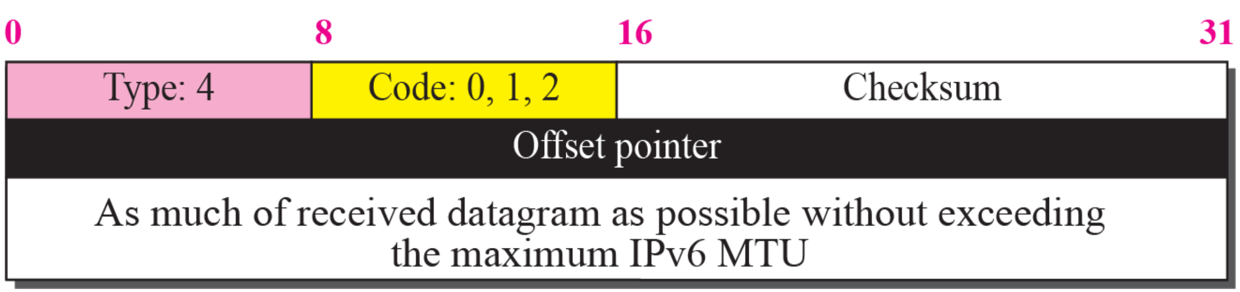


2 Packet too big

code=0 next byte contains the maximum transmission MTU of the next hop



3 Time exceeded



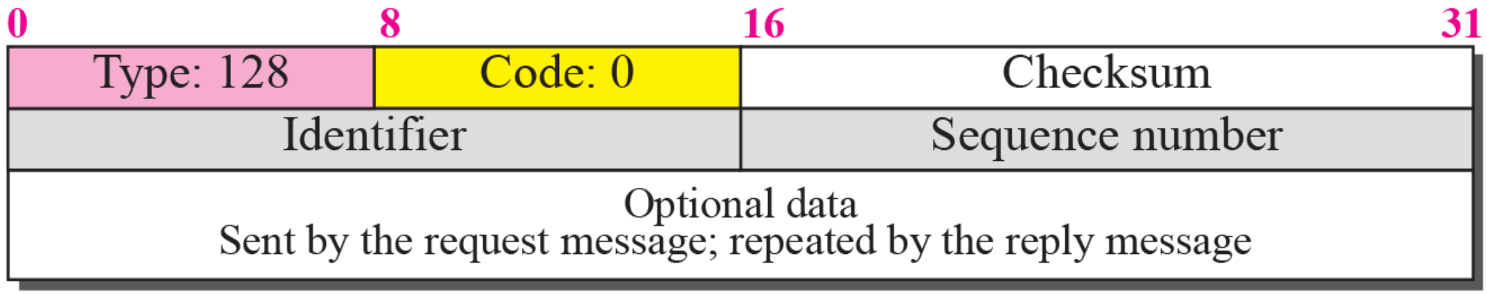
4 Parameter problem

code=0 erroneous header field encountered
code=1 unrecognized next header type encountered
code=2 unrecognized IPv6 option encountered

ICMPv6 Informational Messages

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

ICMPv6 Informational Messages

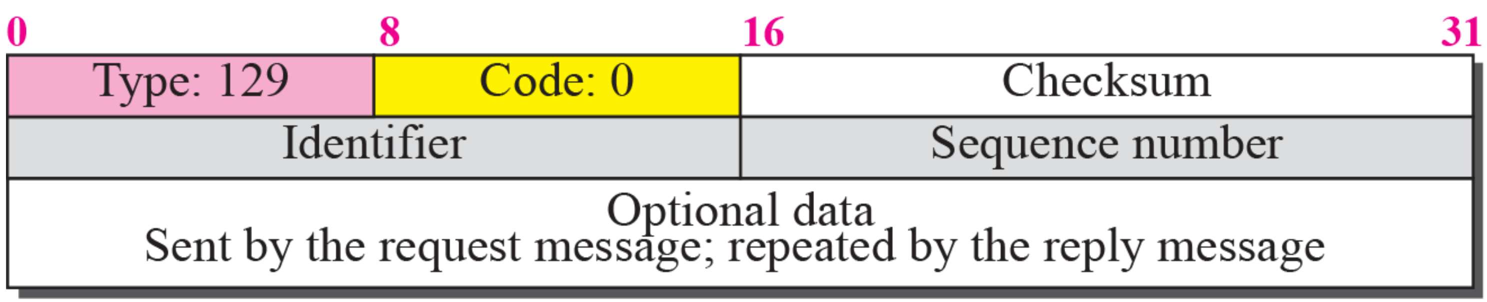


128 Echo request

code=0 and Identifier and sequence number carried

129 Echo reply

code=0 and identifier and sequence number carried



ICMPv6 Neighbor Discovery Protocol (NDP)

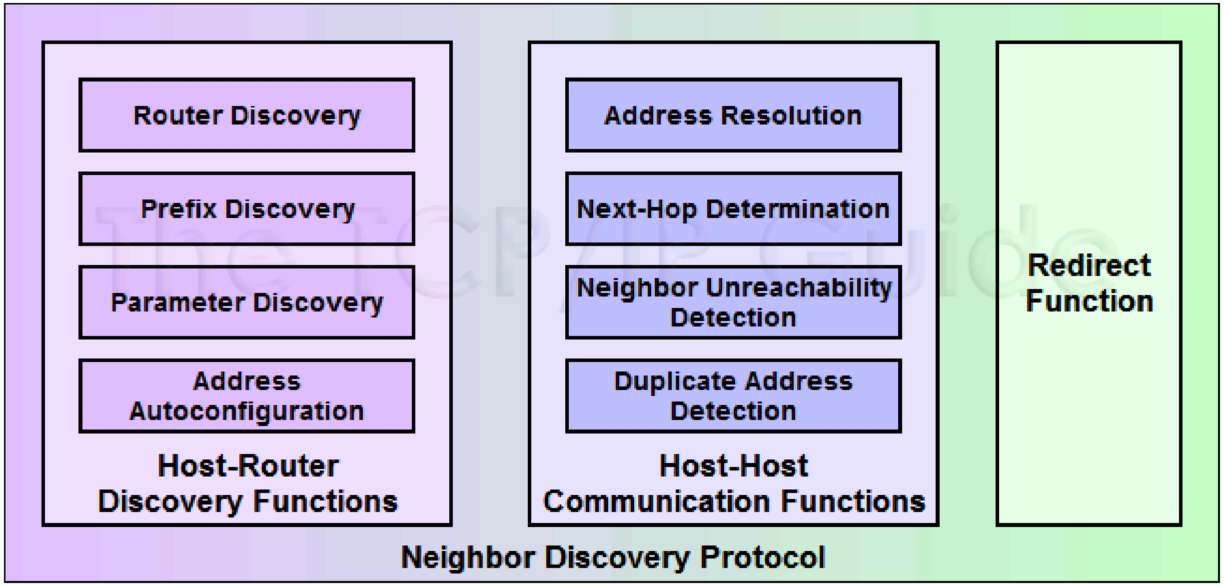
Defined in RFC 2461

- 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 autoconfiguration
- Address resolution
- Next hop determination
- Neighbor unreachable
- Duplicate address
- Redirect

NDP Groups



Mainly 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 is prefix discovery.
  - To determine what network they are on, which in turn 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 Autoconfiguration**
  - 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

