第18章 网际协议(2) IPv6

南京大学计算机系 黄皓教授

2007年10月26日 星期五

1. Introduction

Background of IPv6

- The Internet is growing extremely rapidly.
- The latest Internet Domain Survey, conducted in January 2000, counted over 109.5 million hosts.
- The IPv4 addressing scheme provides for over 4 billion possible addresses, which is 40 times as many Internet hosts.
- Unfortunately, this is not the case for a number of reasons.

Problem of *IP Address Exhaustion*.

- An IP address is divided into a network portion and a local portion which are administered separately.
- Although the address space within a network may be very sparsely filled, allocating a portion of the address space (range of IP addresses) to a particular administrative domain makes all addresses within that range unavailable for allocation elsewhere.

Problem of *IP Address Exhaustion*.

- Two level addressing (network and host) wastes space
- Network addresses used even if not connected to Internet
- Growth of networks and the Internet
- Extended use of TCP/IP
- Single address per host

Problem of *IP Address Exhaustion*.

- It is estimated that the IP address space would be exhausted at some point between 2005 and 2011.
- The use of CIDR and the increased use of DHCP may have relieved pressure on the address space.
- On the other hand, current growth rates are probably exceeding that expectation.

The Problem of IPv4

- Other restrictions in IPv4 also call for the definition of a new IP protocol:
  - Even with the use of CIDR, routing tables, primarily in the IP backbone routers, are growing too large to be manageable.
  - Traffic priority, or class of service, is vaguely defined, scarcely used, and not at all enforced in IPv4, but highly desirable for modern real-time applications.

- In view of these issues, the IETF established an IPng (IP next generation) working group and published ***RFC 1752***
  - The Recommendation for the IP Next Generation Protocol.

Significant features of IP v6

- Expanded address space
  - 128 bit
  - It is said to be sufficient for at least the next 30 years
- Globally unique and hierarchical addressing
  - based on prefixes rather than address classes, to keep routing tables small and backbone routing efficient
- Improved option mechanism
  - Separate optional headers between IPv6 header and transport layer header
  - Most are not examined by intermediate routes
    - Improved speed and simplified router processing
    - Easier to extend options
- Address autoconfiguration
  - Dynamic assignment of addresses

Significant features of IP v6

- Improved Support for Extensions and Options
- Support for encapsulation of itself and other protocols
- Class of service that distinguishes types of data
- The scalability of multicast routing is improved by adding a "scope" field to multicast addresses.
- Built-in authentication and encryption
- Transition methods to migrate from IPv4
- Compatibility methods to coexist and communicate with IPv4

Development of IPv6 Abroad

- US，Europe，Japan

- IETF：Internet Engineering Task Force
- ICANN：Internet Corporation For Assigned Names Numbers
- IPv6 Forum
- The 3rd Generation Partnership Project
- ITU

IP v6 在中国的发展

- 当26个中国人分享一个IP地址的时候，平均每个美国人享有 6 个IP地址。
- 2003年由信息产业部等8个部委联合发起并经国务院批准启动了国家级战略项目：中国下一代互联网示范工程CNGI（China Next Generation Interne）,IPv6是CNGI的一项重要技术。

RFCs on IPv6

No. RFC	Date	Title	
1752	1995	The Recommendation for the IP Next Generation Protocol	
1883	1995	Internet Protocol, Version 6 (IPv6) Specification	
1884	1995	IP Version 6 Addressing Architecture	
1885	1995	Internet Control Message Protocol (ICMPv6) for the Internet ProtocolVersion 6 (IPv6)	
1886	1995	DNS Extensions to support IP version 6	
2373	1998	IP Version 6 Addressing Architecture	

RFCs on IPv6

No. RFC	Date	Title	
1970	1996	Neighbor Discovery for IP Version 6 (IPv6)	
1971	1996	IPv6 Stateless Address Autoconfiguration	
2460	1998	Internet Protocol, Version 6 (IPv6) Specification	
2461	1998	Neighbor Discovery for IP Version 6 (IPv6).	
2462	1998	IPv6 Stateless Address Autoconfiguration	
2463	1998	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.	

RFCs on IPv6

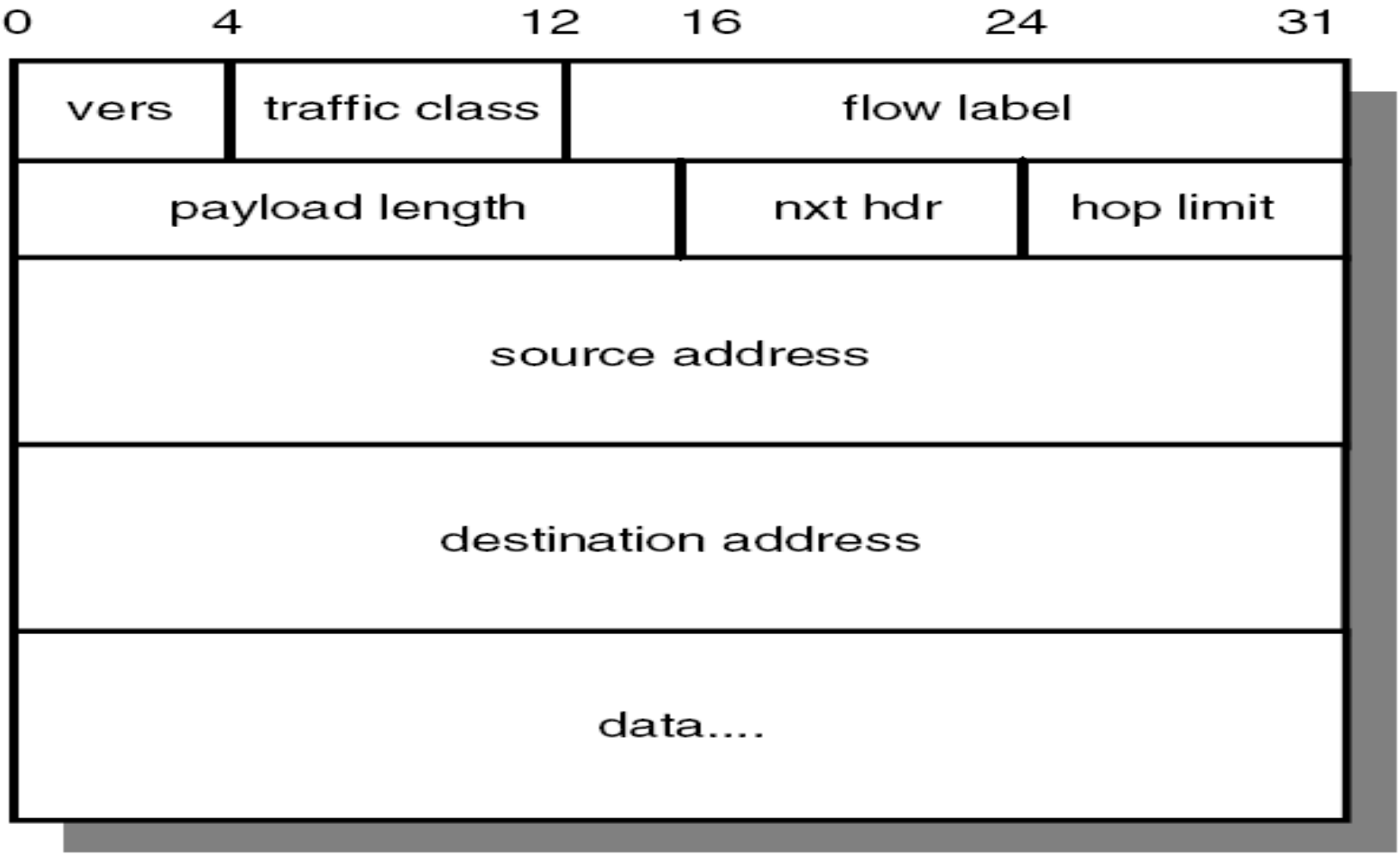
3315	**2003**	**Dynamic Host Configuration Protocol for IPv6 (DHCPv6).**	
3513	**2003**	**Internet Protocol Version 6 (IPv6) Addressing Architecture.**	
3736	**2004**	**Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6.**	
2893	**2000**	**Transition Mechanisms for IPv6 Hosts and Routers**	
4213	**2005**	**Basic Transition Mechanisms for IPv6 Hosts and Routers**	

RFCs on IPv6

No. RFC	Date	Title	
1970	1996	Neighbor Discovery for IP Version 6 (IPv6)	
2461	1998	Neighbor Discovery for IP Version 6 (IPv6).	
1971	1996	IPv6 Stateless Address Autoconfiguration	
2462	1998	IPv6 Stateless Address Autoconfiguration	
3736	2004	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6.	
3315	2003	Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	

2. The IPv6 header format

IPv6 Basic header



IPv6 Basic header

- **Vers**
  - 4-bit Internet Protocol version number: 6.
- **Traffic class**
  - The 8-bit traffic class field allows applications to specify a certain priority for the traffic they generate, thus introducing the concept of *Class of Service*.
  - This enables the prioritization of packets, as in Differentiated Services.
- Flow Label
  - Used by hosts requesting special handling

IPv6 Basic header

- Payload length
  - The length of the packet in bytes (excluding this header)
  - If length is greater than 64 KB, this field is 0 and an option header (Jumbo Payload) gives the true length.
- Source Address
- Destination address

IPv6 Basic header

- **Next Header**
  - Indicates the type of header immediately following the basic IP header.
  - It may indicate an IP option header or an upper layer protocol.

