TCP/IP Protocol & Network Programming Technology

Chapter 3: Basic IP Packet Structures: Header and Payloads

Jungang Xu

Objectives

- Identify the various fields and features that make up an IPv4 header
- Identify the various fields and features that make up an IPv6 header
- Explain the purpose of IPv6 extension headers, as well as the function of each header

Objectives (cont'd.)

- Describe how MTU Discovery works in IPv6 and how it replaces fragmentation of IPv4 packets by routers
- Describe how upper-layer checksums work in IPv6 packets, including the use of pseudo-headers
- Explain the primary differences between IPv4 and IPv6 packet structures and why the differences are significant

IP Packets and Packet Structures

- Internet Protocol (IP)
  - Primarily transmits and delivers data between devices on internetworks
- Each packet contains a header structure comprising a number of specialized fields
  - In addition to the actual data
- IPv4 and IPv6 packets differ significantly, but the basic task of transmitting data is same.

IPv4 Header Fields and Functions

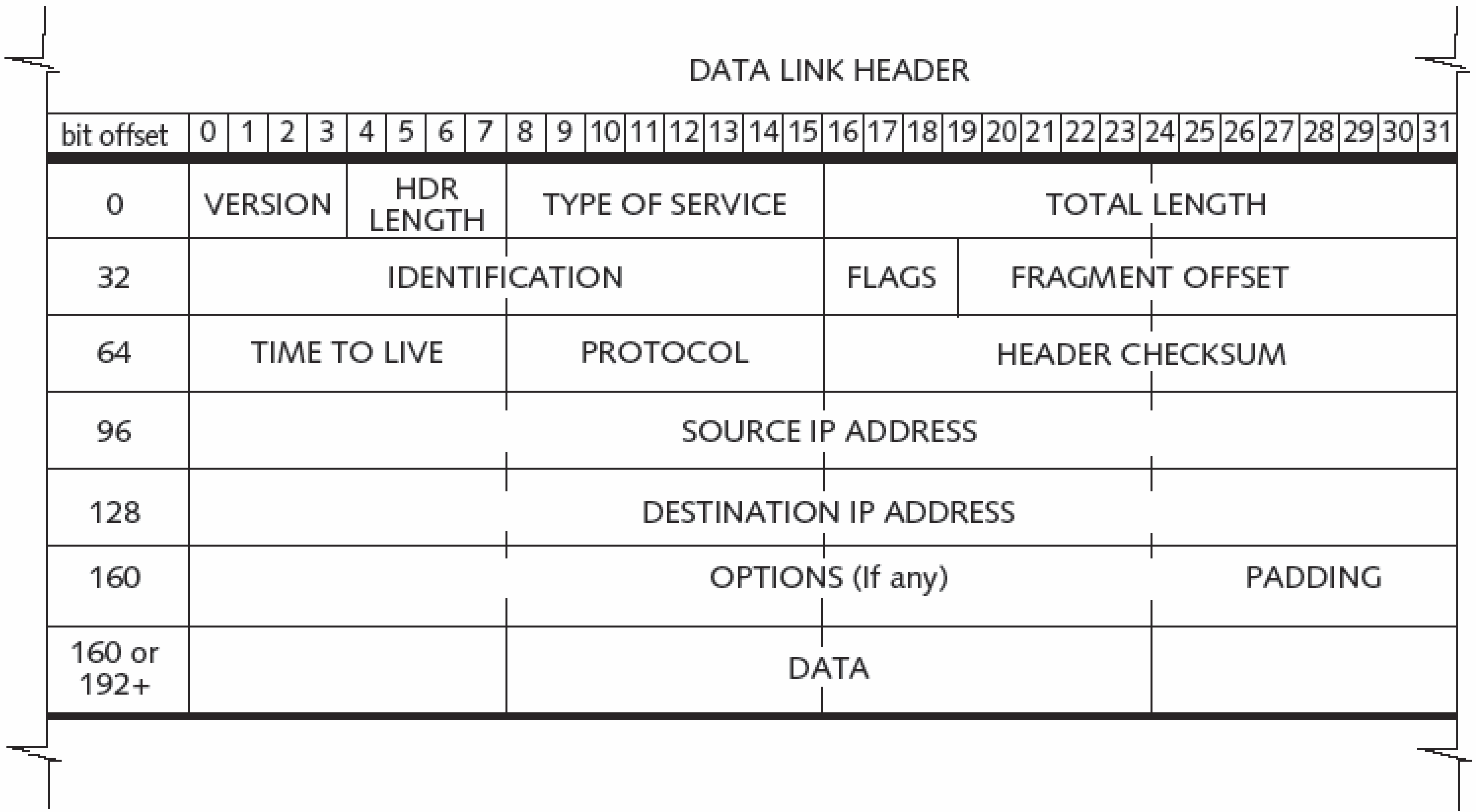


Figure 3-1 IPv4 header structure

- Number of fields: 13 is necessary, one is optional
- Header length: 20-60 Byte
- Total length of packet: 65535 Byte at most, 576 Byte moderately

Version Field

- The first field in the IP header
- Indicates IP version 4 or IPv4
- 4-bit field

Header Length Field

- Also referred to as the Internet Header Length (IHL) field
  - Denotes the length of the IP header only
  - 4-bit field
  - Value: 5-15
- Includes an offset to the data to make it fall on a 32-bit boundary value
- Minimum length for IHL: 20 bytes, 5*32=160bits
- Maximum length for IHL: 60 bytes, 15*32=480 bits

Type of Service Field

- 8-bit field
- Two components
  - Precedence
  - Type of service

P	P	P	T	T	T	T	0

- Precedence
  - Defined in the first 3 bits
  - May be used by routers to prioritize traffic
- Type of Service
  - Defined in the next 4 bits
  - Used by routers to follow a specified path type
- Last bit is reserved, set to 0

Type of Service Field (cont'd.)

Binary	Decimal	Meaning
111	7	Network control
110	6	Internetwork control
101	5	CRITIC/ECP (Critical and Emergency Call Processing)
100	4	Flash override
011	3	Flash
010	2	Immediate
001	1	Priority
000	0	Routine

Type of Service Field (cont'd.)