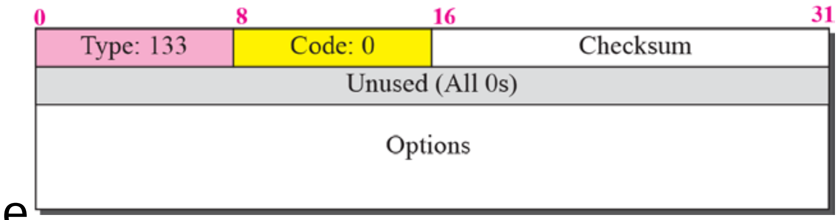
- **Address Resolution**
  - The process by which a device determines the layer two address of another device on the local network from that device's layer three (IP) address.
  - Performed by ARP in IP version 4.
- **Next-Hop Determination**
  - Looking at an IP datagram's destination address and determining where it should next be sent.
- **Neighbor Unreachability Detection**
  - Determining whether or not a neighbor 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

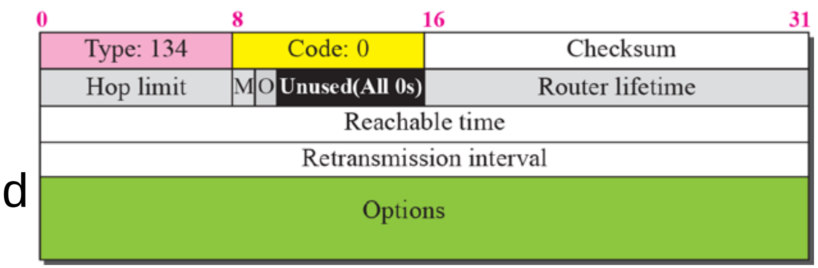
ICMPv6 Router Solicitation/Advertisement

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

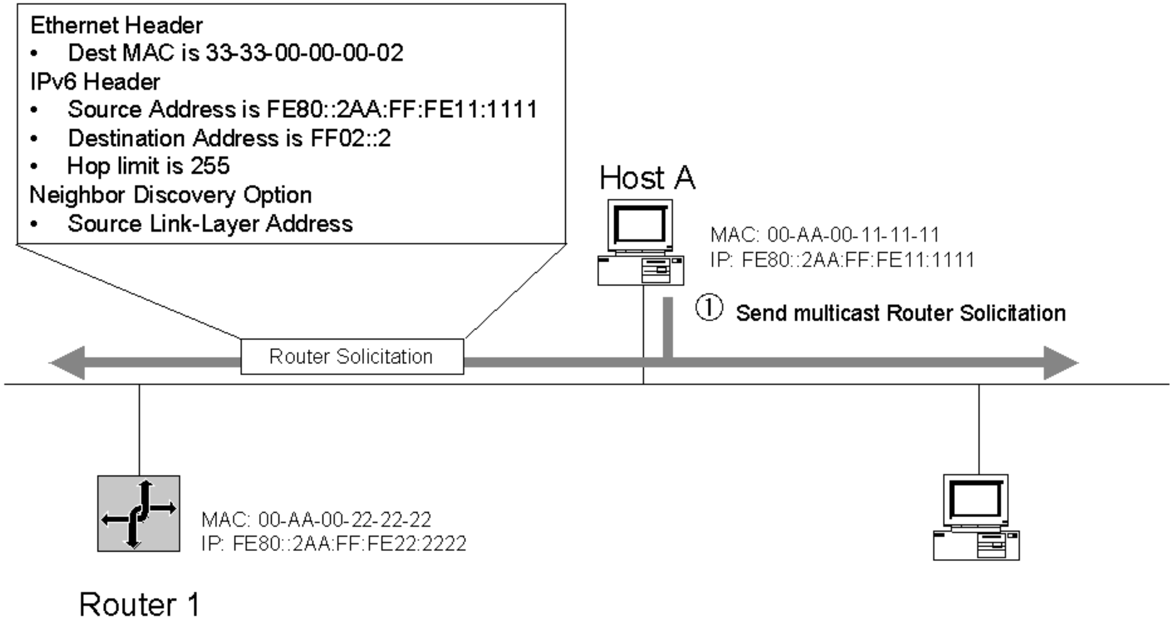
Router Advertisement (ICMPv6 Type 134)



Sent regularly by routers to tell hosts that they exist and provide important prefix and parameter information to them

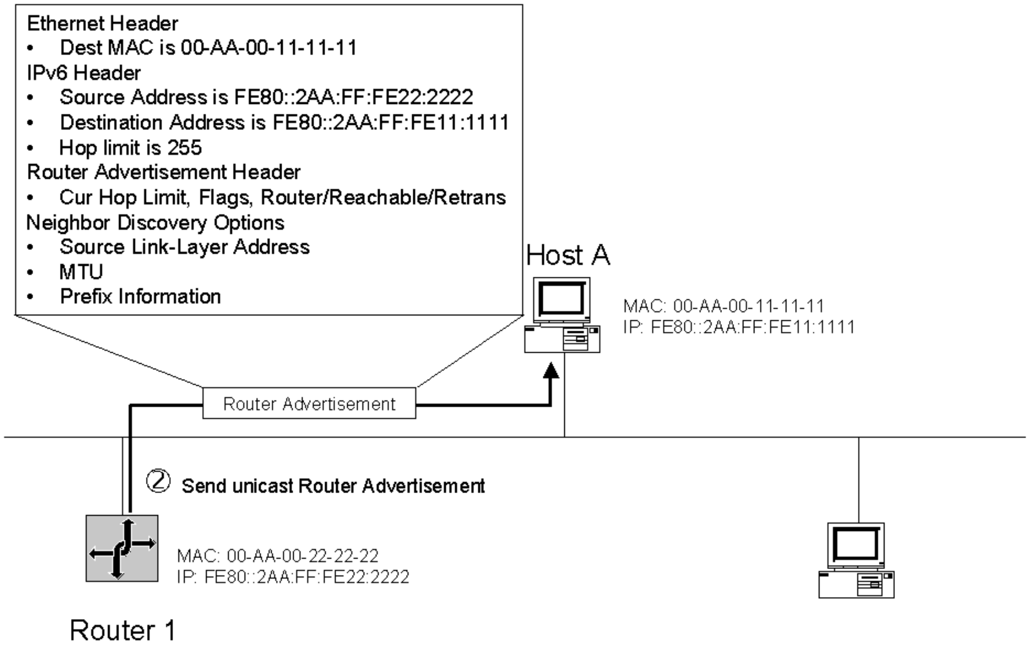
Sent on periodic basis from router
to the 'all nodes address'
Hop limit should be 255
Could include security header
M=1 use DHCP for address configuration
O=1 use stateful protocol for address configuration

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

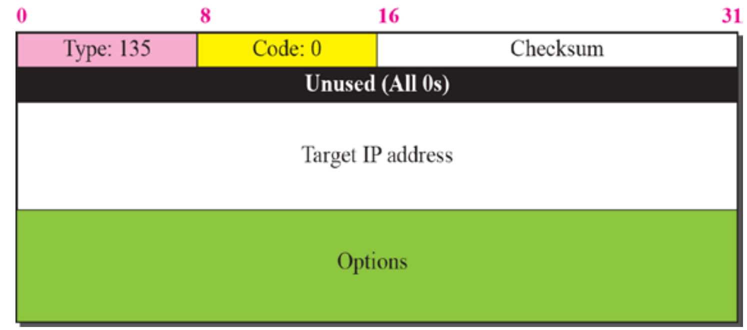
Neighbor Solicitation (ICMPv6 Type 135)

