Transporting Voice by Using IP

The RTP Control Protocol [1/3]

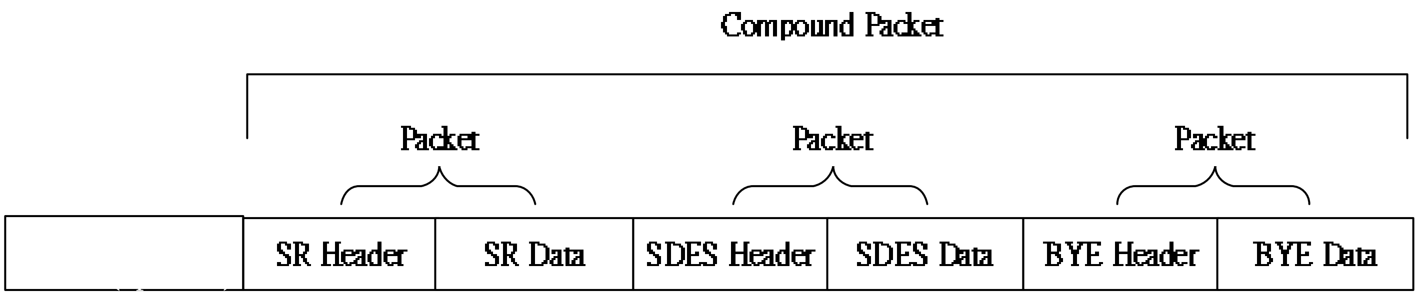
- RTCP
  - A companion control protocol of RTP
  - Periodic exchange of control information
    - For quality-related feedback
  - A third party can also monitor session quality and detect network problems.
    - Using RTCP and IP multicast
- Five types of RTCP packets
  - Sender Report: used by active session participants to relay transmission and reception statistics
  - Receiver Report: used to send reception statistics from those participants that receive but do not send them

The RTP Control Protocol [2/3]

- Source Description (SDES)
  - One or more descriptions related to a particular session participant
  - Must contain a canonical name (CNAME)
    - Separate from SSRC which might change
    - When both audio and video streams were being transmitted, the two streams would have
      - different SSRCs
      - the same CNAME for synchronized play-out
- BYE
  - The end of a participation in a session
- APP
  - For application-specific functions

The RTP Control Protocol [3/3]

- Two or more RTCP packets will be combined
  - SRs and RRs should be sent as often as possible to allow better statistical resolution.
  - New receivers in a session must receive CNAME very quickly to allow a correlation between media sources and the received media.
  - Every RTCP packet must contain a report packet (SR/RR) and an SDES packet
    - Even if no data to report
- An example of RTP compound packet



RTCP Sender Report

- SR
  - Header Info
  - Sender Info
  - Receiver Report Blocks
  - Option
    - Profile-specific extension

00 01	02	03	04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
V=2	P	X	RC	PT=SR=200	Length
SSRC of sender					
NTP Timestamp (most significant word)					
NTP Timestamp (least significant word)					
RTP Timestamp					
sender's packet count					
sender's octet count					
SSRC_1(SSRC of first source)					
fraction lost				fraction lost	
extended highest sequence number received					
interarrival jitter					
last SR (LSR)					
Delay since last SR (DLSR)					
SSRC_2(SSRC of second source)					
:					
profile-specific extensions					

Header Info

- Resemble to an RTP packet
  - Version
    - 2
  - Padding bit
    - Padding octets?
  - RC, report count
    - The number of reception report blocks
    - 5-bit
      - If more than 31 reports, an RR is added
  - PT, payload type (200)

Sender Info

- SSRC of sender
- NTP Timestamp
  - Network Time Protocol Timestamp
    - The time elapsed in seconds since 00:00, 1/1/1900 (GMT)
    - 64-bit
      - 32 MSB: the number of seconds
      - 32 LSB: the fraction of a seconds (200 ps)
- RTP Timestamp
  - The same as used for RTP timestamps in RTP packets
  - For better synchronization
- Sender's packet count
  - Cumulative within a session
- Sender's octet count
  - Cumulative within a session