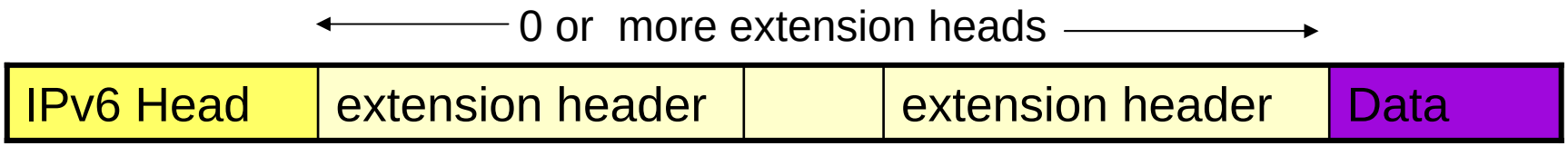
41 IPv6 Header

45 Interdomain Routing Protocol

46 Resource Reservation Protocol

58 IPv6 ICMP Packet

0 Hop-by-Hop Options Header
43 IPv6 Routing Header
44 IPv6 Fragment Header
50 Encapsulating Security Payload
51 IPv6 Authentication Header
59 No Next Header
60 Destination Options Header

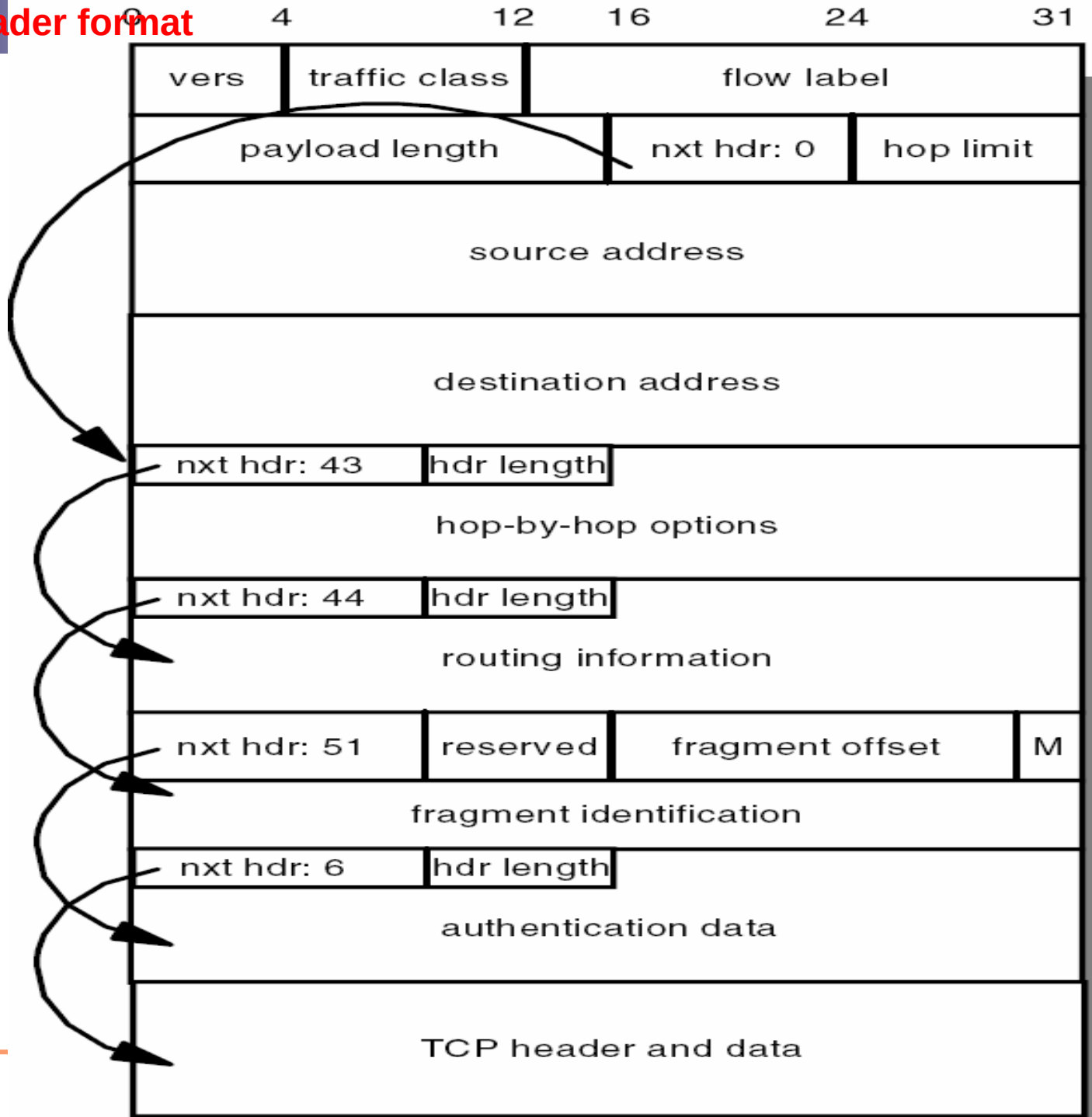


Extension headers

- Every IPv6 packet starts with the basic header.
- Extension headers are used for additional information to be conveyed along with the packet to the destination or to intermediate systems on route.
- Extension headers are placed immediately after the IPv6 basic packet header and are counted as part of the payload length.
- Each extension header has its own 8-bit *Next Header field* as the first byte of the header that identifies the type of the following header.
- This structure allows IPv6 to chain multiple extension headers together.

2. The IPv6 header format

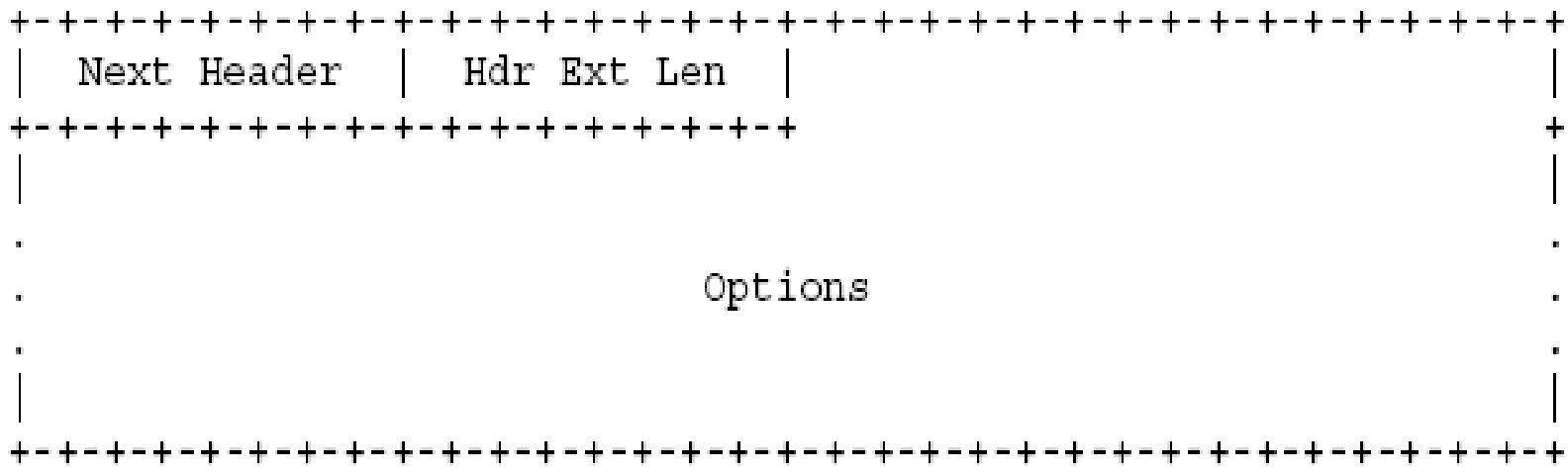
example packet with multiple extension headers



- The length of each header varies, depending on type, but is always a **multiple of 8 bytes**.
- IPv6 nodes that originate packets are required to place extension headers in a specific order.
- The order is important for efficient processing at intermediate routers.
- Routers will generally only be interested in the hop-by-hop options and the routing header.
- IPv6 allows for encapsulation of IPv6 within IPv6 ("tunneling"). This is done with a Next Header value of 41 (IPv6).

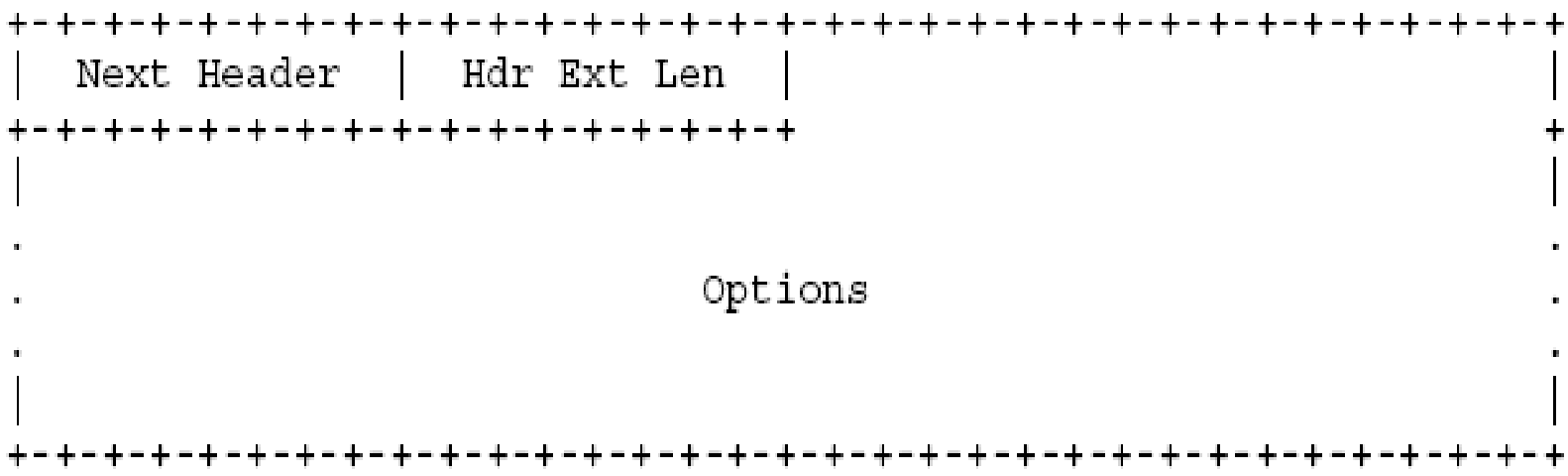
Hop-by-hop header

- A Hop-by-hop header contains options that must be examined by every node the packet traverses, as well as the destination node.
- It must immediately follow the IPv6 header (if present) and is identified by the special value 0 in the Next Header field of the IPv6 basic header.



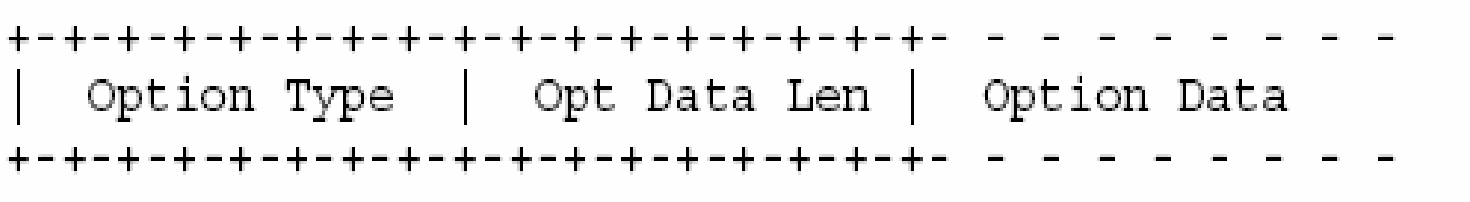
Hop-by-hop header

- examined by every node the packet traverses
- immediately follow the IPv6 header
- Options
  - Variable-length field, of length such that the complete Hop-by-Hop Options header is an integer multiple of 8 octets long.
  - Contains one or more TLV-encoded options

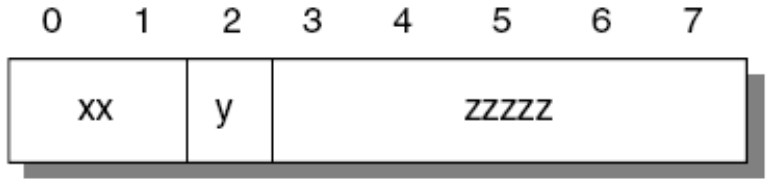


Hop-by-hop header

type-length-value (TLV) encoded "options"



- Option Type



- **XX** A 2-bit number, indicating how an IPv6 node that does not recognize the option should treat it:
  - **0** Skip the option and continue.
  - **1** Discard the packet quietly.
  - **2** Discard the packet and inform the sender with an ICMP Unrecognized Type message.
  - **3** Discard the packet and inform the sender with an ICMPUnrecognized Type message unless the destination address is a multicast address.