- 3 bit: 0-Normal delay, 1- Low delay
- 4 bit: 0-Normal throughout, 1-High throughput
- 5 bit: 0-Normal reliability, 1-High reliability
- 6 bit: 0-Normal cost, 1-minimise monetary cost

Binary	Meaning	Binary	Meaning
0000	Default	0100	Maximum throughput
0001	Minimum cost	1000	Low delay
0010	Maximum reliability	1111	Maximum security

TOS Field Function: Differentiated Services and Congestion Control

- RFC 2474
  - Recommends new definitions for TOS field

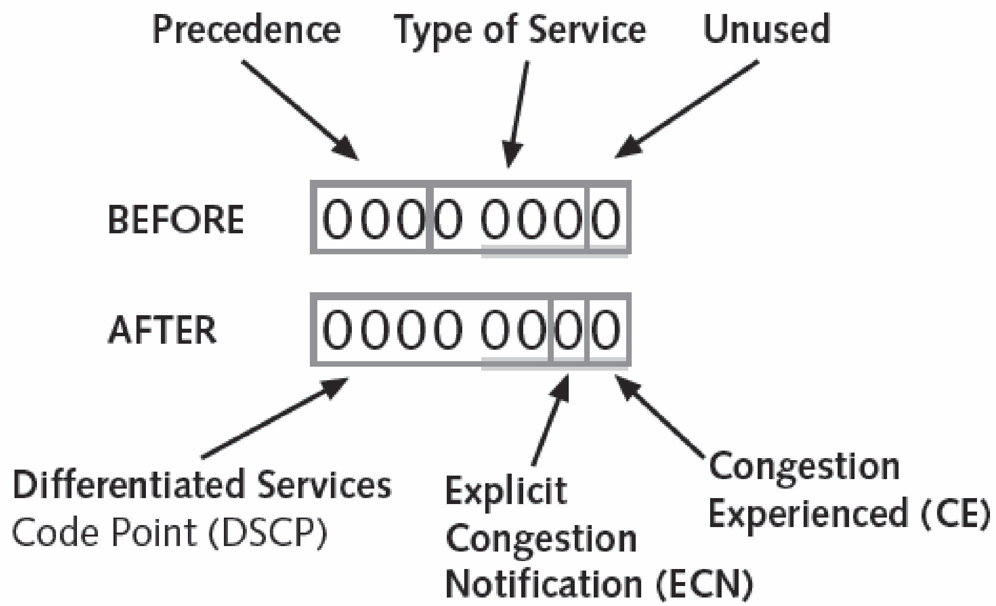


Figure 3-3 DSCP uses bits from the former Precedence and TOS fields

TOS Field Function: Differentiated Services and Congestion Control (cont'd)

Priority	Class 1	Class 2	Class 3	Class 4	Classless
Low discard priority	DSCP 10	DSCP 18	DSCP 26	DSCP 34	
	AF11	AF21	AF31	AF41	
	001010	010010	001010	100010	
Medium discard priority	DSCP 12	DSCP 20	DSCP 28	DSCP 36	
	AF12	AF22	AF32	AF42	
	00100	010100	011100	100100	
High discard priority	DSCP 14	DSCP 22	DSCP 30	DSCP 38	
	AF13	AF23	AF33	AF43	
	001110	010110	011110	100110	
Expedited forwarding					DSCP 46
					101110

AF: Assured forwarding

TOS Field Function: Differentiated Services and Congestion Control (cont'd.)

- Explicit Congestion Notification (ECN)
  - Allows devices <u>notifying each other about congestion before the routers start to drop packets</u>

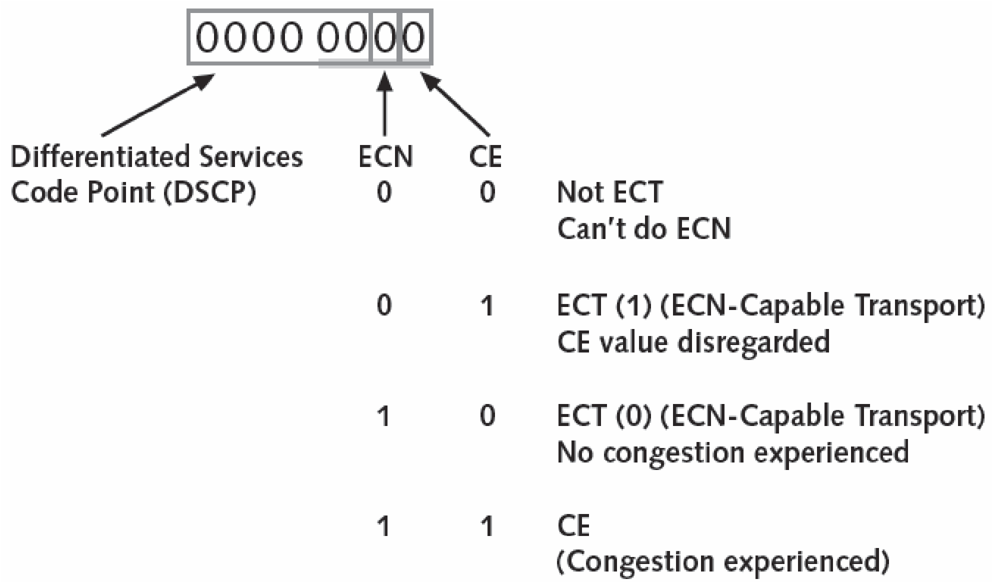


Figure 3-4 Interpretations of the ECN and CE bits

Total Length Field

- Defines the length of the IP header and any valid data
- 16-bit field

Identification Field

- Each individual packet is given a unique ID value when it is sent
- If the packet must be fragmented
  - Same ID number is placed in each fragment
- 16-bit field

Flags Field

Location	Field Definition	Value/Interpretations
Bit 0	Reserved	Set to 0
Bit 1	Don’t Fragment bit	0=may fragment; 1=don’t fragment
Bit 2	More Fragments bit	0=last fragment; 1=more to come

Table 3-5 **Flags field values**

Fragment Offset Field

- Only used if the packet is fragmented
- Shows where to place this packet's data
  - When reassembling fragments at destination host
- Gives the offset in 8-byte values
- 13-bit field