RR blocks [1/2]

- SSRC_n
  - The source identifier of the session participant to which the data in this RR block pertains.
- Fraction lost
  - Fraction of packets lost since the last report issued by this participant
  - By examining the sequence numbers in the RTP header
- Cumulative number of packets lost
  - Since the beginning of the RTP session
- Extended highest sequence number received
  - The sequence number of the last RTP packet received
  - 16 lsb, the last sequence number
  - 16 msb, the number of sequence number cycles

RR blocks [2/2]

- Interarrival jitter
  - An estimate of the variance in RTP packet arrival
- Last SR Timestamp (LSR)
  - Used to check if the last SR has been received
- Delay Since Last SR (DLSR)
  - The duration in units of 1/65,536 seconds

RTCP Receiver Report

- RR
  - Issued by a participant who receives RTP packets but does not send, or has not yet sent
  - Is almost identical to an SR
    - PT = 201
    - No sender information

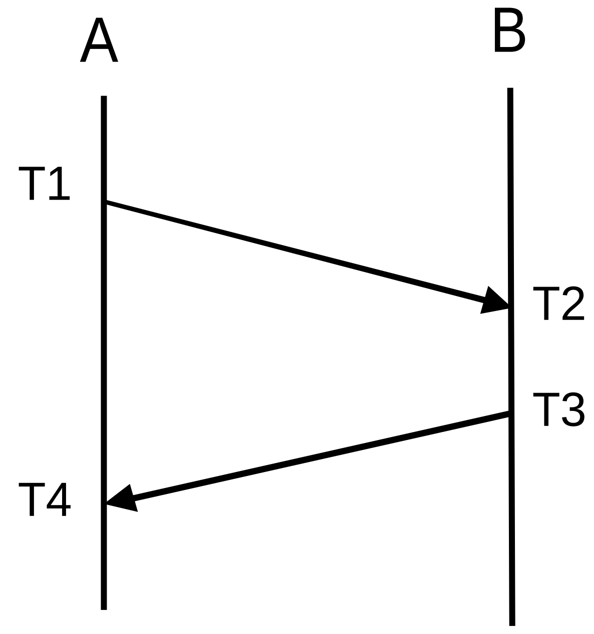
RTCP Source Description Packet

- Provides identification and information regarding session participants
  - Must exist in every RTCP compound packet
- Header
  - V, P, RC, PT=202, Length
- Zero or more chunks of information
  - An SSRC or CSRC value
  - One or more identifiers and pieces of information
    - A unique CNAME (user@host)
    - Email address, phone number, name

- RTCP BYE Packet (PT=203)
  - Indicate one or more media sources (SSRC or CSRC) are no longer active
- Application-Defined RTCP Packet (PT=204)
  - For application-specific data
  - For non-standardized application

Calculating Round-Trip Time

- Use SRs and RRs
- E.g.
  - Report A: A, T1 → B, T2
  - Report B: B, T3 → A, T4
  - RTT = T4-T3+T2-T1
  - RTT = T4-(T3-T2)-T1
  - Report B
    - LSR = T1
    - DLSR = T3-T2



Calculation Jitter

- The variation in delay
- The mean deviation of the difference in packet spacing at the receiver compared to the packet spacing at the sender for a pair of packets
  - This value is equivalent to the derivation in transit time for a pair of packets.
  - S_i = the RTP timestamp for packet i
  - R_i = the time of arrival
  - $D(i,j) = (R_j-R_i)-(S_j-S_i) = (R_j-S_j) - (R_i-S_i)$
- The Jitter is calculated continuously
  - $J(i) = J(i-1) + (| D(i-1,i) | - J(i-1))/16$

Timing of RTCP Packets

- RTCP provides useful feedback
  - Regarding the quality of an RTP session
  - Delay, jitter, packet loss
  - Be sent as often as possible
    - Consume the bandwidth
    - Should be fixed to a small fraction (e.g., 5%)
- An algorithm, RFC 1889
  - Senders are collectively allowed at least 25% of the control traffic bandwidth. (CNAME)
  - The interval > 5 seconds
  - 0.5 – 1.5 times the calculated interval
    - This helps to avoid unintended synchronization where all participants send RTCP packets at the same time instant, hence clogging the network.
  - A dynamic estimate of the avg. RTCP packet size is calculated.
    - To automatically adapt to changes in the amount of control information carried.