Hop-by-hop header

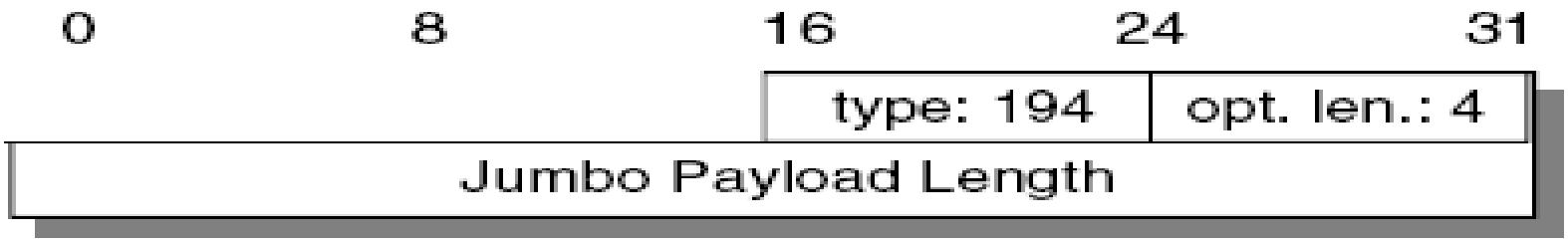
type-length-value (TLV) encoded "options"

- **Y: If set, this bit indicates that the value of the option may change en route.**
  - If this bit is set, the entire Option Data field is excluded from any integrity calculations performed on the packet.
- **Zzzzz**
  - **0** Pad1
  - **1** PadN
  - **194** Jumbo Payload Length

Hop-by-hop header

type-length-value (TLV) encoded "options"

- **Pad1**
  - A X'00' byte used for padding a single byte. NOTE! the format of the Pad1 option is a special case -- it does not have length and value fields.
- **PadN**
  - For N octets of padding, the Opt Data Len field contains the value N-2, and the Option Data consists of N-2 zero-valued octets.
- **Jumbo Payload Length**



Routing header

Routing header

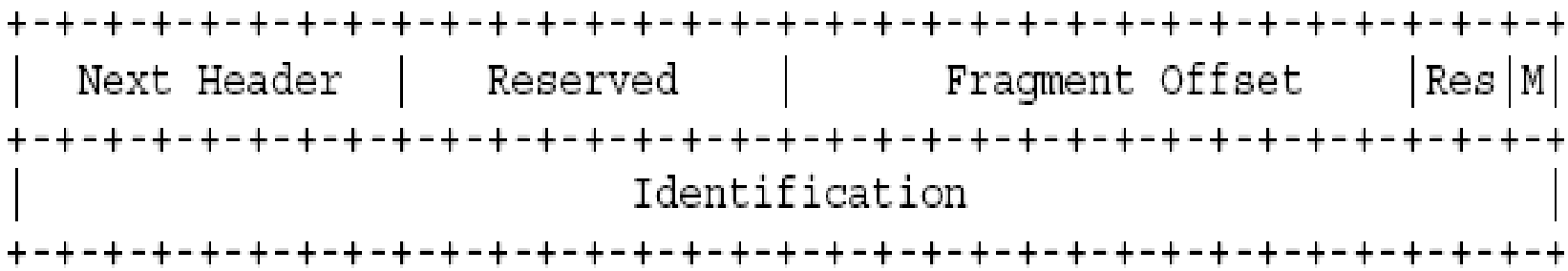
- The source may wish to have more control over the route taken by the packet.
- It may wish, for example, for certain data to take a lower but more secure route than would normally be taken.
- The routing header allows a path through the network to be predefined.
- The only type defined initially is type 0 - Strict/Loose Source Routing.

Routing header

- The first hop on the required path of the packet is indicated by the destination address in the basic header of the packet.
- When the packet arrives at this address, the router swaps the next address from the router extension header with the destination address in the basic header.
- The router also decrements the segments left field by one, then forwards the packet.

Fragment header

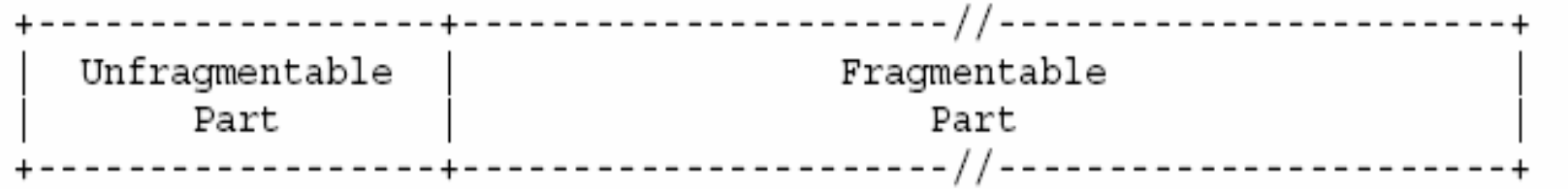
- The Fragment header is used by an IPv6 source to send a packet larger than would fit in the path MTU to its destination.
- Fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.



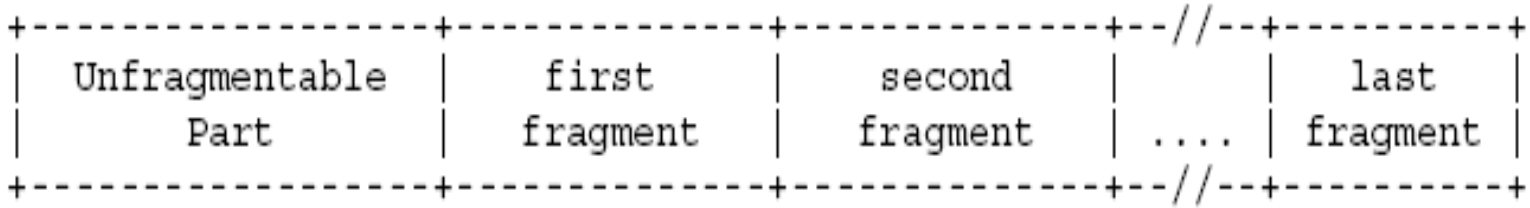
- Res 2-bit reserved field. Initialized to zero for transmission; ignored on reception.
- M flag 1 = more fragments; 0 = last fragment.

Fragment header

- original packet:

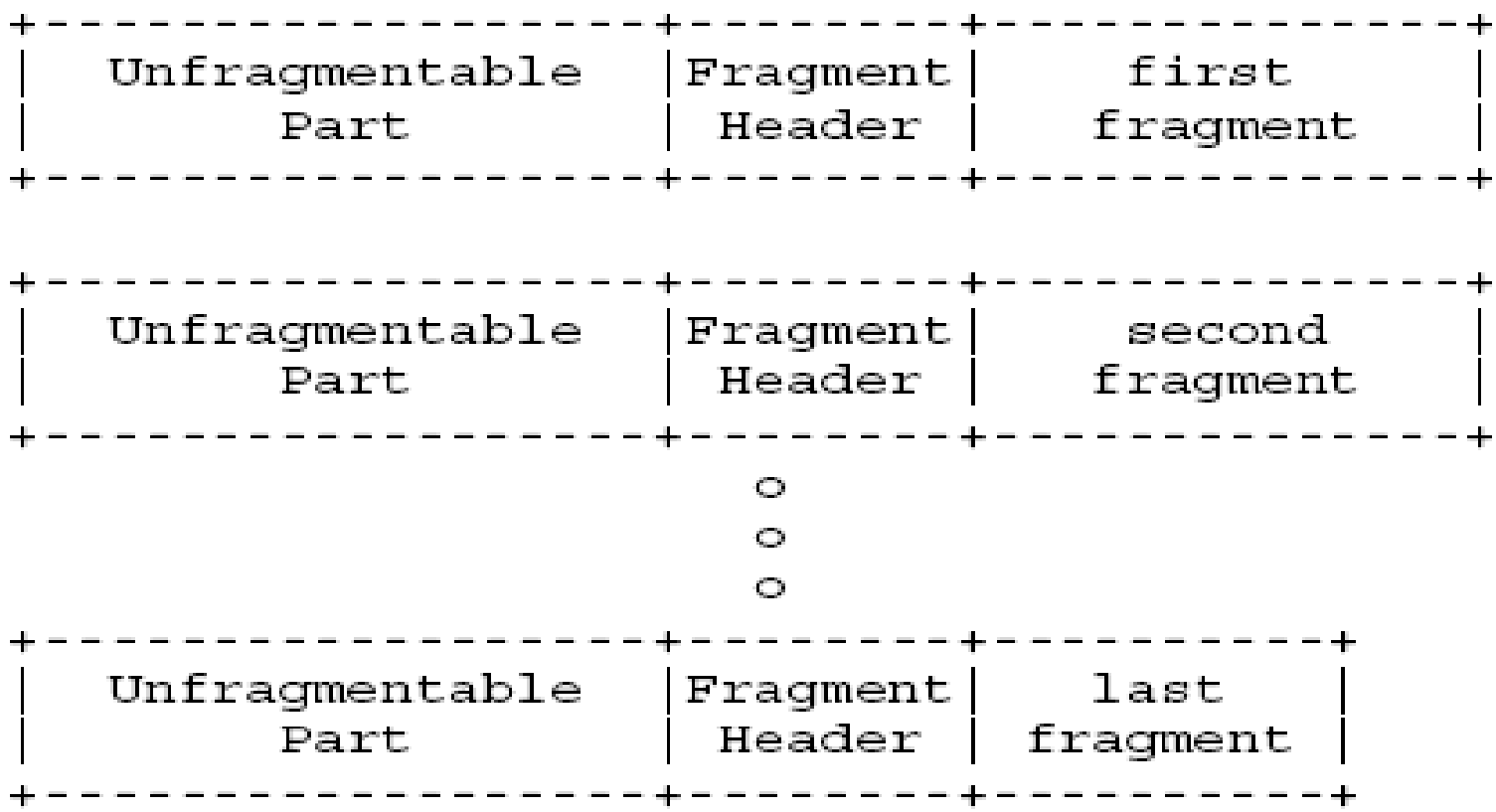


- The Unfragmentable Part consists of the IPv6 header plus any extension headers that must be processed by nodes en route to the destination.