Time to Live Field

- Time to live (TTL)
  - Remaining distance that the packet can travel
- Defined in terms of seconds
  - Value is implemented as a number of hops
- Typical starting TTL values are 32, 64, and 128
  - Maximum TTL value is 255
  - Can less than or greater than starting values
- 8-bit field

Protocol Field

- Defines what is coming up next,8-bit

Number	Description
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
6	Transmission Control Protocol (TCP)
8	Exterior Gateway Protocol (EGP)
9	Any private interior gateway, such as Cisco's IGRP
17	User Datagram Protocol (UDP)
45	Inter-Domain Routing Protocol (IDRP)
58	Internet Control Message Protocol version 6 (ICMPv6)
88	Cisco EIGRP
89	Open Shortest Path First (OSPF)
92	Multicast Transport Protocol (MTP)
115	Layer Two Tunneling Protocol (L2TP)

Table 3-6 Common Protocol field values

Header Checksum Field

- Provides error detection on the contents of the IP header only
  - In addition to the data link error-detection mechanism, like CRC (Cyclic Redundancy Check) in Ethernet
- Required for packets that pass through routers
- 16-bit field

Source Address Field

- IP address of the IP host that sent the packet
- Cannot contain a multicast or broadcast address
- If address is unknown
  - 0.0.0.0 could be used instead

Destination Address Field

- Final destination of the packet
  - Can include a unicast, multicast, or broadcast address

Options Fields

- IP header can be extended by several options
- Options must end on a 4-byte boundary
- Exist primarily to provide additional IP routing controls

Padding

- Used to make sure the header ends at the 32-bit boundary
- Consists of whatever number of 0-filled bytes
  - Making IPv4 header end on a 32-bit boundary

IPv6 Header Fields and Functions

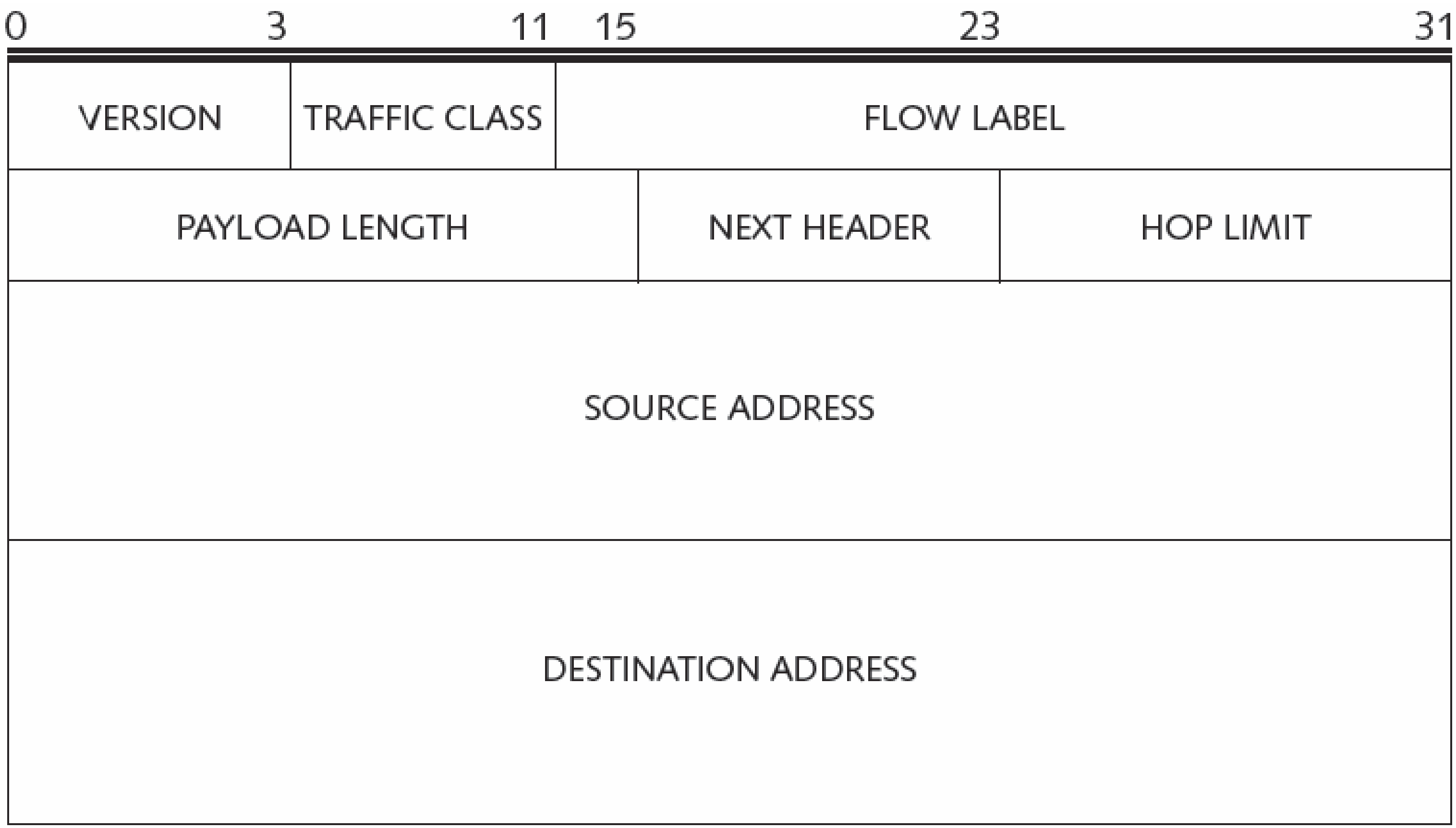


Figure 3-6 IPv6 header structure

Version

- 4-bit IP version number
  - Will always be 6 (bit sequence 0110)

Traffic Class

- 8-bit field
- Used by source network hosts and forwarding routers
  - To distinguished classes or priorities in IPv6 packets