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

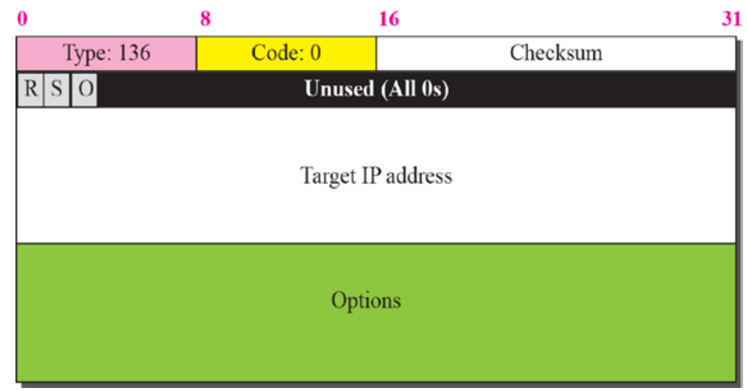


Neighbor Advertisement (ICMPv6 Type 136)

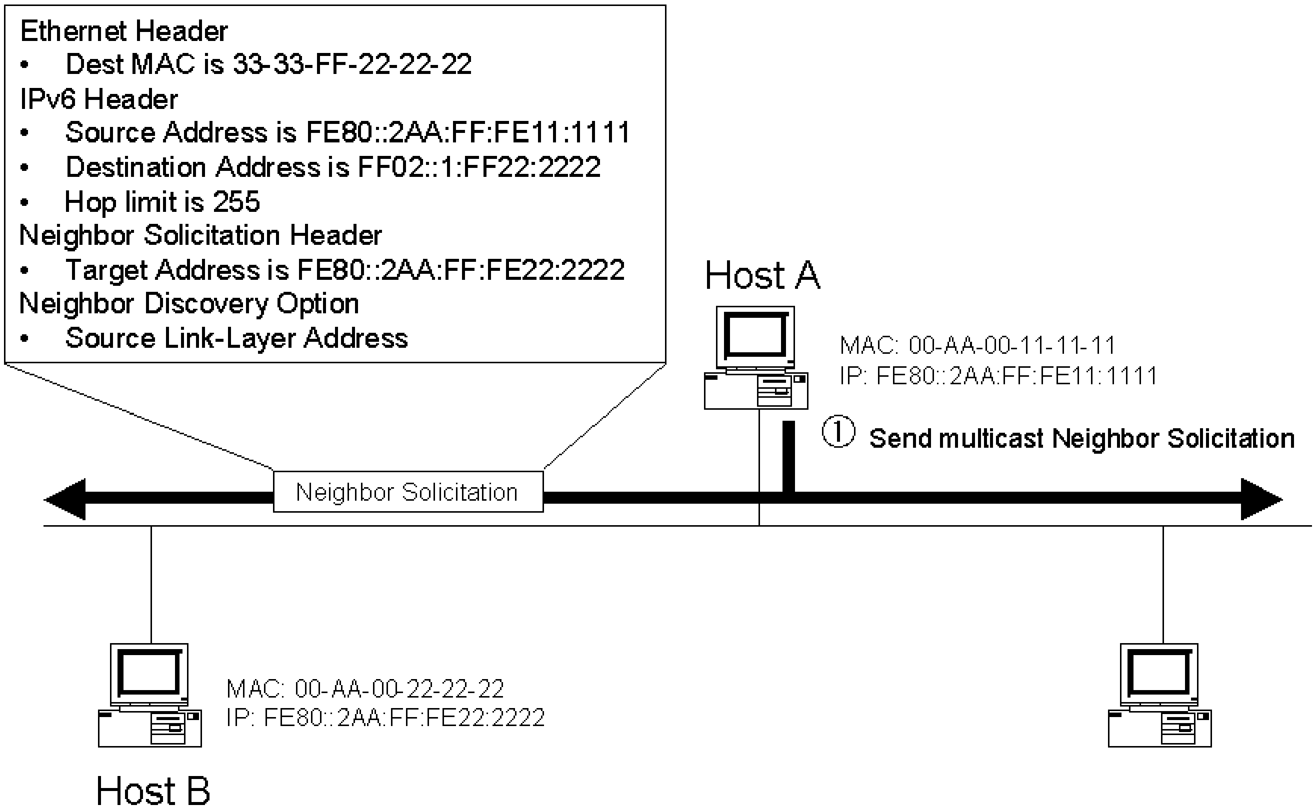
Sent by nodes in response to Neighbor solicitation message

Can be sent unsolicited to quickly ask for information

Identify sender as router, destination address, or over-ride existing cache

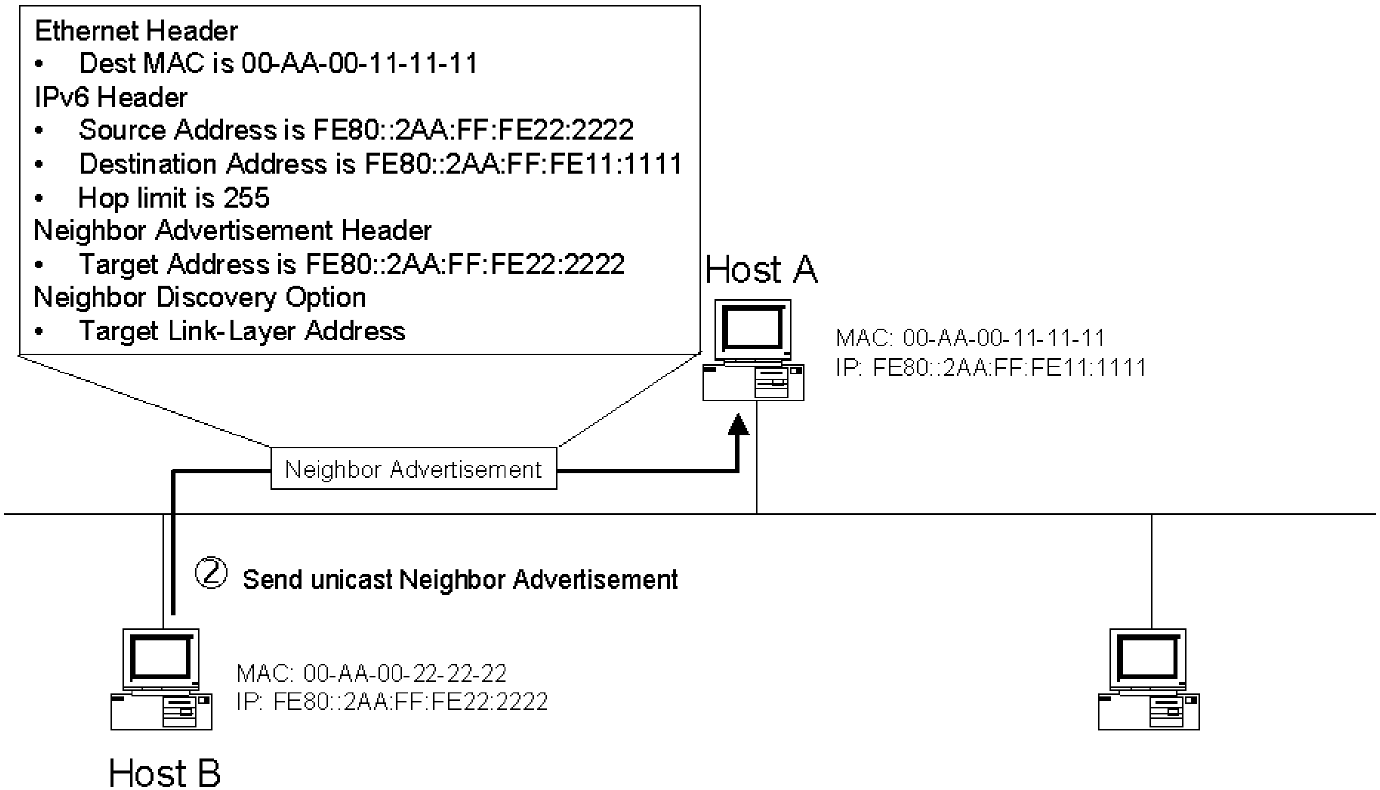


Address Resolution: Multicast Neighbor Solicitation



To send a packet to Host B, Host A must use address resolution to resolve Host B's link-layer address.