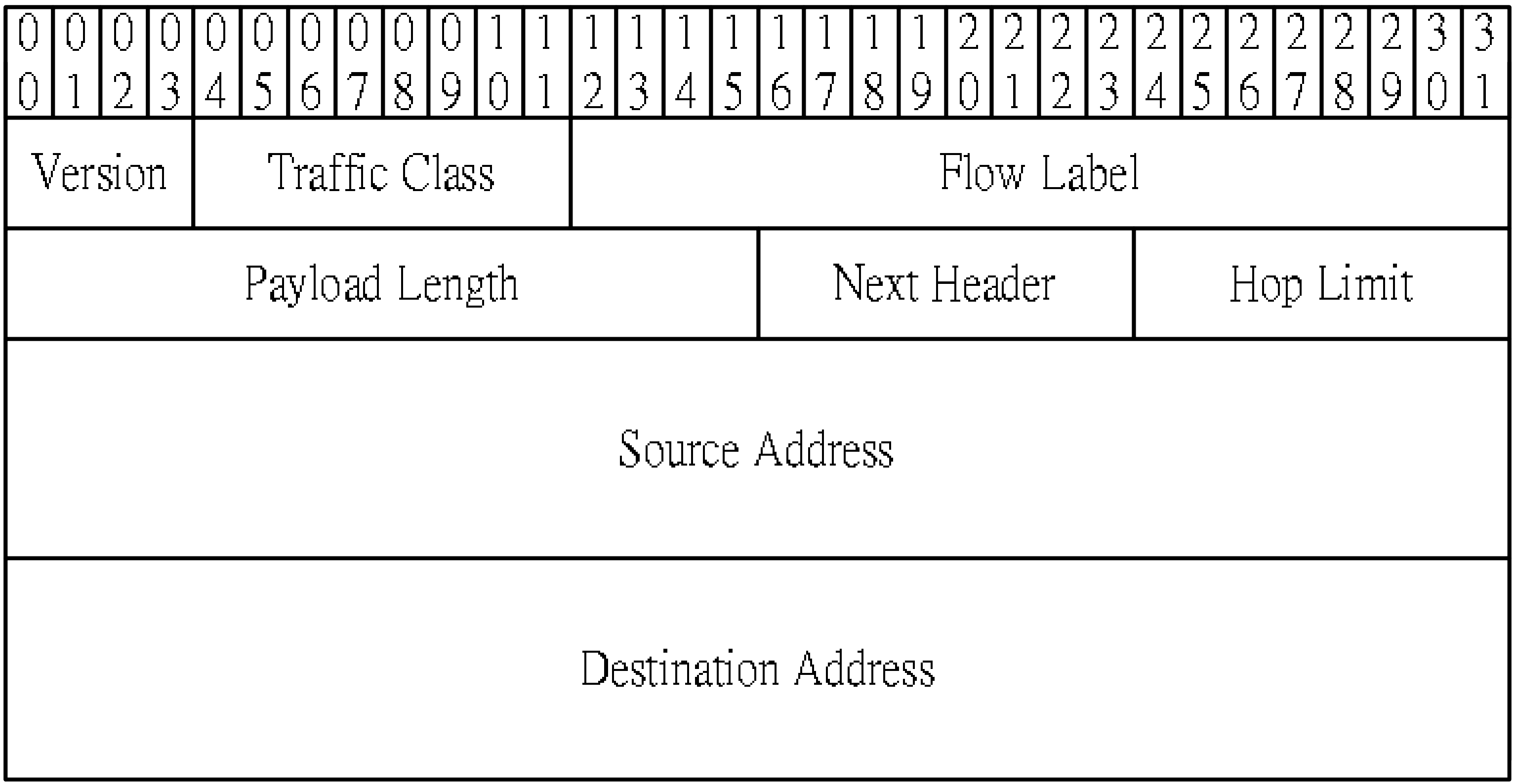
IP Multicast

- An IP diagram sent to multiple hosts
  - Conference
  - To a single address associated with all listeners
- Multicast groups
  - Multicast address
  - Join a multicast group
    - Inform local routers
  - Routing protocols
    - Support propagation of routing information for multicast addresses
    - Routing tables should be set up so that the minimum number of datagrams is sent.
- IP version 4 (IPv4) address space 224.0.0.0 to 239.255.255.255
- Hosts in a particular group use the Internet Group Message Protocol (IGMP) to advertise their membership in a group to routers.

IP Version 6

- The explosive growth of the Internet
  - IPv4 address space, 32-bit
  - Real-time and interactive applications
- Expanded address space, 128 bits
- Simplified header format
  - Enabling easier processing of IP datagrams
- Improved support for headers and extensions
  - Enabling greater flexibility for the introduction of new options
- Flow-labeling capability
  - Enabling the identification of traffic flows (and therefore better support at the IP level) for real-time applications
- Authentication and privacy
  - Support for authentication, data integrity and data confidentiality are included at the IP level.

IPv6 Header [1/3]



IPv6 Header [2/3]

- Version
  - 6
- Traffic Class, 8-bit
  - For the quality of service
- Flow Label, 20-bit
  - Label sequences of packets that belong to a single flow
    - A VoIP stream
  - A flow := source address, destination address, flow label

IPv6 Header [3/3]

- Payload Length, 16-bit unsigned integer
  - The length of payload in octets
  - Header extensions are part of the payload
- Next Header, 8-bit
  - The next higher-layer protocol
    - Same as the Protocol field of the IPv4 header
  - The existence of IPv6 header extensions
- Hop Limit, 8-bit unsigned integer
  - The TTL field of the IPv4 header
- Source and Destination Addresses, 128-bit

IPv6 addresses

- XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
  - X is a hexadecimal character
- E.g., 1511:1:0:0:0:FA22:45:11
  - The symbol “::” can be used to represent a number of contiguous fields with zero values.
  - = 1511:1::FA22:45:11
- 0:0:0:0:AA11:50:22:F77 = ::AA11:50:22:F77
  - “::” can appears only once