Fragment header

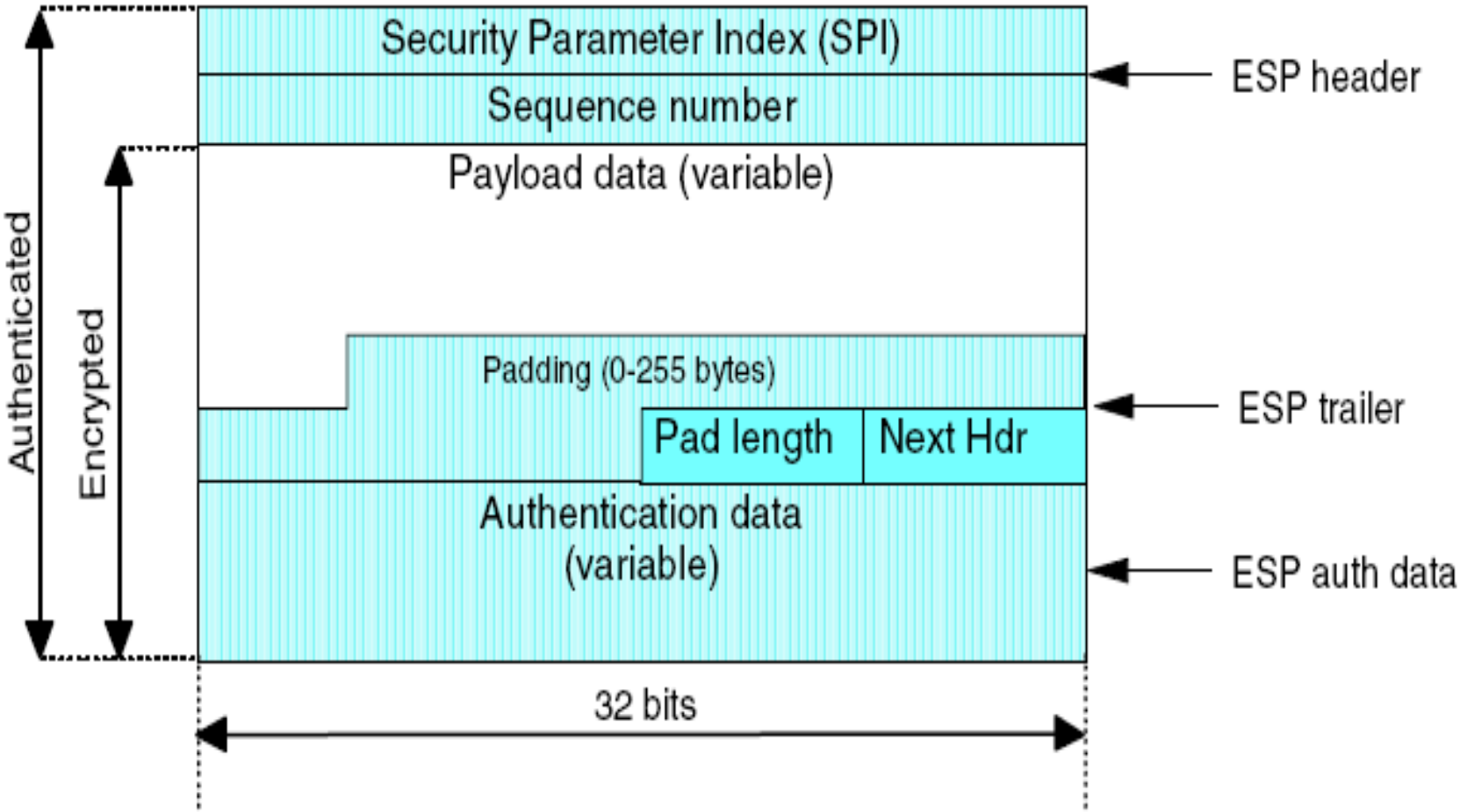
fragment packets:



Authentication header

Next header	Payload length	Reserved
Security parameter index (SPI)		
Sequence number		
Authentication data		

Encapsulating Security Payload



Destination options header

- The value for the preceding Next Header field is 60.
- Normally, the destination options are only intended for the final destination only and the destination options header will be ***immediately before the upper layer header.***
- Destination options can also be intended for intermediate nodes, in which case they must ***precede a routing header***.

3. Pv6 addressing

RFC3513：Internet Protocol Version 6 (IPv6) Addressing Architecture.

RFC2373： IP Version 6 Addressing Architecture

Addressing Model

- IPv6 addresses of all types are assigned to interfaces, not nodes.
- All interfaces are required to have at least one link-local unicast address.
- A single interface may also have multiple IPv6 addresses of any type (unicast, anycast, and multicast) or scope.

- IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces
- There are three types of addresses
  - **Unicast**: An identifier for a single interface.
  - **Anycast**: An identifier for a set of interfaces (typically belonging to different nodes).

    A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance).
  - **Multicast:** *An identifier for a set of interfaces (typically belonging different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.*

Text Representation of Addresses

1) The preferred form is x:x:x:x:x:x:x:x, where the 'x's are the hexadecimal values of the eight **16-bit pieces** of the address.
   - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

2) The use of "::" indicates one or more groups of 16 bits of zeros.

1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
FF01:0:0:0:0:0:0:101	FF01::101
0:0:0:0:0:0:0:1	::1
0:0:0:0:0:0:0:0	::

If there are more groups of all zeroes that are not consecutive, only one may be substituted by the double colon; the others would have tobe noted as 0.

Text Representation of Addresses (2)

3) mixed environment of IPv4 and IPv6 nodes is x:x:x:x:x:x:d.d.d.d,

- six high-order 16-bit pieces of the address
- four low-order 8-bit pieces of the address (standard IPv4 representation).

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

::13.1.68.3

::FFFF:129.144.52.38

Text Representation of Address Prefixes

- IPv6 address prefix is represented by the notation:

  ipv6-address/prefix-length

  - **ipv6-address** **is an IPv6 address**
  - **prefix-length** **how many of the leftmost contiguous bits of the address comprise the prefix.**
  - **12AB:0000:0000:CD30:0000:0000:0000:0000/60**
  - **12AB::CD30:0:0:0:0/60**
  - **12AB:0:0:CD30::/60**

Text Representation of Address Prefixes

- IPv6 address prefix is represented by the notation:

  ipv6-address/prefix-length

  12AB:0000:0000:CD30:0000:0000:0000:0000/60
  Not legal：12AB:0:0:CD3/60
  Can not differentiate from
  ::12AB:0:0:CD3/60
  12AB:0:0:CD30::/60

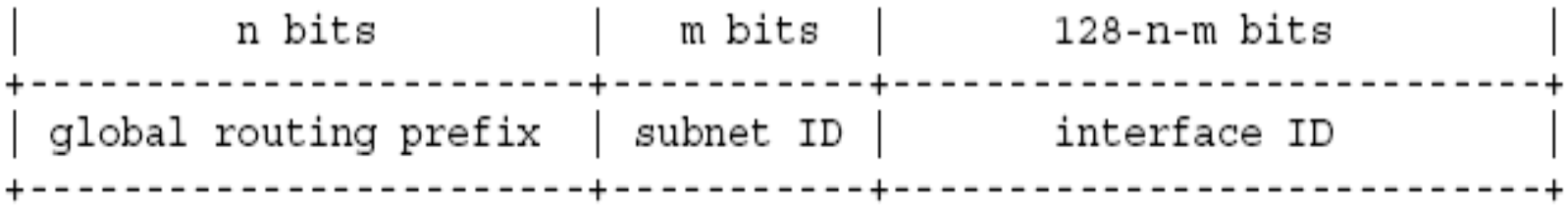
  the node address
  12AB:0:0:CD30:123:4567:89AB:CDEF

  subnet number
  12AB:0:0:CD30::/60

Unicast Addresses

- There are several types of unicast addresses in IPv6,
  - in particular：global unicast, site-local unicast, and link-local unicast.
- The Unspecified Address： 0:0:0:0:0:0:0:0
  - One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address.
- The loopback address：0:0:0:0:0:0:0:1
  - a virtual interface (typically called "the loopback interface")

Global Unicast Addresses



- global routing prefix：assigned to a site
- subnet ID：an identifier of a link within the site
- interface ID：Interface Identifiers

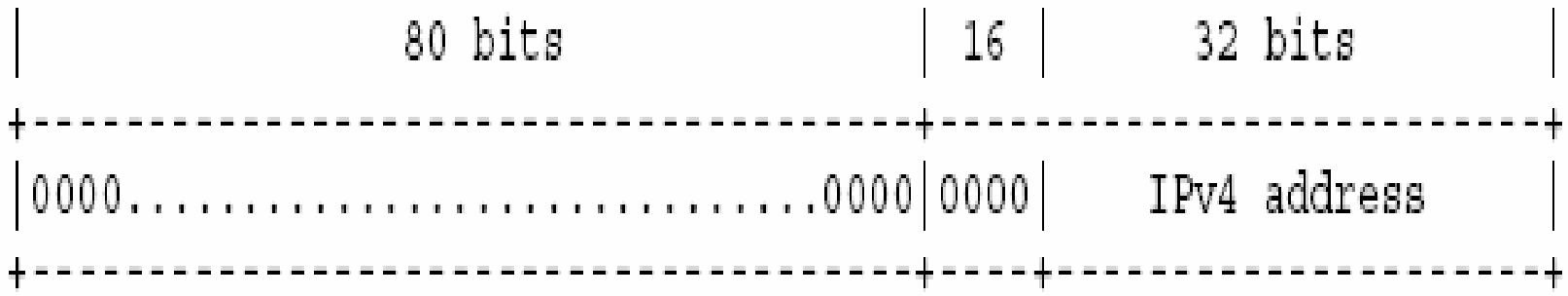
- All global unicast addresses have a 64-bit interface ID field (i.e., **n + m = 64**).
  - **Except those that start with binary value 000**.

Interface Identifiers

- Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link.
- They are required to be unique within a subnet prefix.
- It is recommended that the same interface identifier not be assigned to different nodes on a link.
- In some cases an interface's identifier will be derived directly from that interface's link-layer address.
- Note that the uniqueness of interface identifiers is independent of the uniqueness of IPv6 addresses.