Address Resolution: Unicast Neighbor Notification



Host B, having registered the solicited-node multicast address of 33-33-FF-22-22-22 with its Ethernet adapter, receives and processes the Neighbor Solicitation. Host B responds with a unicast Neighbor Advertisement message

Neighbor Solicitation and Advertisement

Traces | Query Builder | Packet Summary | Session Summary

Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages
320	06:14:34:0405	72	2001:428:3804:0	FF02::1:FF00:1	ICMPv6	
321	06:14:34:0460	161	10.2.0.236	239.255.255.250	UDP	
322	06:14:34:0596	72	FE80::1	2001:428:3804:0	ICMPv6	

Traces | Query Builder | Packet Summary | Session Summary | Packet Details

Packet Details

Packet Details Hex

Packet Details

```
Packet ID : 320
Time : 4/10/2012 06:14:34:0405 HAT

IP Version 6
Source       : 2001:428:3804:0:D78:D8B8:F88D:8A5A
Destination : FF02::1: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: 0xEE6B
Target Address: FE80::1

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

Packet Details

Packet Details Hex

Packet Details

```
Packet ID : 322
Time : 4/10/2012 06:14:34:0596 HAT

IP Version 6
Source       : FE80::1
Destination : 2001:428:3804:0:D78:D8B8:F88D:8A5A
Traffic Class : 0x000
Flow Label : 0x000
Payload Length : 32
Next Header(Protocol) : ICMPv6
Hop Limit : 255

ICMPv6 Informational Message:
Type: Neighbor Advertisement (136)
Code:  0
Checksum: 0xD8D5
Flags:
  1... = Router: Set
  .1.. = Solicited: Set
  ..1. = Override: Set
Target Address: FE80::1

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

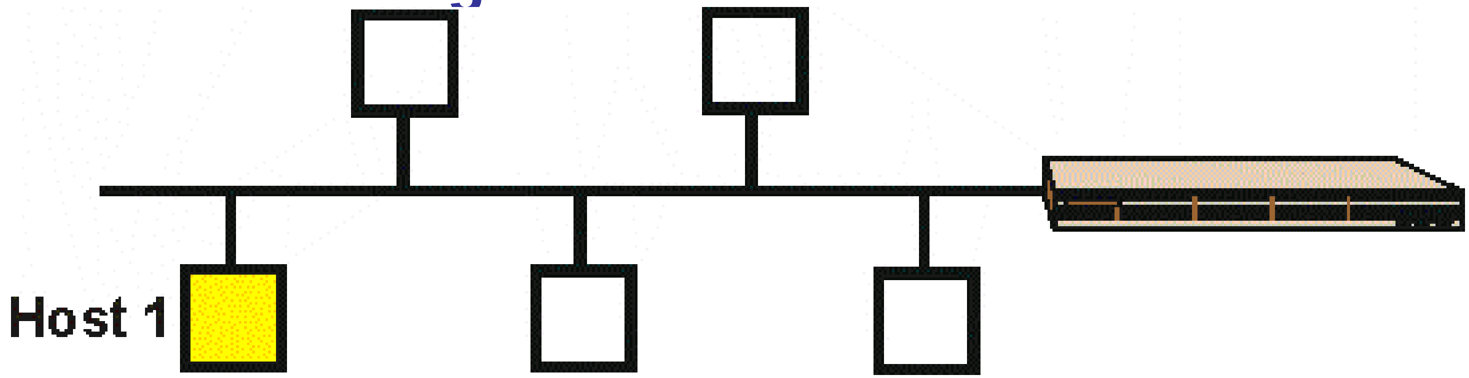
Neighbor Discovery Table

```
RouterA#show ipv6 neighbors
IPv6 Address                  Age Link-layer Addr State Interface
FEC0::1:200:86FF:FE4B:F9CE      0 0000.864b.f9ce  REACH FastEthernet0/0
<waiting of 10 minutes>
RouterA#show ipv6 neighbors
IPv6 Address                  Age Link-layer Addr State Interface
FEC0::1:200:86FF:FE4B:F9CE      2 0000.864b.f9ce  STALE FastEthernet0/0
FE80::200:86FF:FE4B:F9CE       10 0000.864b.f9ce  STALE FastEthernet0/0
```

Adding a static entry in neighbour discovery table (Cisco feature)

```
RouterA(config)#ipv6 unicast-routing
RouterA(config)#ipv6 neighbor fec0::1:0:0:1:b fastEthernet 0/0 0080.12ff.6633
RouterA(config)#exit
RouterA#show ipv6 neighbors
IPv6 Address                  Age Link-layer Addr State Interface
FEC0::1:200:86FF:FE4B:F9CE     15 0000.864b.f9ce  STALE FastEthernet0/0
FEC0::1:0:0:1:B                 - 0080.12ff.6633  REACH FastEthernet0/0
FE80::200:86FF:FE4B:F9CE       15 0000.864b.f9ce  STALE FastEthernet0/0
```

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

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Protocol	Messages	Local Port	Rmt. Port	Seq. Number	Ack. Number	Window Size
132	06:13:39:2874	104	FE80::1	FF02::1	ICMPv6						

