IPv6 Details

Vermont State University

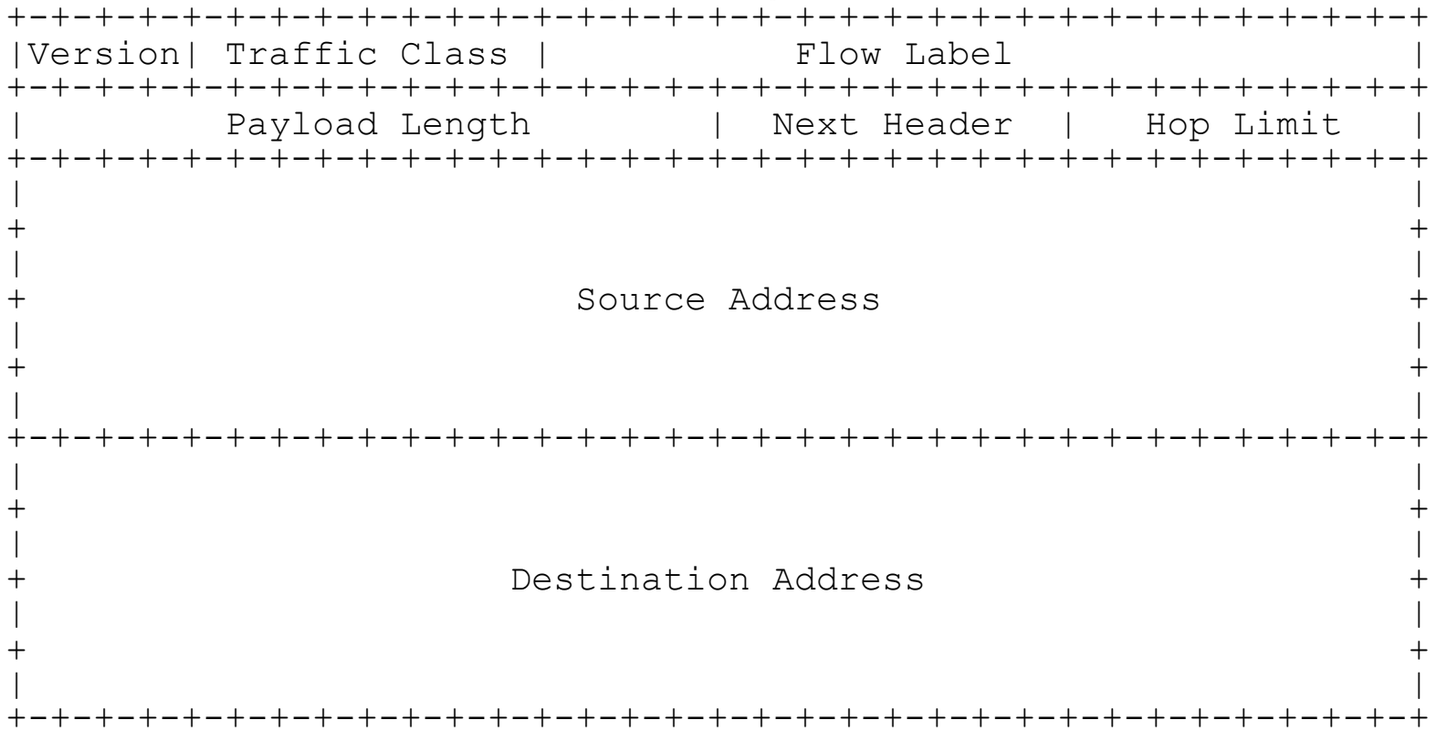
Peter Chapin

General Goals

- Simplified header (relative to IPv4)
  - Routers should not have to compute a checksum.
    - IPv4 has a header checksum that needs to be recomputed at each step.
    - Instead, underlying link protocol or upper-level transport or application protocol can do error detection.
  - Many features are relegated to “extension headers.”
    - The application only uses extensions that it needs.
    - Keeps header size reasonable.
- No (on-network) fragmentation allowed.
  - Fragmentation in IPv4 has proved problematic.

Header

- IPv6 header is (nominally) 40 bytes.

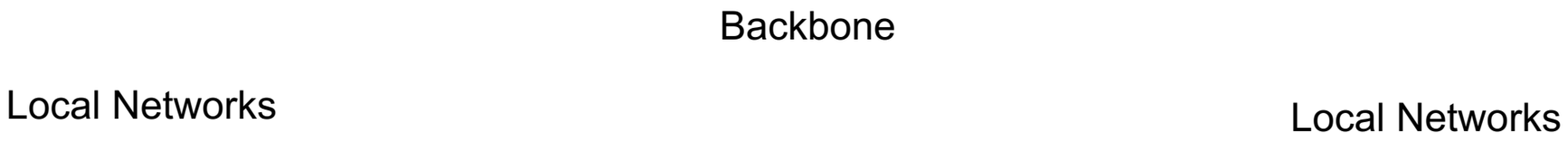


Hop Limit

- “Hop limit” field is similar to IPv4's “time to live.”
  - Number of routers the packet can pass through.
    - Limits packets from circulating indefinitely in an erroneous routing loop.
  - Field 8 bits so maximum number of hops just 255.
    - Is this enough?
    - IPv6 networks can contain a huge number of nodes.
- *Defn: The “diameter” of the network is the maximum number of hops between any pair of nodes.*

Diameter of the Internet?