IPv6 special addresses

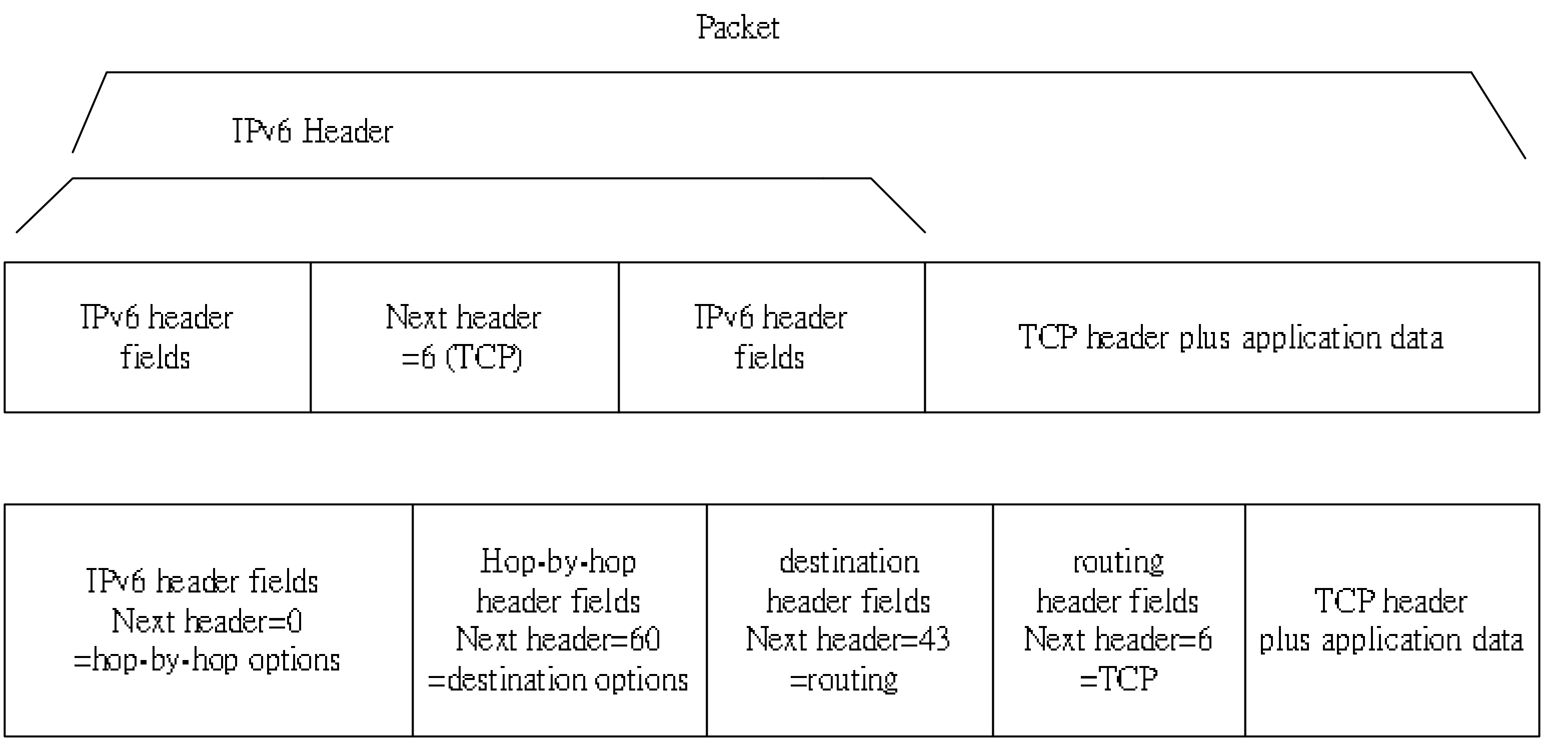
- The all-zeros address, ::
  - An unspecified address; a node does not yet know its address
  - The all-zeros address must not be used as a destination address.
- The loopback address, ::1
  - To send an IPv6 packet to itself
  - On a virtual internal interface
- IPv6 address with embedded IPv4 address (type 1)
  - 96-bit zeros + 32-bit IPv4 address
  - ::140.113.17.5
  - Used by IPv6 hosts and routers that tunnel IPv6 packets through an IPv4 infrastructure
- IPv6 address with embedded IPv4 address (type 2)
  - 80-bit zeros + FFFF + 32-bit IPv4 address
  - 0:0:0:0:0:FFFF:140.113.17.5
  - ::FFFF:140.113.17.5
  - Applied to nodes that do not support IPv6

IPv6 Header Extensions

- To be placed between the fixed header and the actual data payload
- Next Header
  - The type of payload carried in the IP datagram
  - The type of header extension
  - Each extension has its own next header field.