Packet Details

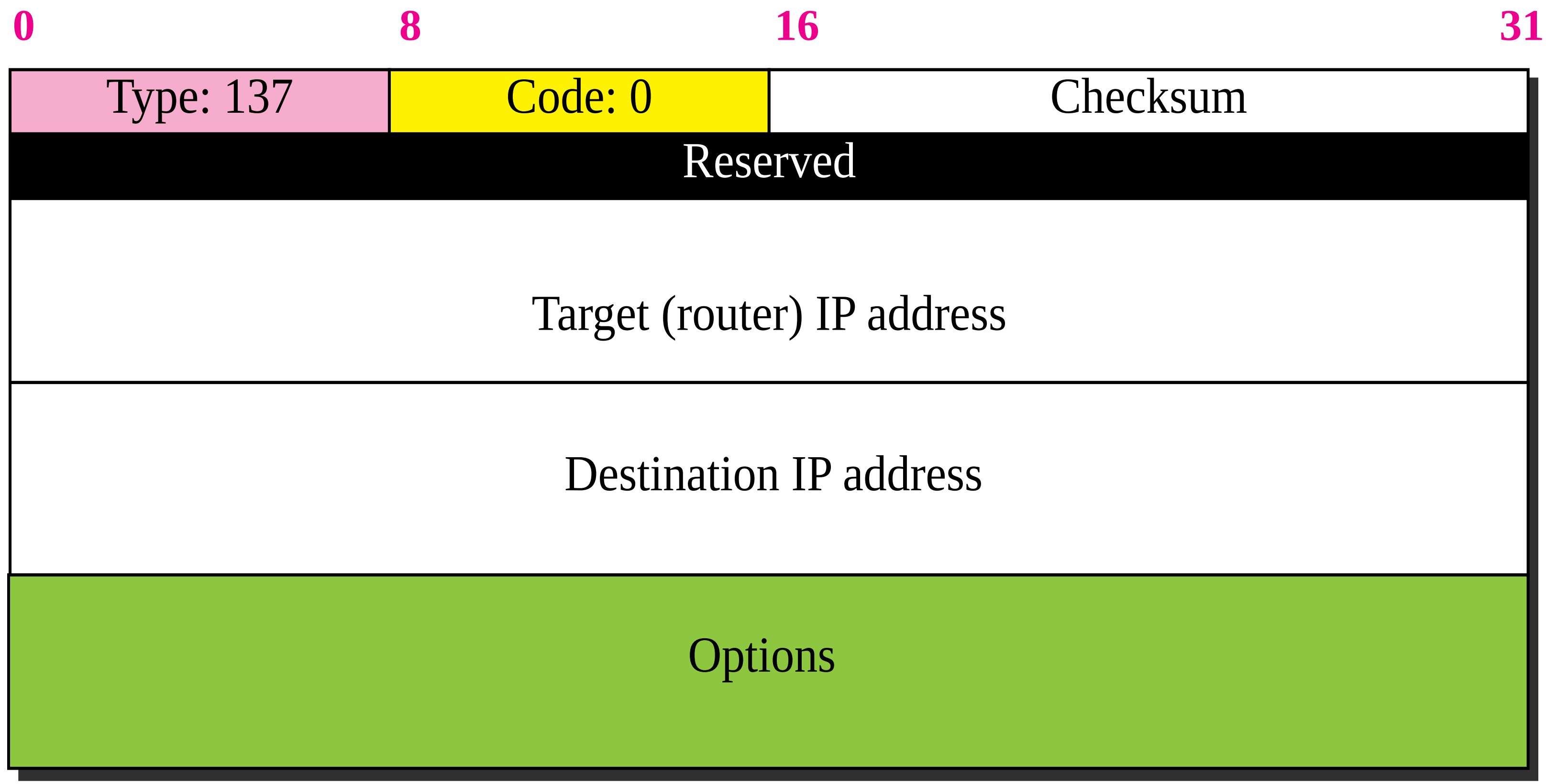
Packet Details Hex

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 : 0x000
Flow Label : 0x000
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
```

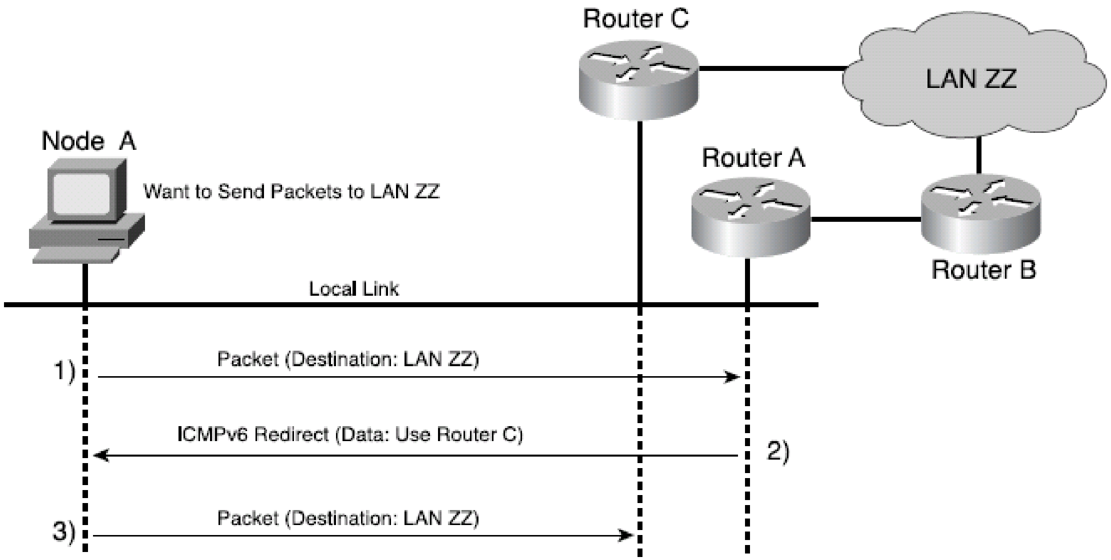
```
ICMPv6 Option
    Type: Source Link_layer Address(1)
    Length: 8 bytes
    Link-layer address: 00:08:E2:60:18:1A

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



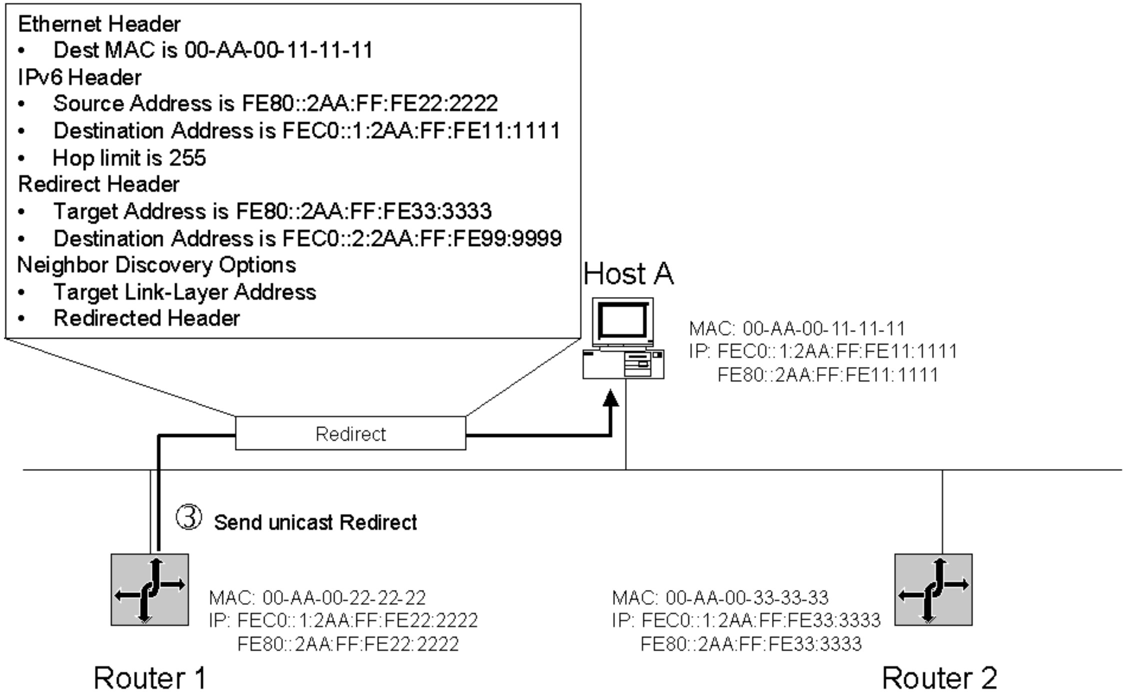
An option is added to let the host know the physical address of the target router