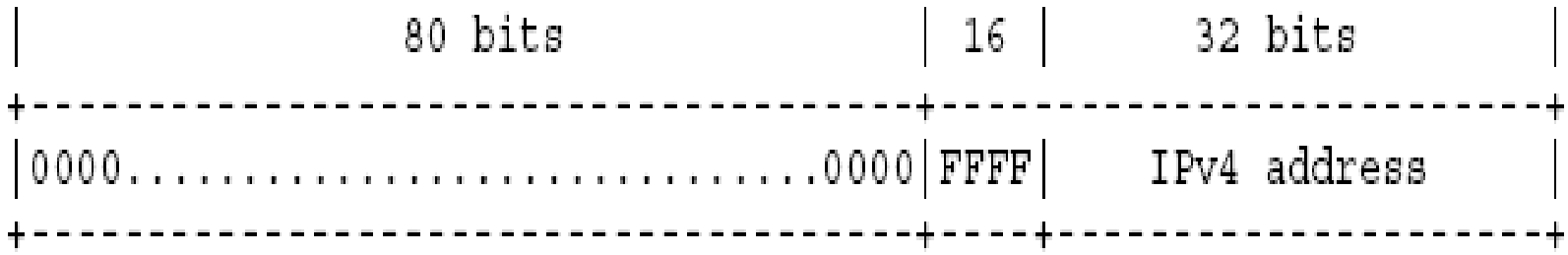
IPv6 Addresses with Embedded IPv4 Addresses

- The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure.
- IPv6 nodes that use this technique are assigned special IPv6 unicast addresses that carry a global IPv4 address in the low-order 32 bits.
- This type of address is termed an "IPv4-compatible IPv6 address" and has the format

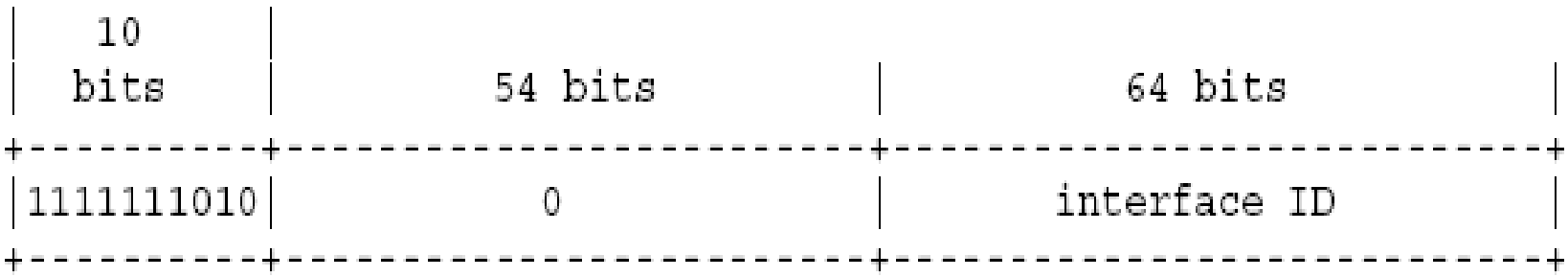


IPv6 Addresses with Embedded IPv4 Addresses

- represent the addresses of IPv4 nodes as IPv6 addresses.



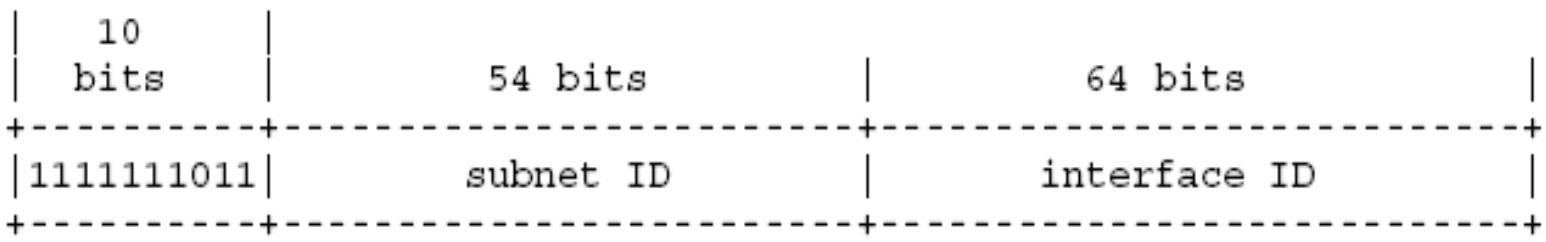
Local-Use IPv6 Unicast Addresses



10 bits	54 bits	64 bits
1111111010	0	interface ID

- Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.
- Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.

- Site-Local addresses

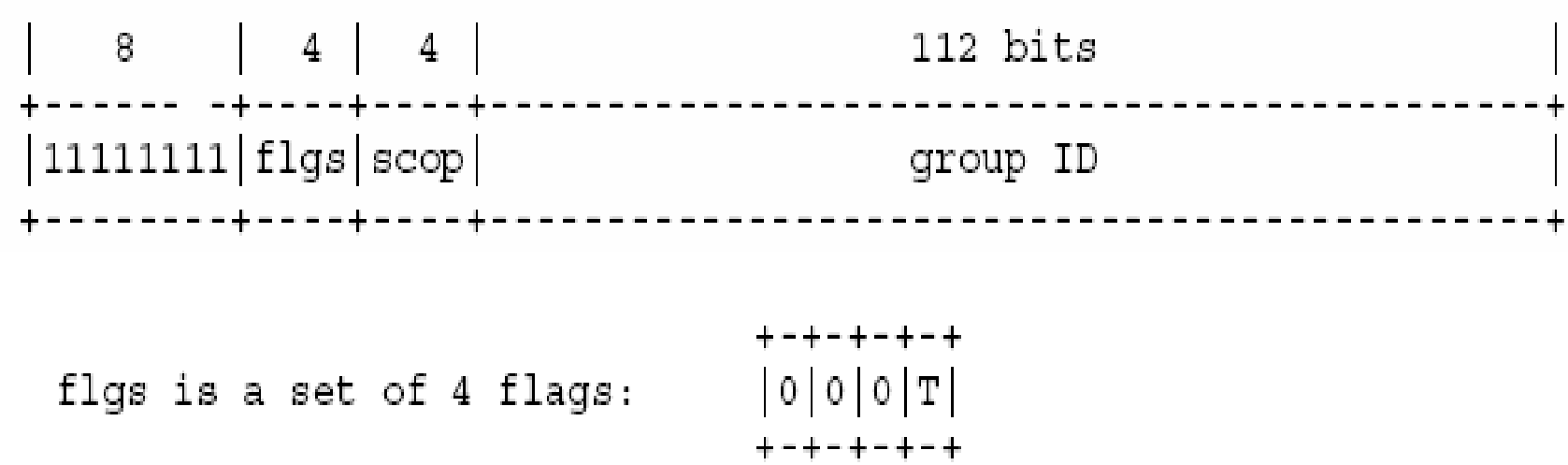


FE

Site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.

Routers must not forward any packets with site-local source or destination addresses outside of the site.

Multicast Addresses



- T = 0 indicates a permanently-assigned
- T = 1 indicates a non-permanently-assigned

Multicast Addresses

- scop is a 4-bit multicast scope value used to limit the scope of the multicast group.

1	node-local scope
2	link-local scope
5	site-local scope
8	organization-local scope
E	global scope

Reserved IPv6 Address

- **RFCV2375:** IPv6 Multicast Address Assignments.

Link-Local Scope	
FF02:0:0:0:0:0:0:1	All Nodes Address
FF02:0:0:0:0:0:0:2	All Routers Address
FF02:0:0:0:0:0:0:1	All Nodes Address
FF02:0:0:0:0:0:0:2	All Routers Address
FF02:0:0:0:0:0:0:B	Mobile-Agents
FF02:0:0:0:0:0:1:2	All-dhcp-agents
FF02:0:0:0:0:1:FFXX:XXXX	Solicited-Node Address
Site-Local Scope	
FF05:0:0:0:0:0:0:2	All Routers Address
FF05:0:0:0:0:0:1:3	All-dhcp-servers
FF05:0:0:0:0:0:1:4	All-dhcp-relay

A Node's Required Addresses

- Its Link-Local Address for each interface
- Loopback Address
- Assigned Unicast Addresses
- All-Nodes Multicast Address
- Solicited-Node Multicast Address for each of its assigned
- unicast and anycast addresses
- Multicast Addresses of all other groups which the host belongs.

4. Internet Control Message Protocol Version 6 (ICMPv6)

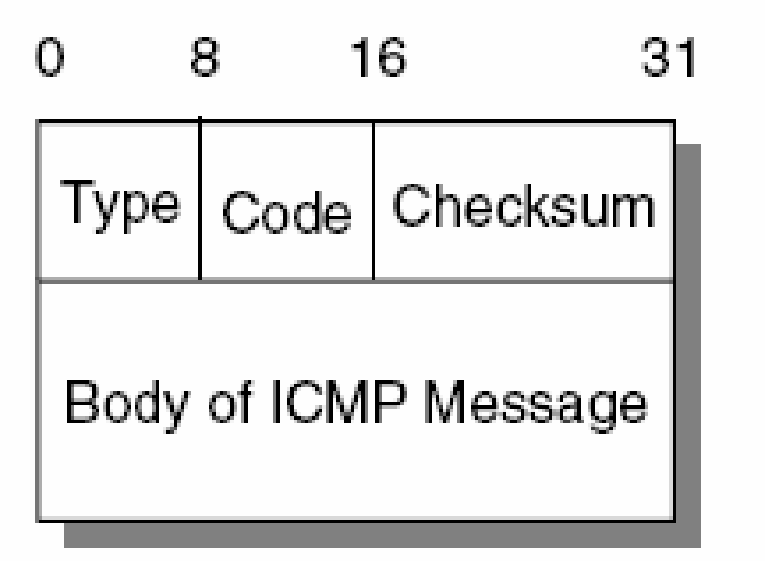
RFC2461 — **Neighbor Discovery for IP Version 6 (IPv6)**

RFC2462 — **IPv6 Stateless Address Autoconfiguration**

RFC2463 — **Internet Control Message Protocol Version 6 (ICMPv6)**

ICMPv6 messages

- Every ICMPv6 message is preceded by an IPv6 header
- The ICMPv6 header is identified by a Next Header value of **58** in the immediately preceding header.