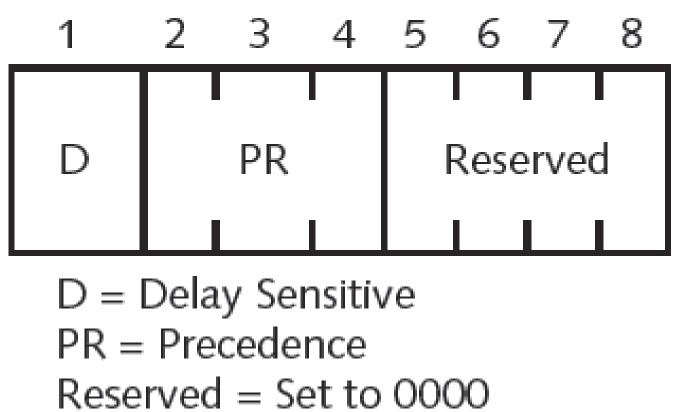


Figure 3-7 Traffic Class field structure

Flow Label Field

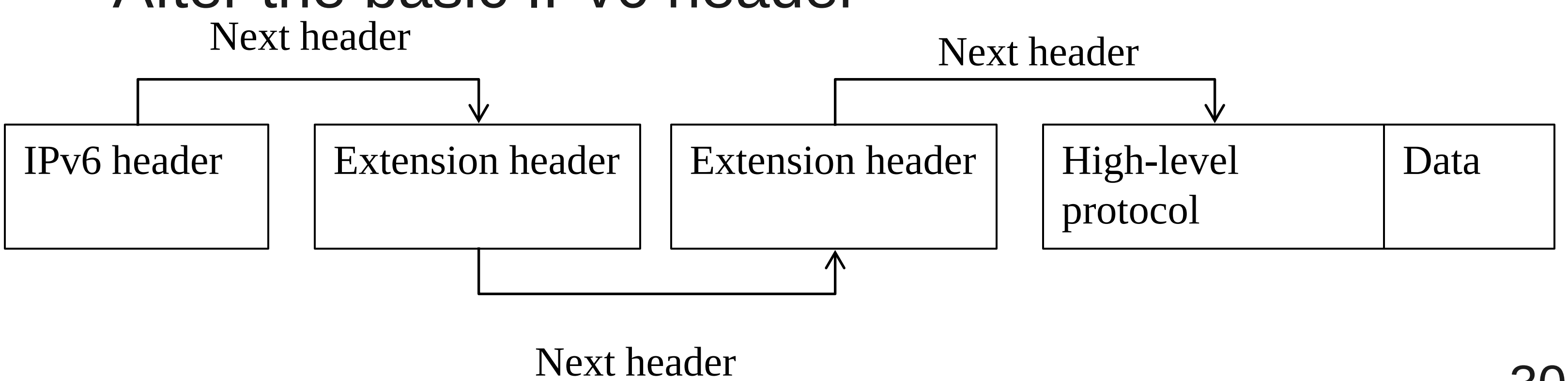
- 20-bit field
- Flow
  - Set of packets
  - Source host requires special handling by the intervening IPv6 routers using this field
- RFCs
  - 3697: Proposed standard
- Value of the Flow Label 0
  - For packets not part of any flow
- Network nodes not supporting the Flow Label must ignore this field

Payload Length Field

- 16-bit field
- Describes the size of the payload in octets
  - Including any extension headers
- Length = 0
  - When Hop-by-Hop Options extension header possesses jumbogram options

The Role of the Next Header Field

- Significant addition to the IPv6 header format
  - Specifies the header type of the header immediately following the IPv6 header
- When an IPv6 packet uses extension headers
  - Field points to the first extension header
- IPv6 also supports chaining headers together
  - After the basic IPv6 header



Hop Limit Field

- 8-bit Hop Limit field
  - Decrements by one each time it is forwarded by a network node
- Maximum value of 255

Source Address Field

- Contains the 128-bit address of the source of the packet

Destination Address Field

- Contains the 128-bit address of the recipient of the packet
  - May not be the final recipient of the packet if a Routing extension header is available

IPv6 Extension Headers

- Extension headers
  - Allow additional functionality to be implemented in an IPv6 packet
- Each extension header is identified by a specific Next Header value
- IPv6 packet can carry 0 header or several extension headers
- Extension headers are strictly processed in the required order

IPv6 Extension Headers (cont'd)

Decimal	Hexadecimal	Extension headers or protocol
0	00	Hop-by-Hop options extension header
1	01	ICMPv4
2	02	IGMPv4
4	04	IP-in-IP encapsulation
6	06	TCP
8	08	EGP
17	11	UDP
41	29	IPv6
43	2B	Routing extension header
44	2C	Fragment extension header
50	32	ESP extension header
51	33	Authentication extension header
60	3C	Destination option extension header

Extension Header Ordering

- As defined in RFC 2460:
  - Hop-by-Hop Options
  - Destination Options
  - Routing
  - Fragment
  - Authentication
  - Encapsulating Security Payload (ESP)