Router Redirect



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 neighbor (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

Router Redirect Process



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

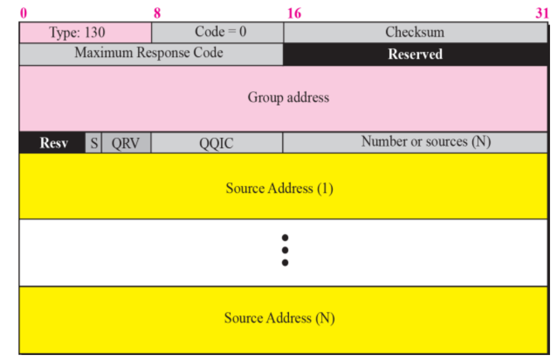
Allows routers to discover nodes that wish to receive multicast packets on all the routers links

Query can be general or specific

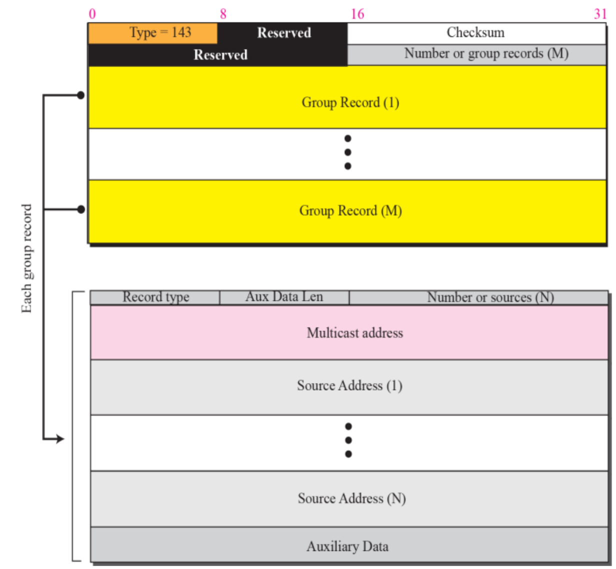
- Tell me all nodes with multicast address x
- Tell me all nodes and their multicast addresses

Maximum response delay only is used with the Query message

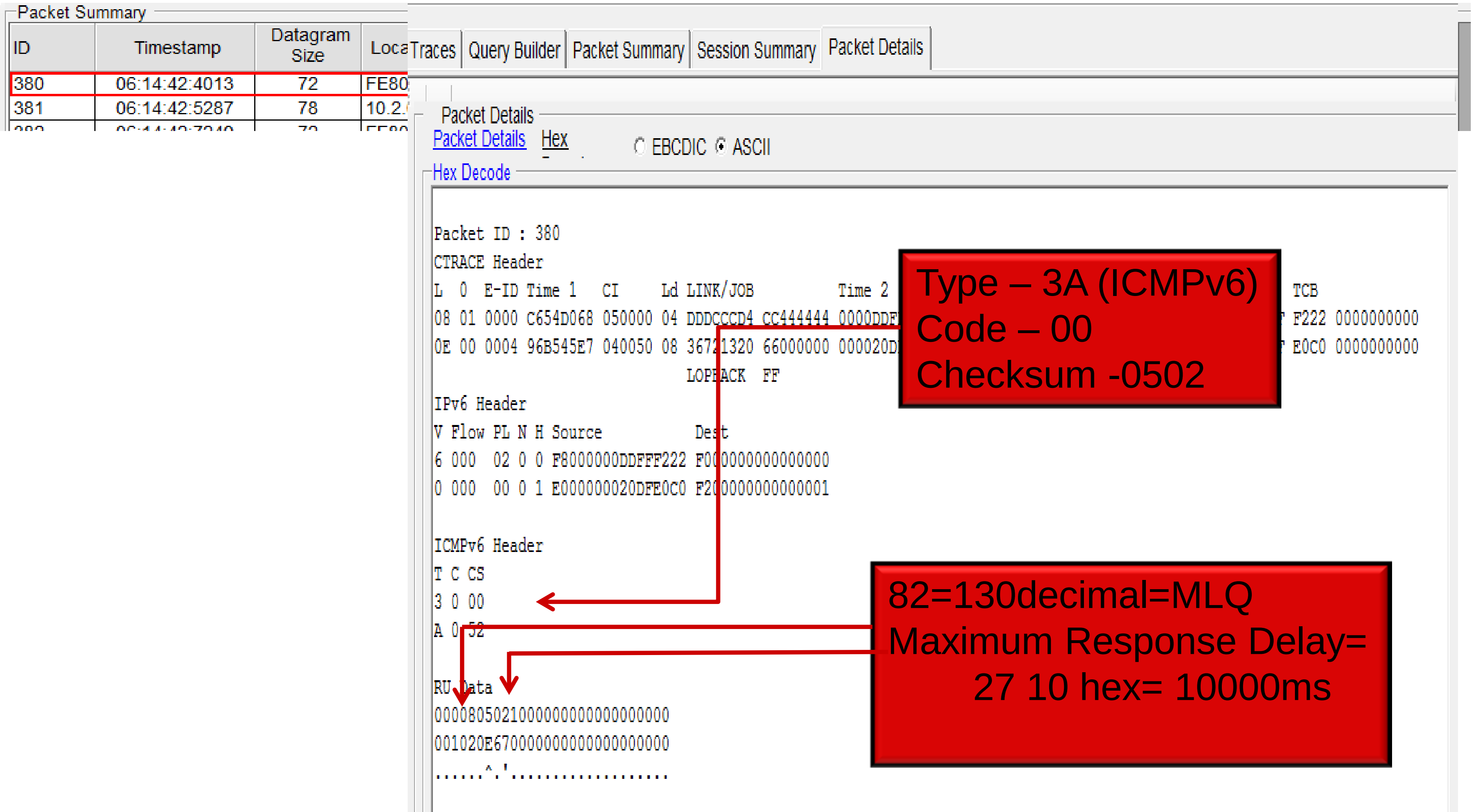
Membership Query



Membership Report



Trace Multicast Listener Query



Multicast Listener Report

Packet Summary

ID	Timestamp	Datagram Size	Local IP	Rmt. IP	Window Size
380	06:14:42:4013	72	FE80::D2D0:FDF	FF02::1	
381	06:14:42:5287	78	10.2.0.123	10.2.255.255	
382	06:14:42:7249	72	FE80::E488:BE1	FF02::1:3	

Traces | Query Builder | Packet Summary | Session Summary | Pac

Packet Details

Packet Details Hex ○ EBCDIC ● ASCII

Hex Decode

```
Packet ID : 382
CTRACE Header
L  0  E-ID Time 1   CI      Ld LINK/JOB          Ti
08 01 0000 C6542058 000010 04 CCECDF44 CC444444 00
0E 00 0004 96B632E7 0A0050 08 39236100 66000000 00
                              CISCO1   FF
IPv6 Header
V Flow PL N H Source           Dest
6 000  02 0 0 F8000000E8B1112C F000000000000000
0 000  00 0 1 E000000048E60F02 F200000000000103

ICMPv6 Header
T C CS
3 0 00
A 0 52

RU Data
000080A90000F000000000000000
001030CD0000F200000000000103
............................
```

83=131decimal=MLR

Maximum Response Delay= 00 00hex= 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