ICMPv6 messages

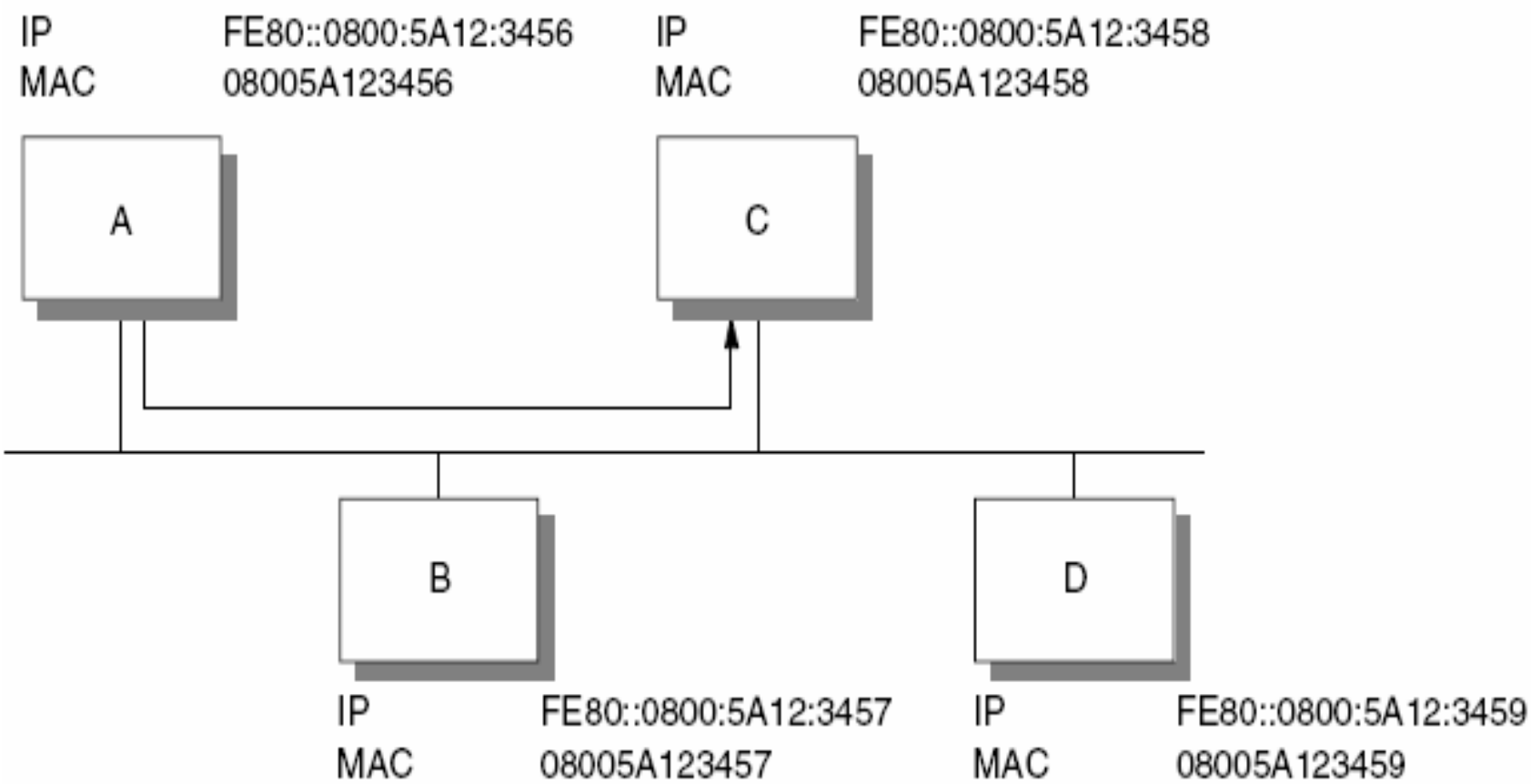
- There are two classes of ICMPv6 messages.
  - Error messages have a Type from 0 to 127.
  - Informational messages have a Type from 128 to 255.

1	Destination Unreachable
2	Packet Too Big
3	Time (Hop Count) Exceeded
4	Parameter Problem

128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message

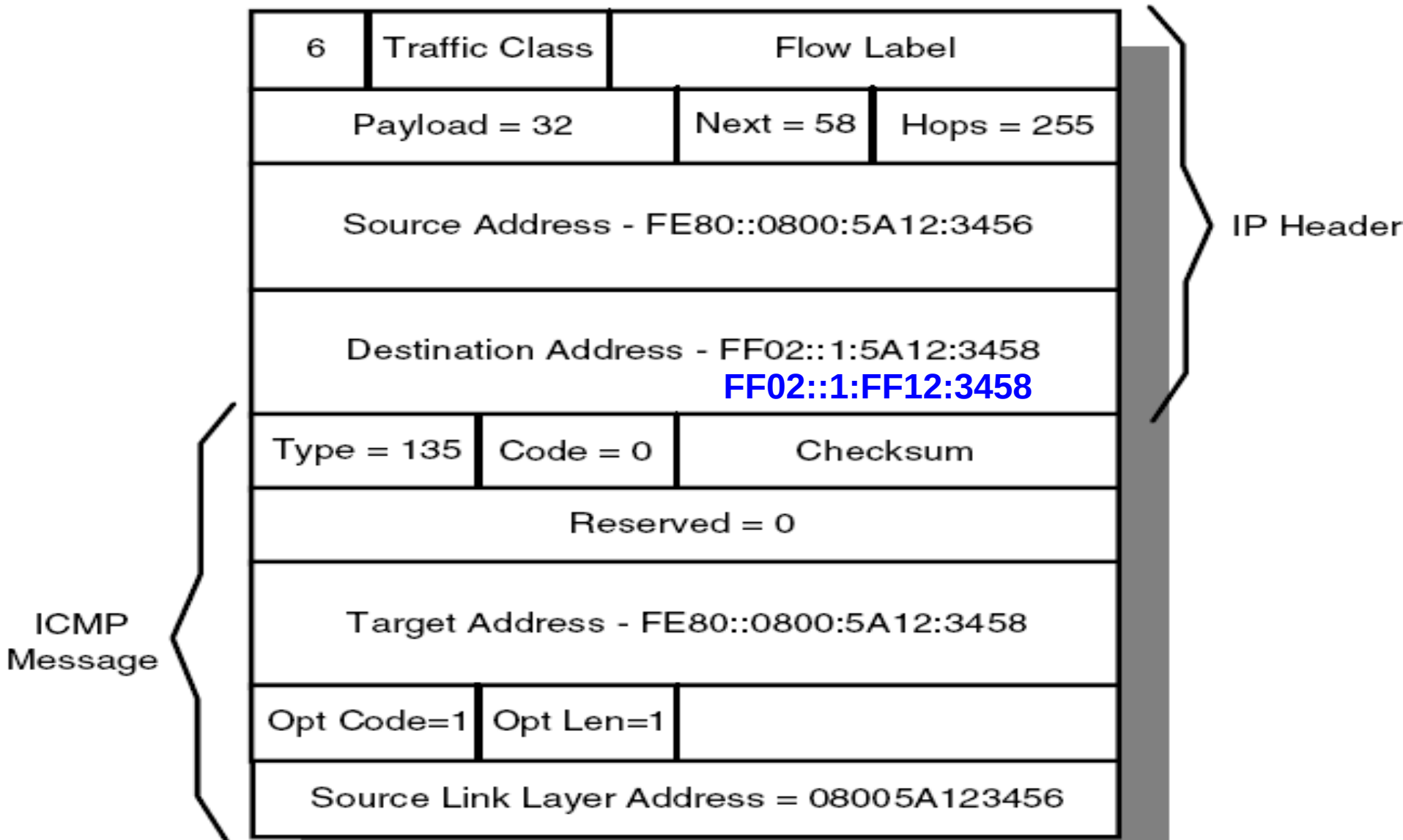
(1) Address resolution

RFC2461：Neighbor Discovery for IP Version 6 (IPv6)



(1) Address resolution

neighbor solicitation message



(1) Address resolution

neighbor solicitation message

- IP Fields
  - Destination Address
    - Either the solicited-node multicast address corresponding to the target address (here is FF02::1:FF12:3458)

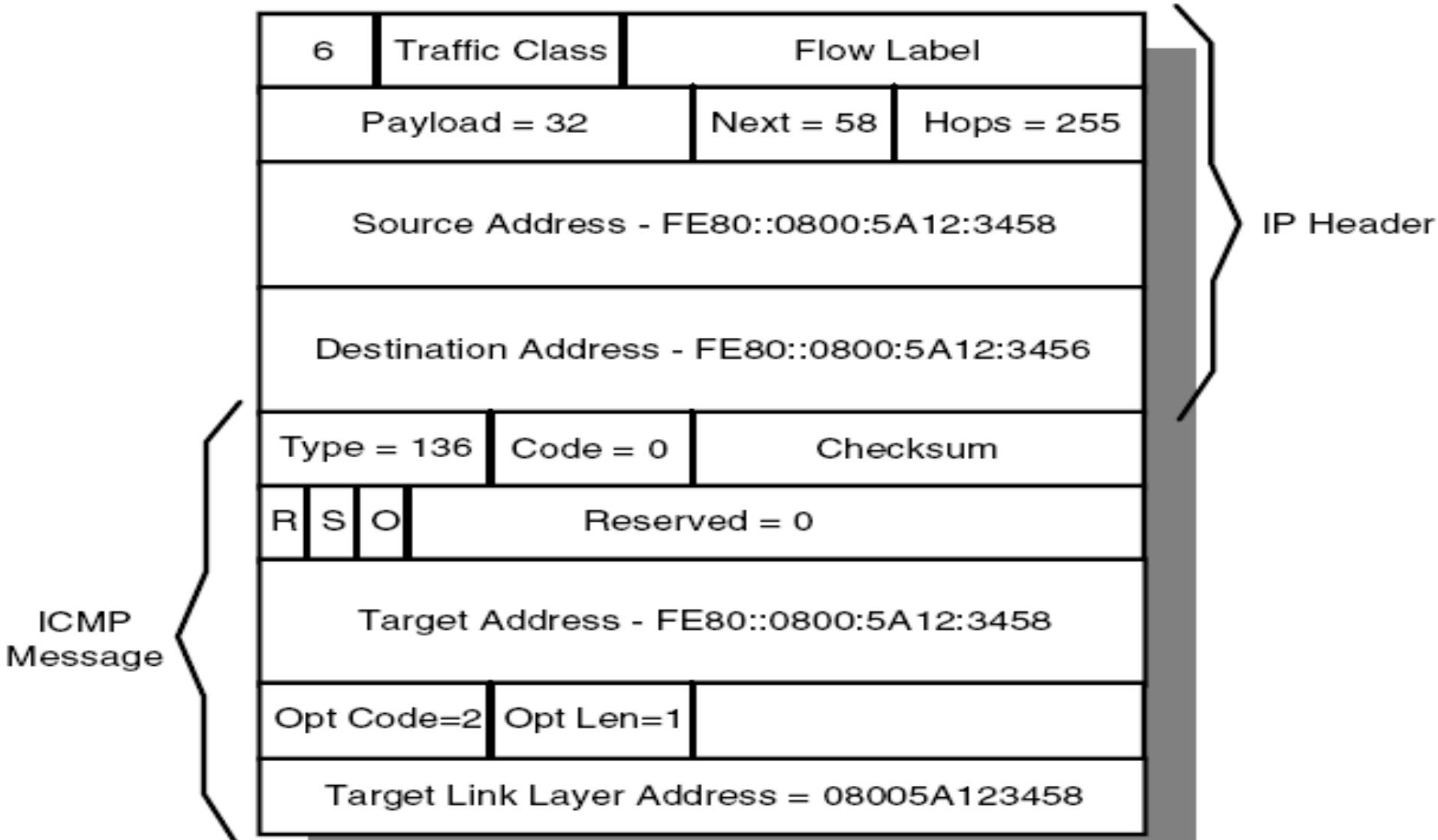
      Every workstation *must* respond to its own **solicited node address**.

      but other workstations will simply ignore it.