Hop-by-Hop Options Extension Header

- Allows maximum flexibility in header definition and functionality

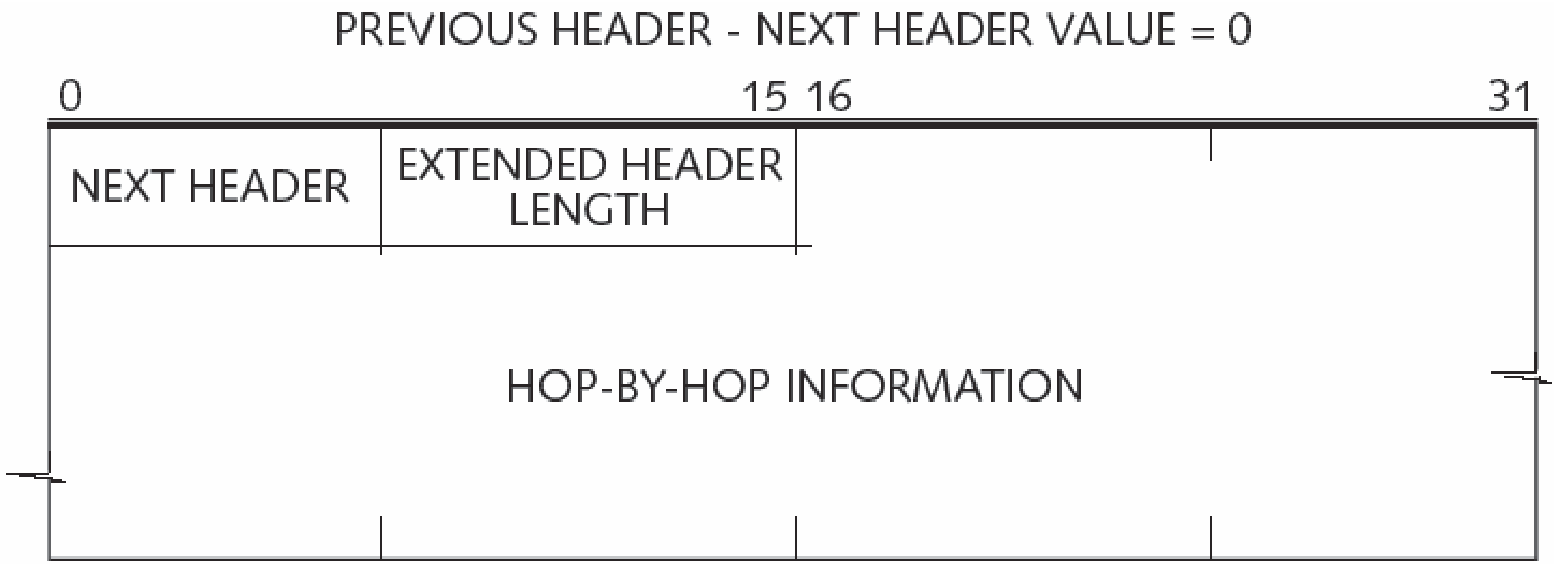


Figure 3-10 Hop-by-Hop Options extension header

Destination Options Extension Header

- Support options for packet handling and preferences
- Encrypt it if it appear after ESP, it can be checked just for the last destination host

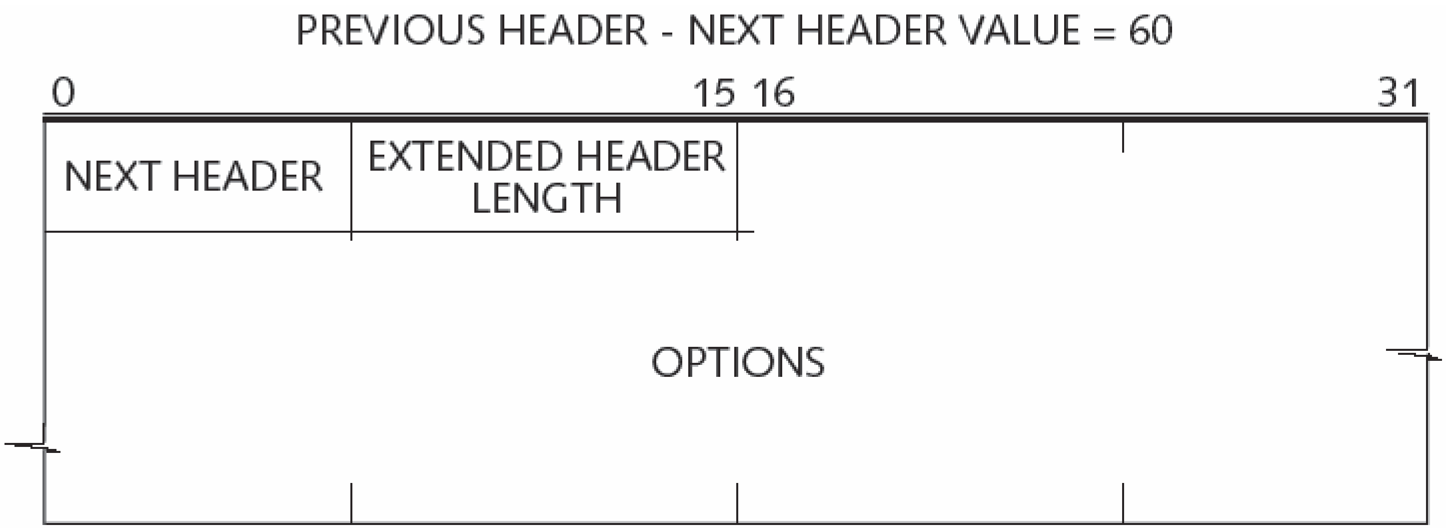


Figure 3-11 Destination Options extension header

Routing Extension Header

- Supports strict or loose source routing for IPv6

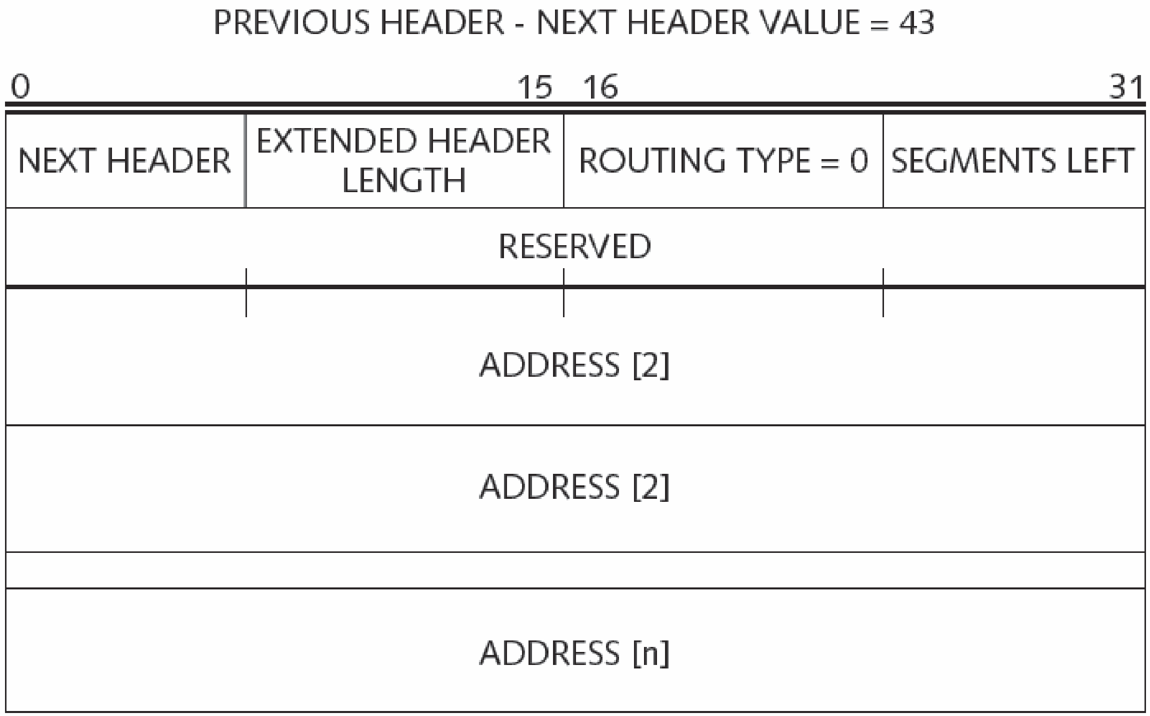


Figure 3-12 Routing extension header

Fragment Extension Header

- IPv6 does not support fragmentation at forwarding routers
- For packets that are larger than the PMTU
  - IPv6 Fragment extension header is used
  - Flag M, 0 for last segment, 1 for others