Header extension

- Use the next header field

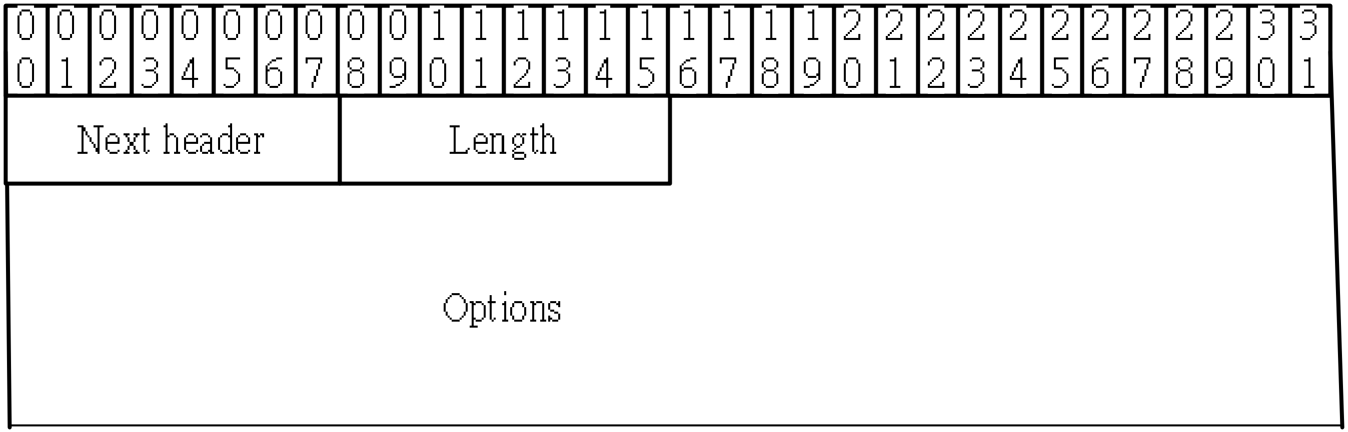


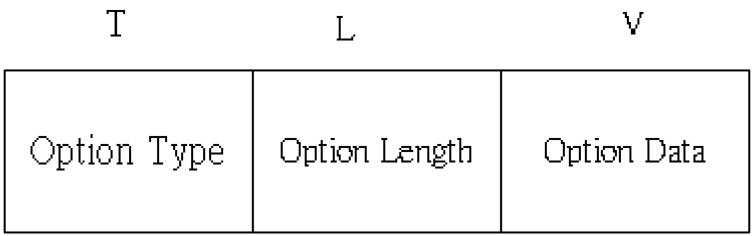
Hop-by-hop Extension [1/3]

- It is the only one exception.
  - Examined and processed by every intermediate node
  - If present, the hop-by-hop extension must immediately follow the IP header
  - Of variable length
- Next header
- Length of this header extension
  - in units of eight octets
- Options
  - TLV (Type-Length-Value) format
    - Type: 8-bit
    - Length: 8-bit (in units of octets)
    - Value: variable length
  - Type [0:2] are of special significance

Hop-by-hop Extension [2/3]