- Nobody knows for sure.
- However... node count grows exponentially with the diameter.
  - Thus a large hop count field may be unnecessary
  - This was a debated topic in the design of IPv6.



Flows

- Flows are an experimental feature (RFC-3697)
  - Not widely implemented (as far as I know)
  - Stream of packets designated as a “flow” by the source.
    - Often associated with a transport connection.
  - Defined by (source-address, destination-address, flow label)
  - The source must use a flow label of zero by default.
  - Applications and transport protocols MUST have a means for setting the flow label.
- Intended to be used for quality-of-service (QoS) applications.

Extension Headers

- Various kinds are defined
  - Hop-by-hop (processed by routers).
  - Destination options for all destinations in the routing header (if there is one)
  - Routing (requested path through the network)
  - Fragment (source node *can* fragment packets, so support is still necessary)
  - Authentication (AH... part of IPsec)
  - Encapsulation Security Payload (ESP... part of IPsec)
  - Destination options (only for final destination)

Layout

Main Header

Next Hdr

Next Hdr | Hdr Length | Header contents... — Extension #1

Next Hdr | Hdr Length | Header contents... — Extension #2

Special marker for end-of-list

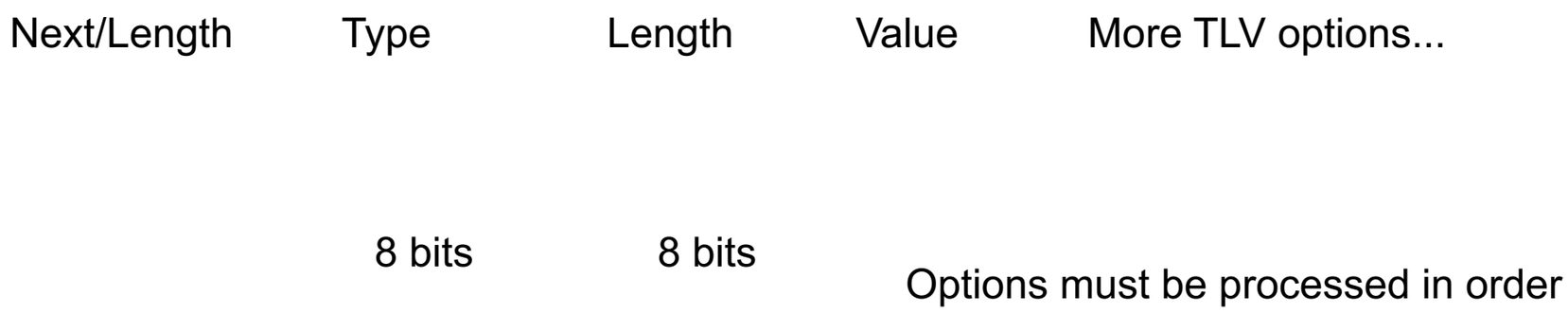
This design allows for easy future expansion.
New extension headers can be defined at any time.

Extension Header Notes

- A few rules of interest... (see RFC-2460)
  - Headers are only processed by the destination
    - Except for “hop-by-hop options”... which must be first.
      - Routers don't have to dig around looking for them!
  - Headers must be processed in the order given.
    - Some extensions may prohibit further processing.
  - An unrecognized header causes the packet to be discarded.
    - An ICMPv6 message is returned to the sender.
    - “Don't process packets you don't fully understand.”

Option Headers Format

- Option Headers have a generic format.
  - Contain a variable number of “type-length-value” (TLV) encoded options.
  - New options can be defined later.



Type Field

- Option type field has additional structure.

Flag: Can option data change in route?

Actual type field just five bits.

How to process if unrecognized
0 => Skip option.
1 => Discard packet.
2 => Discard packet and send ICMPv6
3 =>Like (2) for non multi-cast.

Neighbor Discovery Protocol

- Used for... (see RFC-2461)
  - Finding link-layer addresses that correspond to an IPv6 address (like IPv4's ARP).
  - Finding routers on a given link.
  - Finding the link's prefix(es) (global addresses)
  - Link parameters
- ND thus combines the functionality of several separate IPv4 protocols.

Special ND Addresses

- Some ND functions are done before the node has a normal address.
  - FF02::1 Link scope all nodes multi-cast (used to talk with all nodes on a particular link).
  - FF02::2 Link scope all routers multi-cast (used to talk with all routers on a particular link).
- Solicited node multi-cast (RFC-4291)
  - Suppose node address = 4037::1:800:200E:8C6C
  - Solicited node address = FF02::1:FF0E:8C6C
    - Prefix FF02::1:FF00:0000/104
    - Lower 24 bits from the address above.

ND (ICMP) Message Types

- Router Solicitation
- Router Advertisement
  - Contains a list of link prefixes
  - Options: hop limit, link MTU, etc., hosts should use.
- Neighbor Solicitation
  - Multi-cast to the solicited-node address.
- Neighbor Advertisement
  - Unicast back to the requesting node.
- Redirect