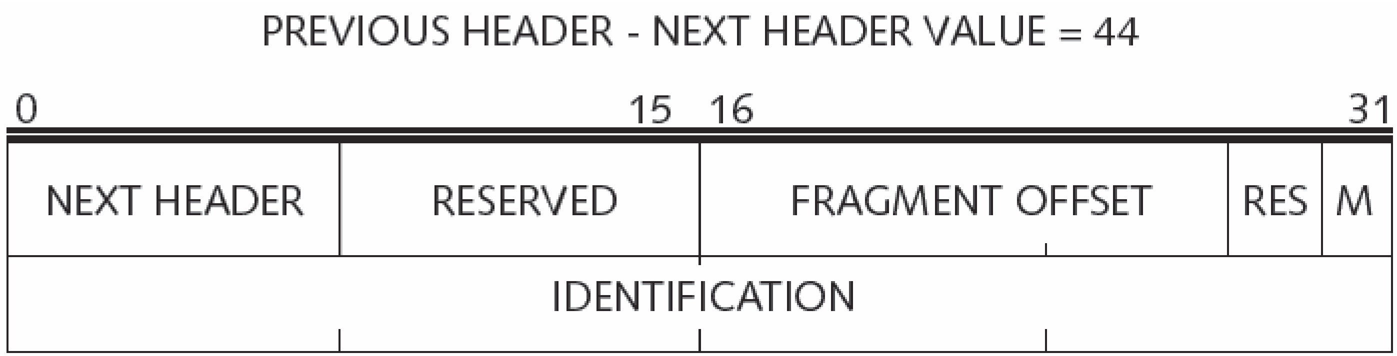


Figure 3-13 Fragment extension header

Authentication Extension Header

- Specifies the true origin of a packet and provides integrity check

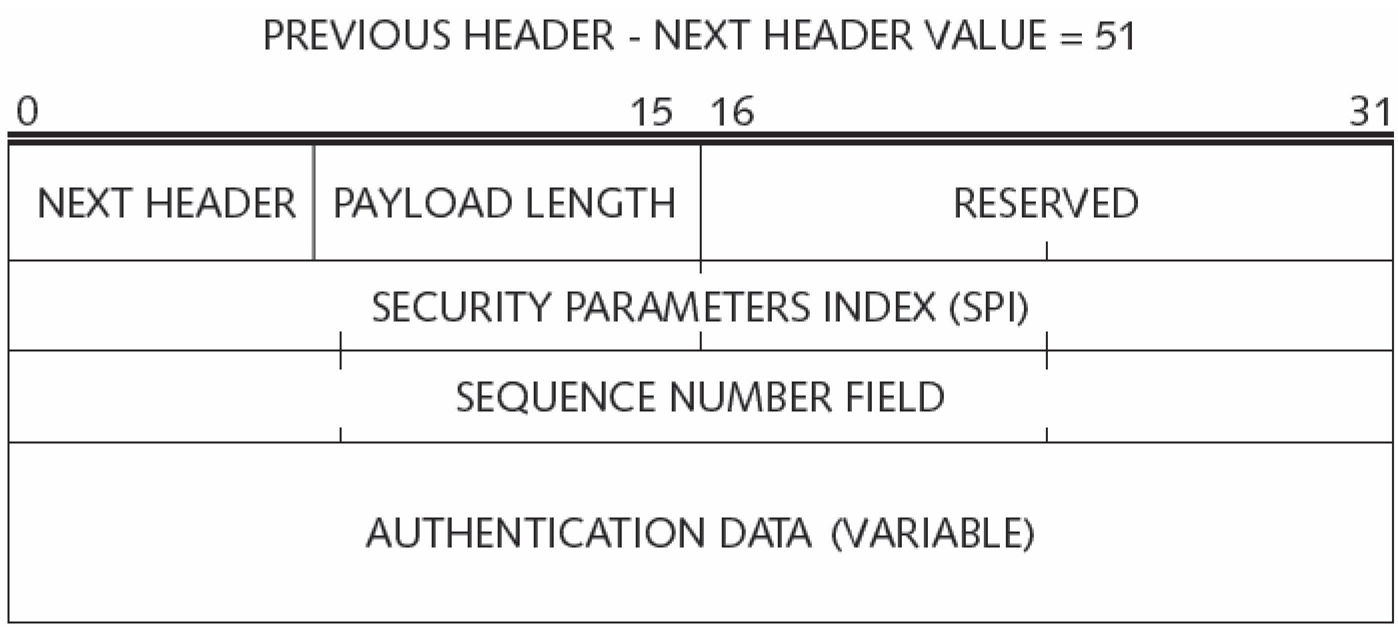
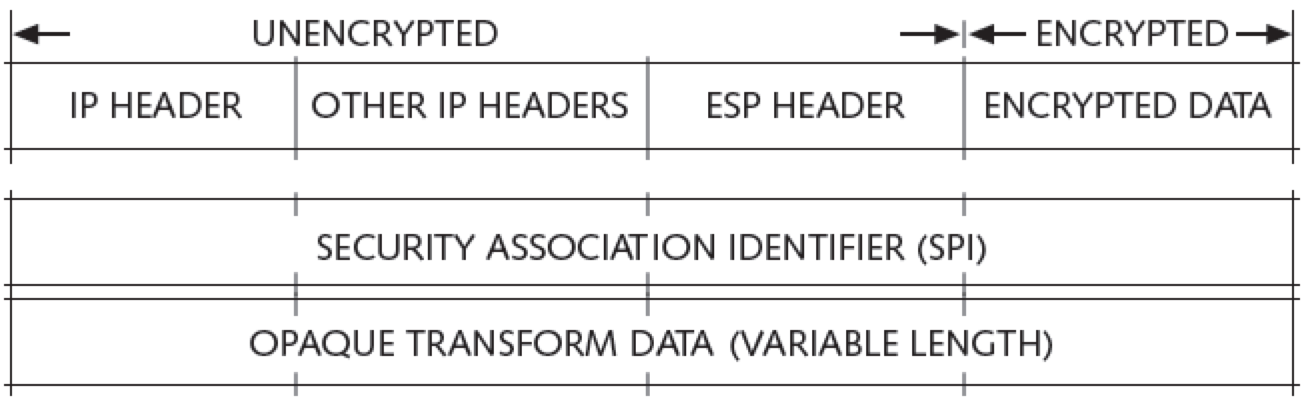