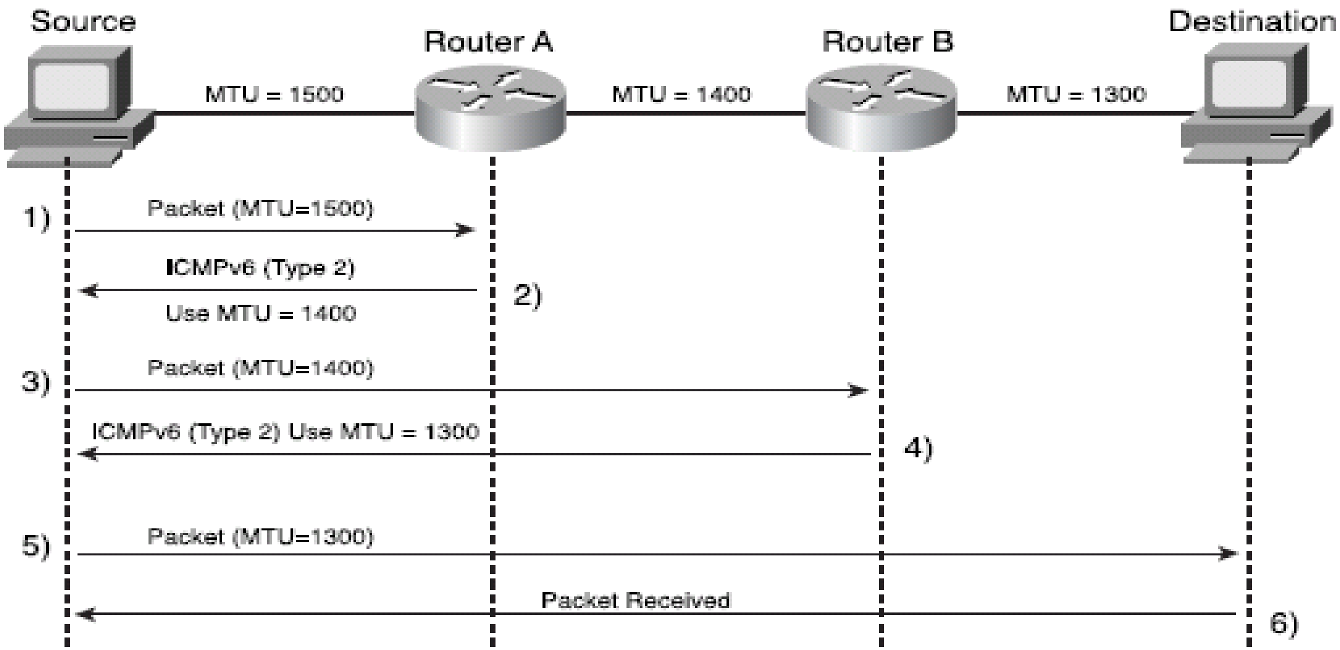
The source node may fragment packets by itself only when the path MTU is smaller than the packets to deliver

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

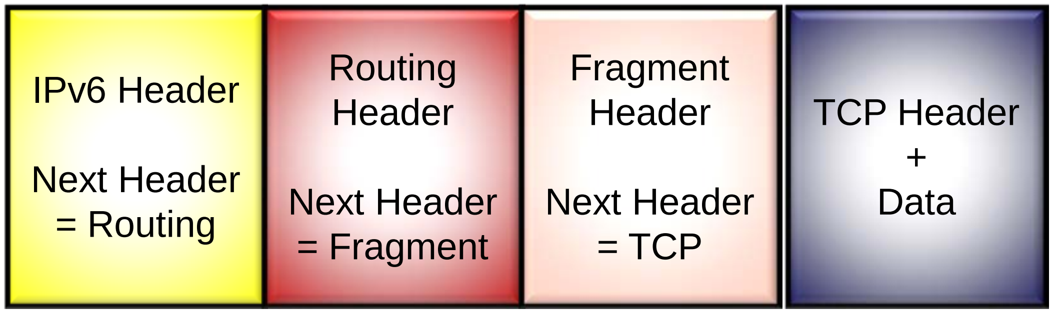
MTU Size Error Feedback
- Since routers cannot fragment datagrams, they must drop them if they are forced to try to send a too-large datagram over a physical link.
- A feedback process has been defined using ICMPv6 that lets routers tell source devices that they are using datagrams that are too large 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



Fragmentation



For purposes of fragmentation, IPv6 datagrams are broken into two pieces:

Unfragmentable 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***.

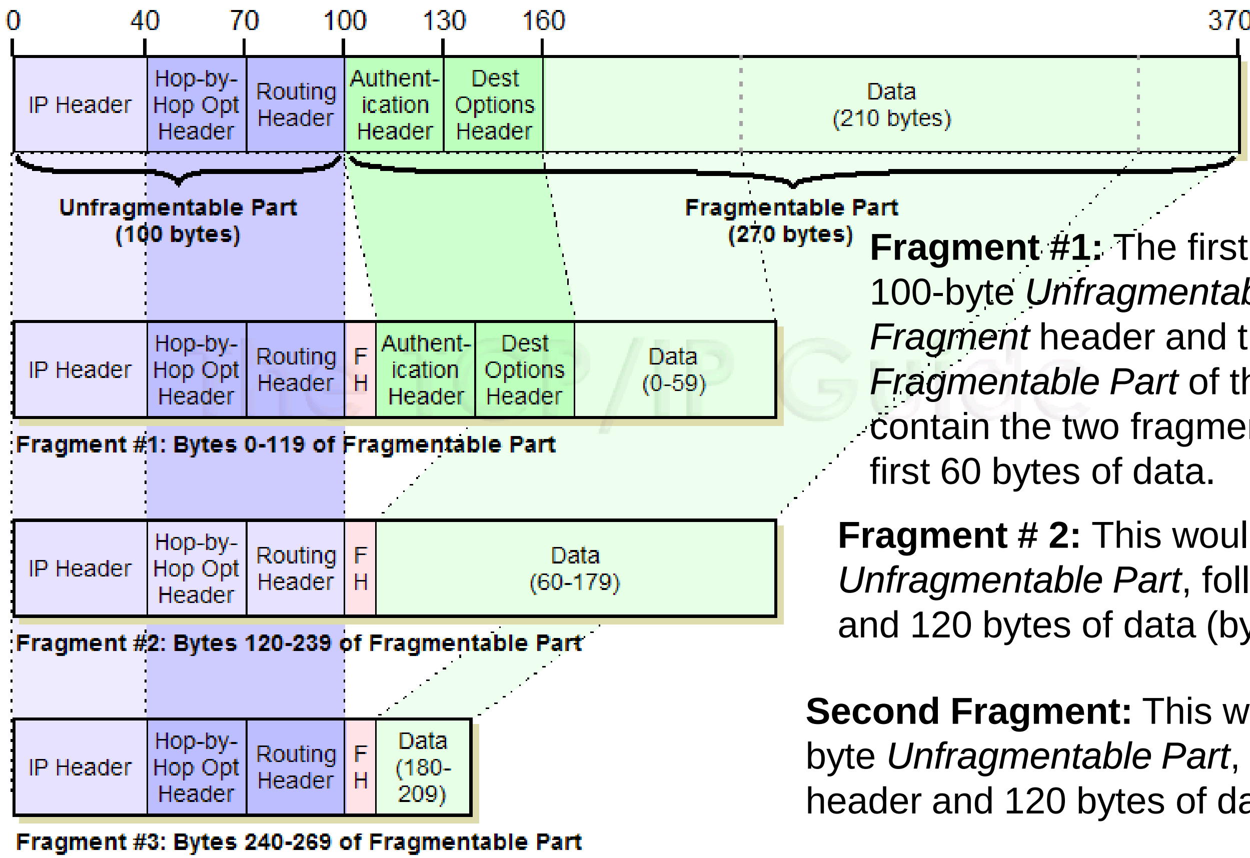
Fragmentable Part

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).