      This is an improvement over ARP in IPv4, which uses broadcast frames that have to be processed by every node on the link.
    - or the target address.
- ICMP Fields
  - Target Address：The IP address of the target of the solicitation. It MUST NOT be a multicast address.

(1) Address resolution

neighbor advertisement



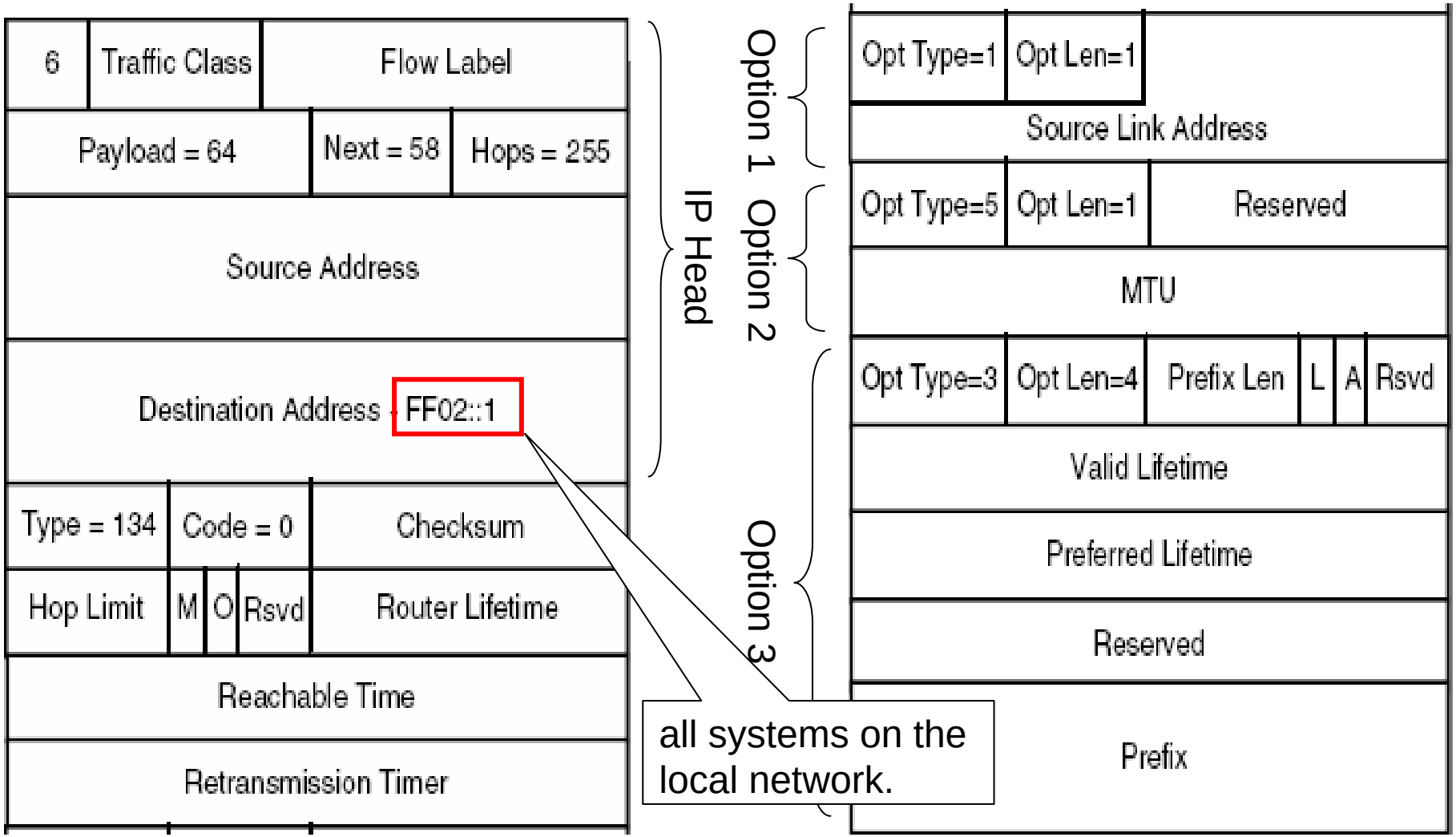
(1) Address resolution

(2007-10-30)neighbor advertisement

- The neighbor advertisement is addressed directly back to Workstation A.
- The ICMP message option contains the target IP address together with the target's link layer (MAC) address.
- Flags
  - **R** Router Flag. This bit is set on if the sender of the advertisement is a router.
  - **S** Solicited Flag. This bit is set on if the advertisement is in response to a solicitation.
  - **O** Override Flag. When this bit is set on, the receiving node must update an existing cached link layer entry in its neighbor cache.
- Neighbor advertisement messages may also be sent by a node to force updates to neighbor caches if it becomes aware that its link layer address has changed.

(2) Router and prefix discovery（RFC2461）

Router advertisement message format



（2）Router and prefix discovery

- **Destination address**
  - This address is the special multicast address defining all systems on the local link.
- **M flag**
  - If this bit is set, the node should use DHCP to obtain its IP address.
- **O flag**
  - If this bit is set then the node uses DHCP to obtain other configuration parameters.

（2）Router and prefix discovery

- **Router lifetime**
  - How long the node should consider this router to be available. If this time period is exceeded and the node has not received another router advertisement message, the node should consider this router to be unavailable.
- **Reachable time**
  - This sets a parameter for all nodes on the local link. It is the time in milliseconds that the node should assume a neighbor is still reachable after having received a response to a neighbor solicitation.
- **Retransmission timer**
  - This sets the time, in milliseconds, that nodes should allow between retransmitting neighbor solicitation messages if no initial response is received.

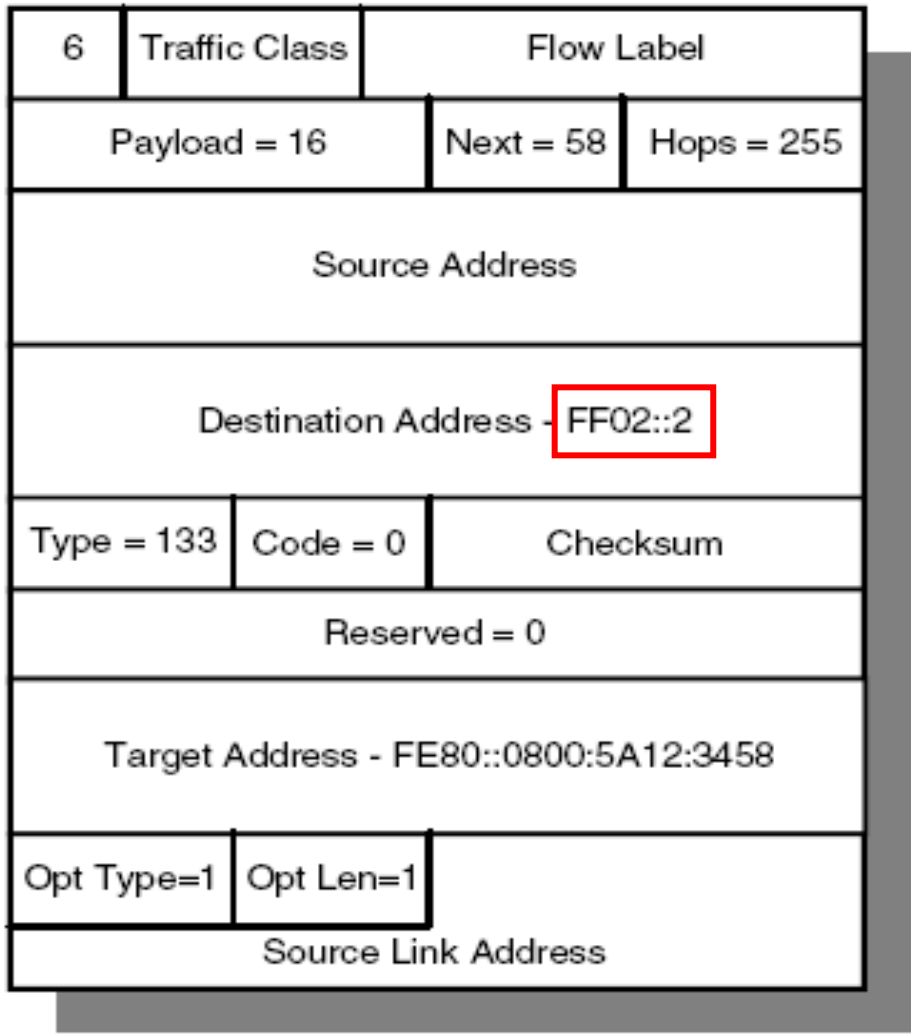
（2）Router and prefix discovery

- **Option 1 (source link address)**
  - Allows a receiving node to respond directly to the router without having to do a neighbor solicitation.
- **Option 5 (MTU)**
  - Specifies the maximum transmission unit size for the link. For some media, such as Ethernet, this value is fixed, so this option is not necessary.
- **Option 3**
  - Defines the address prefix for the link. Nodes use this information to determine when they do, and do not, need to use a router.

(2) Router and prefix discovery

Router solicitation message format

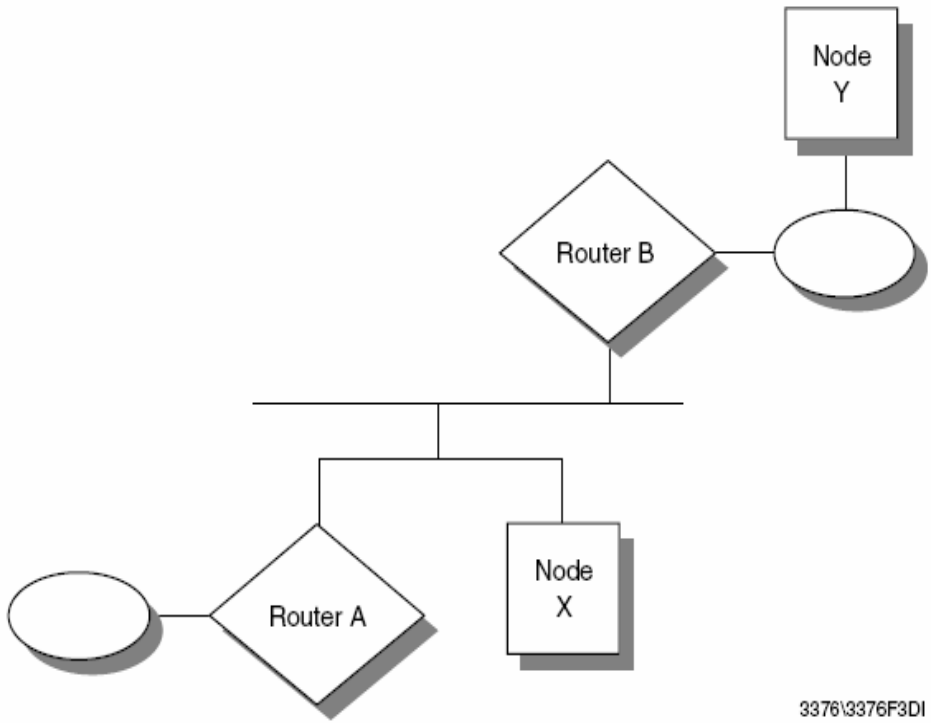
- **Destination address**
  - This address is the special multicast address defining all routers on the local link.
- **Source link-layer address**
  - The link-layer address of the sender, if known



（3）Redirection

- ICMPv6 allows for *redirection* to a more efficient path for a particular destination.