Figure 3-15 Authentication extension header

Encapsulating Security Payload Extension Header and Trailer

- Used to encrypt data
- Must always be the last header of the header chain
  - Indicates the start of encrypted data
- Encapsulating Security Payload extension header (Figure 3-16):



Jumbograms

- Jumbograms
  - Very large packets
  - Use the Hop-by-Hop Options extension header to add an alternate Packet Length field of 32 bytes
  - Carry a single chunk of data larger than 64 kilobytes
    - Up to over four billion bytes

Quality of Service

- Quality of Service
  - Ability of a network to provide better service to specific types of network traffic
- Handled by the *diffserv* working group at the IETF
  - Per-hop behavior (PHB)
  - Per-domain behavior (PDB)
- Resource Reservation Protocol (RSVP)
  - Early attempt to promote a more formal approach to dynamic resource allocation on the Internet

Router Alerts and Hop-by-Hop Options

- IPv6 header
  - Eliminates all the fields relating to QoS
- RFC 2711
  - Defines the router alert option in the Hop-by-Hop Options extension header
- Router alert option
  - Tells intervening routers to examine the packet more closely for important information

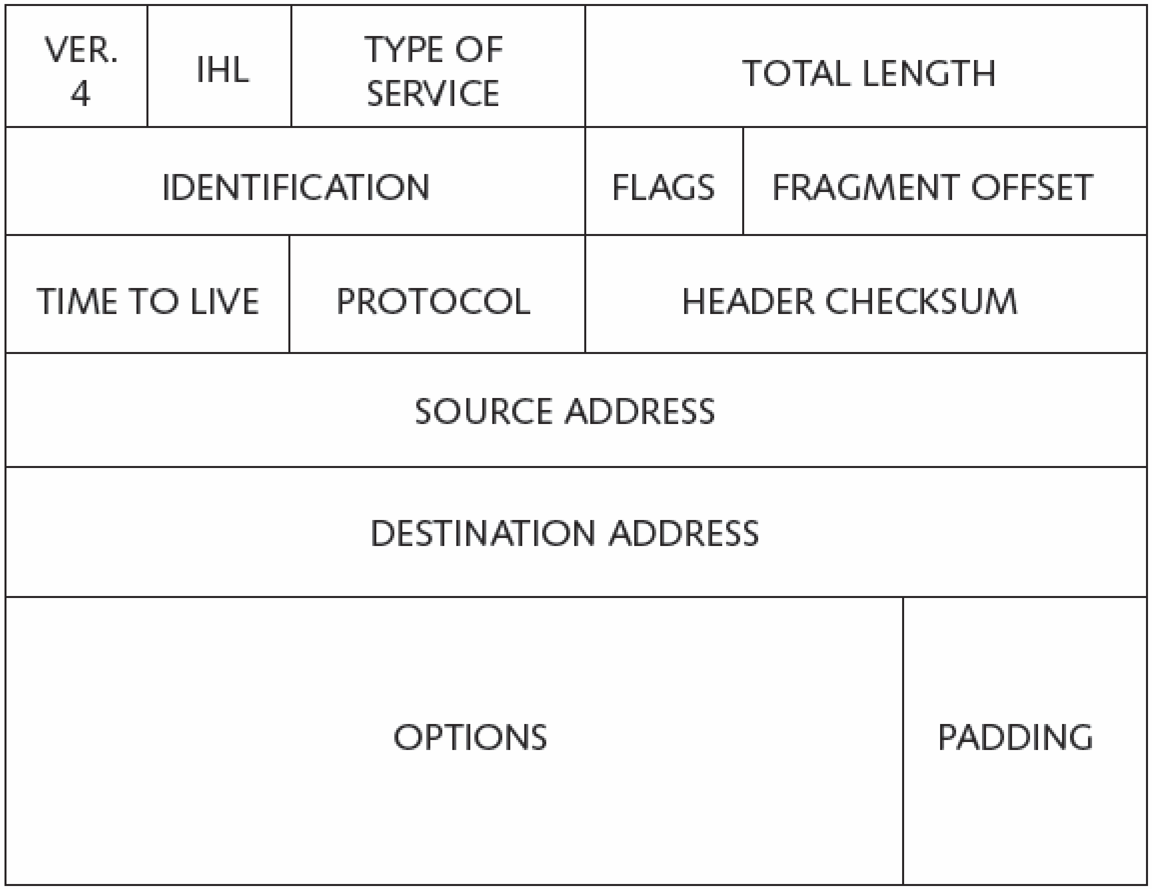
IPv6 MTU and Packet Handling

- Path MTU (PMTU) Discovery
  - Mechanism in IPv6 for discovering the MTU of an arbitrary network path
  - Defined in RFC 1981
  - Determines if the PMTU has increased or can accommodate a larger PMTU size
- Supports multicast as well as unicast transmissions

Upper-Layer Checksums in IPv6

- Upper-layer protocol containing addresses from the header in the checksum computation
  - Must include the 128-bit IPv6 address
- When running UDP over IPv6
  - Checksum is mandatory
  - Pseudo-header is used to imitate the actual IPv6 header

A Rationale for IPv6 Header Structures vis-à-vis IPv4



IPv4 HEADER

Figure 3-21 Side-by-side comparision of IPv4 and IPv6 packet structures

A Rationale for IPv6 Header Structures vis-à-vis IPv4 (cont'd.)