Unfragmentable Part must be present in each fragment, while the **fragmentable part** is split up amongst the fragments.

Fragmentation Example

Suppose we need to send this over a link with an MTU of only 230 bytes. Three fragments, are created, because of the need to put the two 30-byte unfragmentable extension headers in each fragment, and the requirement that each fragment be a length that is a multiple of 8.

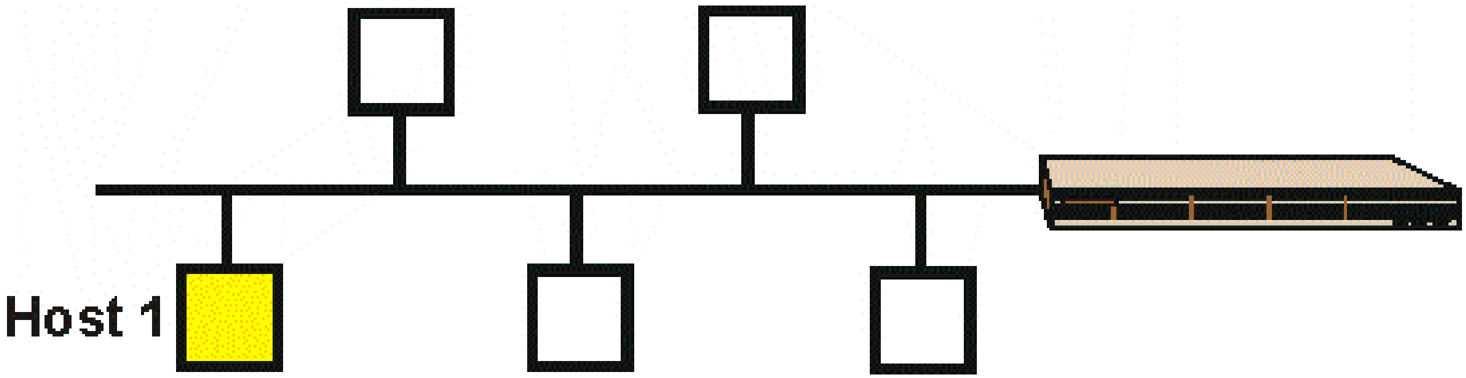


Fragment #1: The first fragment would consist of the 100-byte *Unfragmentable Part*, followed by an 8-byte *Fragment* header and the first 120 bytes of the *Fragmentable Part* of the original datagram. This would contain the two fragmentable extension headers and the first 60 bytes of data.

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

Second Fragment: This would also contain the 100-byte *Unfragmentable 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**

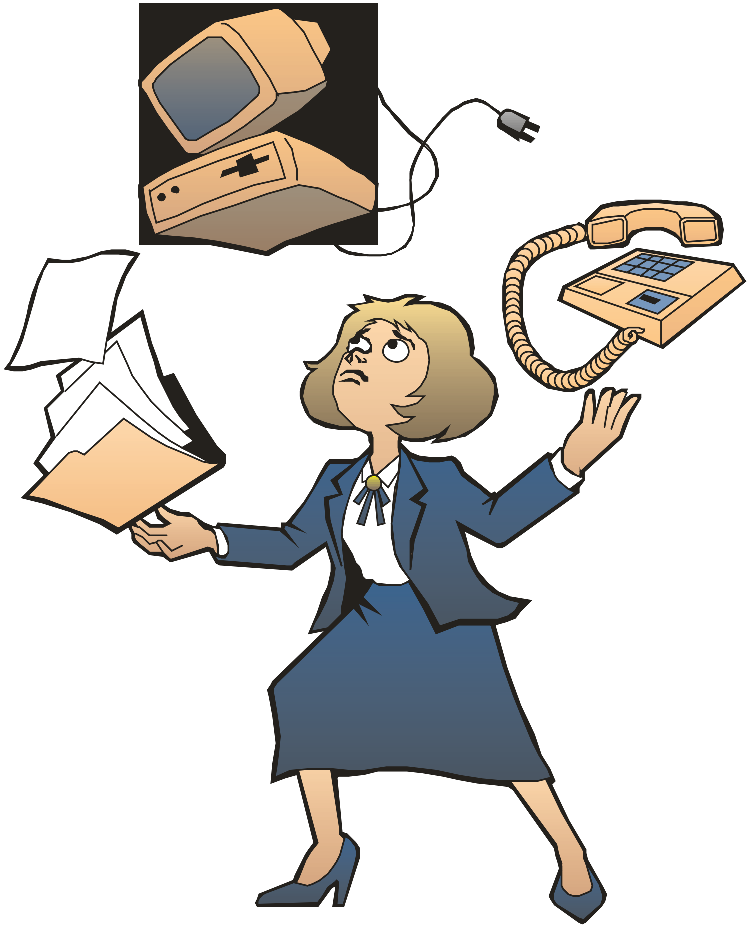
Changes Needed to Implement IPv6

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



AES Sessions

Session	Title	Day	Time	Room
11918	Performance Factors in Cloud Computing	Tuesday August 7	3:00 PM	Grand Ballroom Salon A
11156	IPv6 Basics	Wednesday August 8	8:00 AM	Grand Ballroom Salon A
11895	Network Problem Diagnosis with Packet Traces	Wednesday August 8	9:30 AM	Platinum Ballroom Salon 9
11165	I'm Running IPv6 How Do I Access?	Wednesday August 8	4:30 PM	Grand Ballroom Salon A
11164	IPv6 Deep Dive	Thursday August 9	3:00 PM	Grand Ballroom Salon A
11161	Managing an IPv6 Network	Friday August 10	8:00 AM	Grand Ballroom Salon A
11162	Home Networking with IPv6	Friday August 10	11:00 AM	Grand Ballroom Salon A

AES aesclever.com

Questions?

Vielen Dank

Köszönettel

Teşekkürler

THANK YOU

Obrigado!

תודה

Bedankt

شكراً

Ευχαριστώ

Gracias

ขอบคุณ

Merci

Díky

धन्यवाद

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

Hvala

IPv6 References

IPv6 Home Page

http://www.ietf.org/

http://playground.sun.com/pub/ipng/html/ipng-main.html

http://www.getipv6.info/index.php/IPv6_Presentations_and_Documentshttp://www.6ren.net

http://www.ipv6forum.com

http://arin.net

http://www.internet2.edu

http://www.ipv6.org

http://ipv6.or.kr/english/natpt.overview

http://www.research.microsoft.com/msripv6

http://www.ipv6.org.uk

Books

New Internet Protocol - Prentice Hall - ISBN 0-13-241936-x
IPNG and the TCP/IP Protocols - John Wiley and Sons - ISBN-0-471-13088-5
IPv6 The New Internet Protocol - ISBN-0-13-24-241936
IPNG Internet Protocol Next Generation - ISBN-0-201-63395-7
Internetworking IPv6 with Cisco Routers - ISBN 0-07-022831-1

IPv6 RFC’s

View any IPv6 RFC

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