- Hop-by-hop header extension





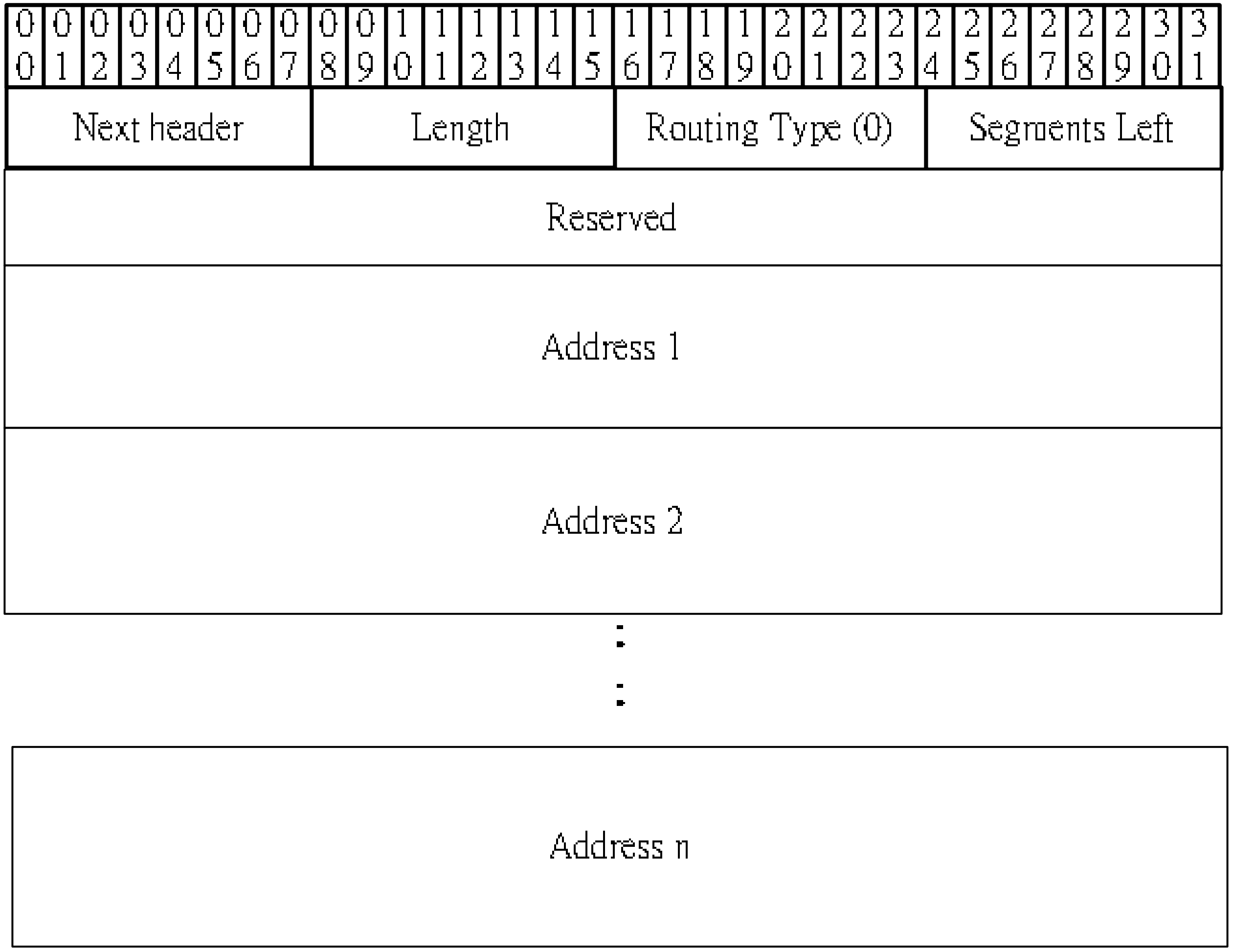
T=Type
L=Length
V=Value

Hop-by-hop Extension [3/3]

- Option Type: the first two bits (how the node react if it does not understand the option)
  - 00: skip this option and continue processing the header
  - 01: discard the packet
  - 10: discard the packet and send an ICMP Parameter Problem, Code 2 message to the originator of the packet
  - 11: do above only if the destination address in the IP header is not a multicast address
- Option Type: the third bit
  - 1, the option data can be changed
  - 0, cannot

- Destination options extension
  - Has the same format as the hop-by-hop extension
  - Only the destination node examine the extension.
  - Header type = 60
- Routing Extension
  - A routing type field to enable various routing options
  - Only routing type 0 is defined for now
    - Specify the nodes that should be visited

Routing Extension [1/2]



Routing Extension [2/2]

- Routing type
- Segments Left
  - The number of nodes that still need to be visited
- A list of IP addresses needs to be visited
- Is this type of header analyzed by intermediate node?
  - Yes or no
  - A->B->C->D->Z
  - A->B, 3, (C,D,Z)
  - A->C, 2, (B,D,Z) by B
  - A->D, 1, (B,C,Z) by C
  - A->Z, 0, (B,C,D) by D

Interoperation IPv4 and IPv6

- IPv4 and IPv6 will coexist for a long time
  - IPv4 nodes ⇔ IPv6 nodes
  - IPv6 nodes ⇔ IPv6 nodes via IPv4 networks
  - IPv4 nodes ⇔ IPv4 nodes via IPv6 networks
- IPv4-compatible nodes with IPv4-compatible addresses at the boundaries of IPv6 networks
  - IPv6 in IPv4 packets