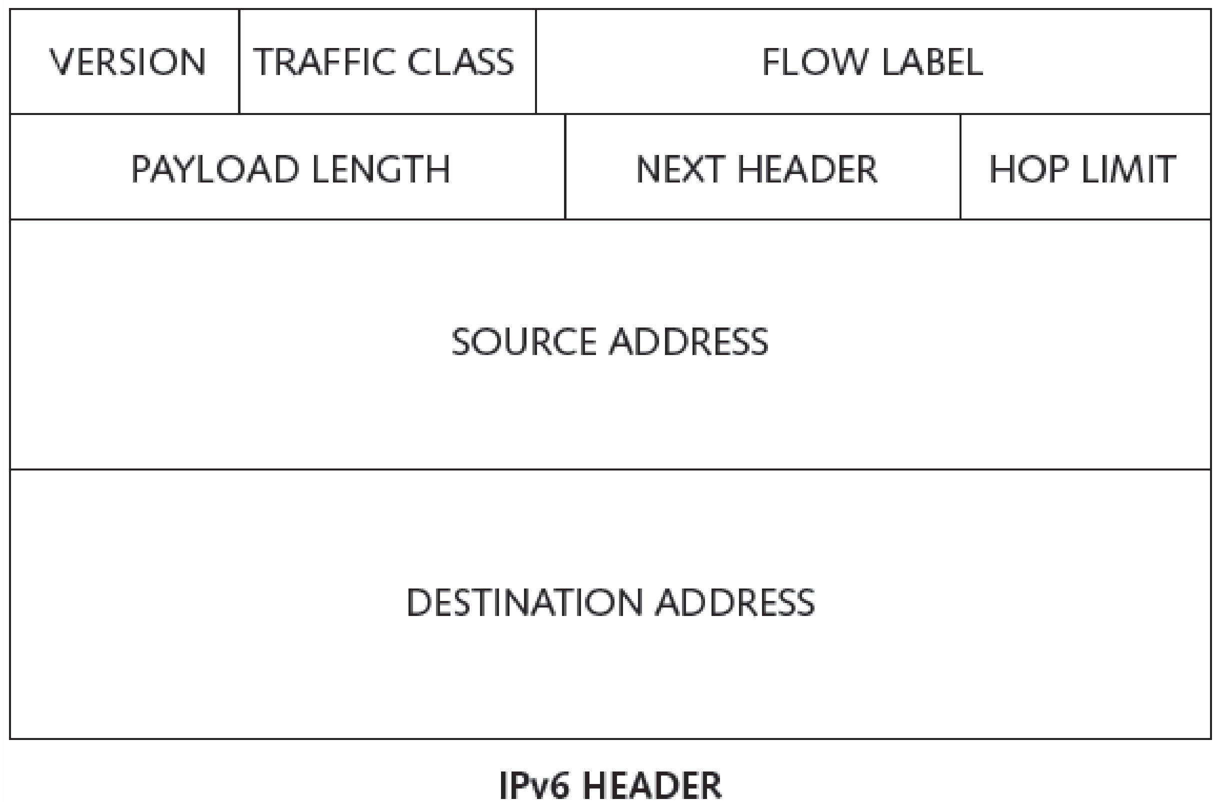


Figure 3-21 Side-by-side comparision of IPv4 and IPv6 packet structures

Comparing IPv4 and IPv6 Headers

IPv4	IPv6
The IPv4 header includes a checksum.	The IPv6 header does not include a checksum.
The IPv4 header does not identify packet flows for QoS management by routers.	The IPv6 header uses a Flow Label field to identify packet flows for QoS management by routers.
The IPv4 header includes an Options field.	The IPv6 header does not manage options; any optional data is managed by extension headers.
ICMPv4 Router Discovery is used to determine the best default gateway to the destination address; however, this action is optional.	ICMPv6 Router Solicitation and Router Advertisement messages are used to discover the best default gateway to the destination address; this action is mandatory.
IPv4 must support a 576-byte packet size, which can be fragmented.	IPv6 must support a 1,280-byte packet size, which is not fragmented.
Packets are fragmented by the source network node and by routers.	Packets are fragmented only by the source network node.
TTL decrements packet hops as a function of time (1 second = 1 hop).	Hop Limit decrements packet hops as a function of distance.

Table 3-11 **Comparison of IPv4 and IPv6 headers**

A Summary of the IPv4 to IPv6 Transition

- RFC 3056 (“6to4”)
  - Specifies an optional method for IPv6 sites to communicate with one another over IPv4 networks without setting up tunneling
  - Prone to misconfigured network nodes
  - Pop name is 6to4
- Transport Relay Translator (TRT)
  - Allows IPv6 network nodes to send and receive TCP and UDP traffic with IPv4 network nodes
  - Just for bidirectional data flow

Summary

- IPv4 header fields have been the method for providing reliable sending and receiving of data on networks for decades
- The IPv6 header structure is much simpler than the one for IPv4, but it performs the same basic function
- IPv6 extension headers are used to add any special functionality to an IPv6 Packet
- The Hop-by-Hop Options extension header carries data that affects routers along the network path

Summary (cont'd.)

- Jumbograms are a special type of service for IPv6 packets that can use the Hop-by-Hop Options extension header to add an alternate packet length field for the packet
- IPv6 MTU Discovery (technically, PMTU Discovery) is the ability of a source node to discover the maximum MTU size
- Upper-layer checksums are mandatory when running UDP over IPv6

Summary (cont'd.)

- Although the IPv6 header is much larger than the IPv4 header, that's mainly because of the much larger address space for IPv6
- The significant differences between IPv4 and IPv6 packet headers illustrate these protocols' incompatibility
  - Punctuate the difficulty in transitioning a worldwide internetwork infrastructure to the latest version of IP

Homework

- Developing a glossary of this chapter
  - English full name (Acronym): Chinese full name
  - E.g. Transmission Control Protocol (TCP): 传输控制协议
- Exercises
  - 1~25
- Hands-on projects
  - 3-1~3-3
  - Write only one project report for all projects