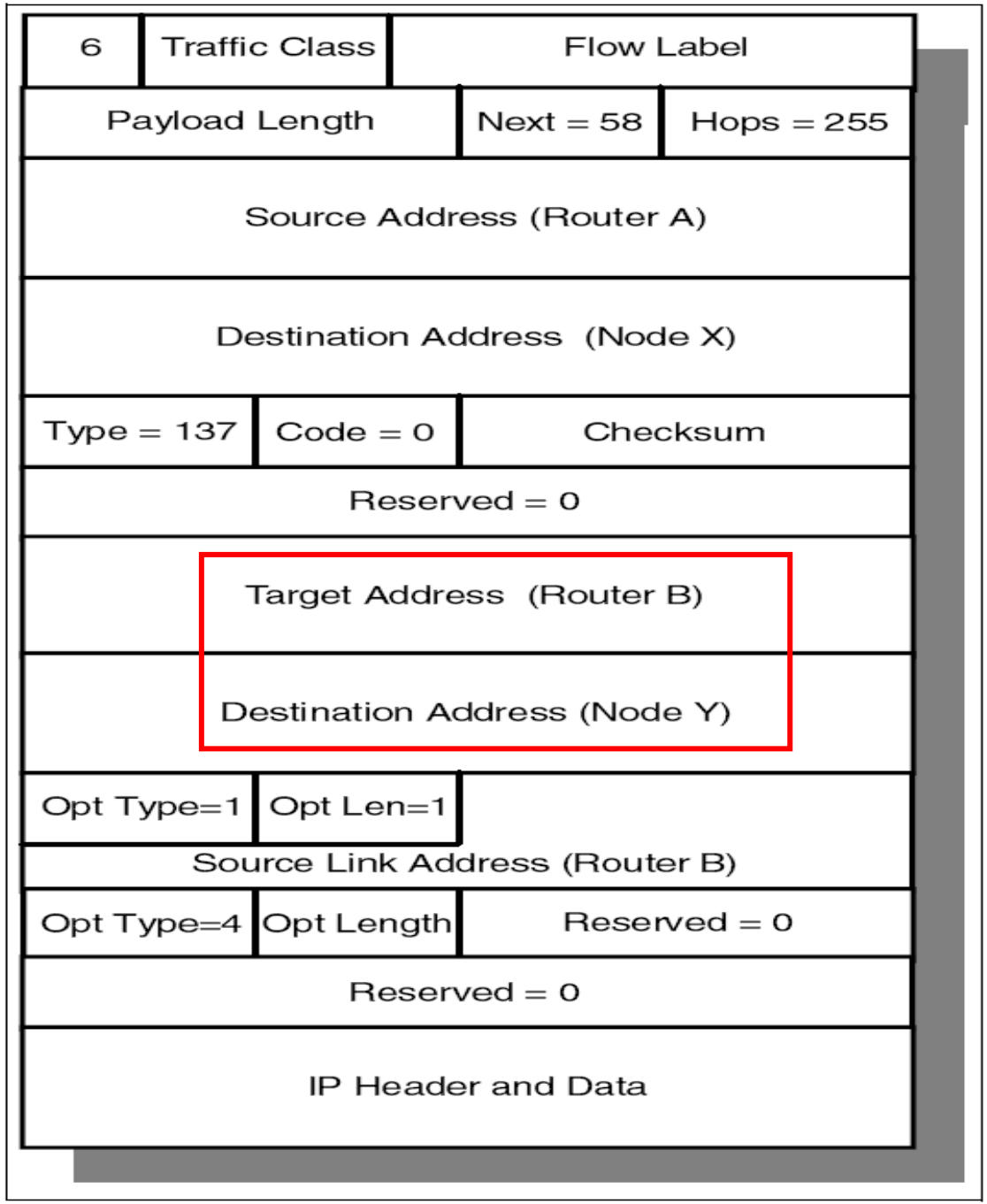
- X has received router advertisement messages from both A and B.
- X wishes to send data to Y.
- By comparing Y's IP address against the local link prefix, X knows that Y is not on the local link, and that it must therefore use a router.
- Node X selects router A from its list of default routers
- As soon as A has forwarded the packet to Y (via B), A sends a *redirect* message to X.



(3)Redirection

ICMP fields

- **Target address**
- **Destination address**
- **Option (target link layer address)**
- **Option 4 (redirected header)**



(4) Stateless address autoconfiguration

- RFC2462：IPv6 Stateless Address Autoconfiguration
- The size of the 128-bit address itself represents a potential problem to the TCP/IP administrator.
- IPv6 has been designed with the capability to automatically assign an address to an interface at initialization time.
- IPv6 nodes will generally always use autoconfiguration to obtain their IPv6 address.
  - This may be achieved using DHCP (*stateful* autoconfiguration)
  - *stateless* autoconfiguration (new feature of IPv6)

(4) Stateless address autoconfiguration

1. During system startup, the node begins the autoconfiguration by obtaining an interface token from the interface hardware, for example, a 48-bit MAC address on token-ring or Ethernet networks.
2. The node creates a tentative link-local unicast address. This is done by combining the well-known link-local prefix (FE80::/10) with the interface token.
3. The node attempts to verify that this tentative address is unique by issuing a neighbor solicitation message with the tentative address as the target.
4. If no response is received, the node assigns the link-level address to its interface.

(4) Stateless address autoconfiguration

5. The host then sends one or more router solicitations to the all-routers multicast group.
6. If there are any routers present, they will respond with a router advertisement.
7. If no router advertisement is received, the node should attempt to use DHCP to obtain an address and configuration information.
8. If no DHCP server responds, the node continues using the link-level address and can communicate with other nodes on the same link only.
9. If a router advertisement is received in response to the router solicitation, then this message contains several pieces of information that tells the node how to proceed with the autoconfiguration process

(4) Stateless address autoconfiguration

- **M flag**
  - If this bit is set, the node should use DHCP to obtain its IP address.
- **O flag**
  - If this bit is set then the node uses DHCP to obtain other configuration parameters.
- **Prefix option**

(4) Stateless address autoconfiguration

- If stateless address configuration is to be used,
  - the prefix is taken from the router advertisement and added to the interface token to form the global unicast IP address, which is assigned to the network interface.
- The working node will continue to receive periodic router advertisements.
  - If the information in the advertisement changes, the node must take appropriate action.

(4) Stateless address autoconfiguration

- it is possible to use both stateless and stateful configuration simultaneously.
- It is quite likely that stateless configuration will be used to obtain the IP address,
- but DHCP will then be used to obtain further configuration information.

(5) Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

- **RFC 3315**
- IPv6 (DHCP) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes.
- It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility.
- This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462).

(5) DHCP for IPv6

Client-server Exchanges Involving **Two Messages**

I. When a server has IPv6 addresses and other configuration information committed to a client, the client and server may be able to complete the exchange using only two messages.

II. The client sends a Solicit message to the **All_DHCP_Relay_Agents_and_Servers** requesting the assignment of addresses and other configuration information.

The server immediately responds with a Reply message. The configuration information and the addresses in the Reply message are then immediately available for use by the client.

(5) DHCP for IPv6

Client-server Exchanges Involving **Two Messages**

- Each address assigned to the client has associated preferred and valid lifetimes specified by the server.
- To request an extension of the lifetimes assigned to an address, the client sends a Renew message to the server.
- The server sends a Reply message to the client with the new lifetimes, allowing the client to continue to use the address without interruption.

(5) DHCP for IPv6

Client-server Exchanges Involving **Four Messages**

I. The client sends a Solicit message to the **All_DHCP_Relay_Agents_and_Servers** address to find available DHCP servers.

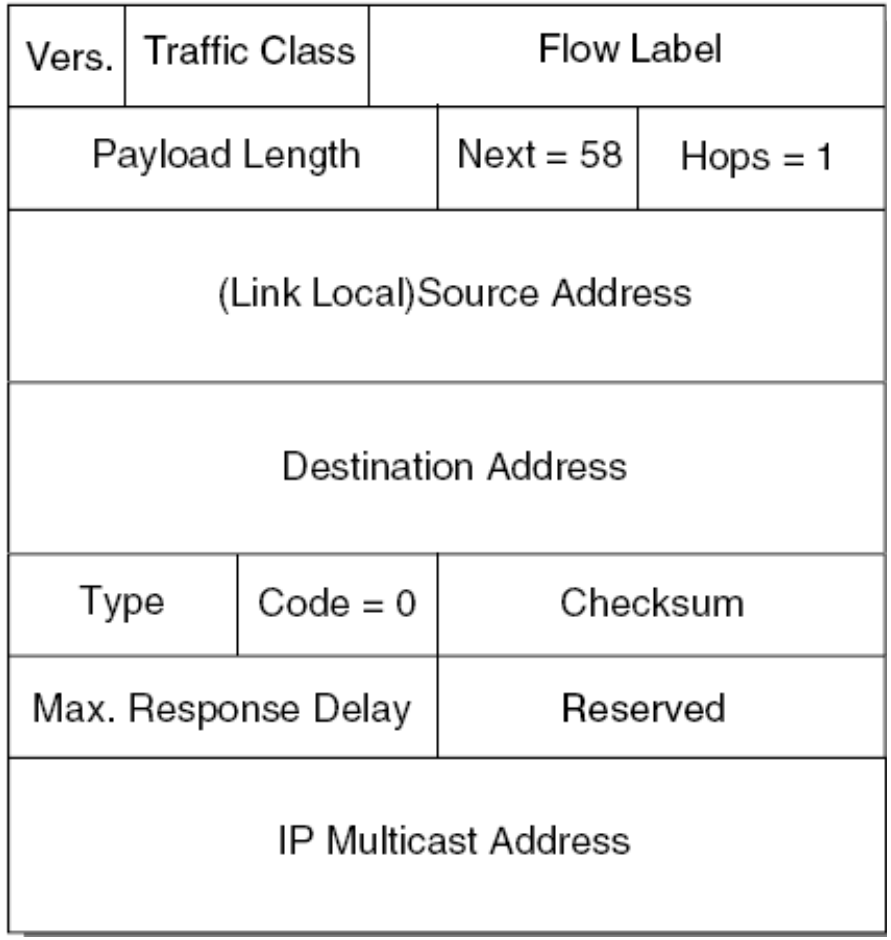
II. Any server that can meet the client's requirements responds with an Advertise message.

III. The client then chooses one of the servers and sends a Request message to the server asking for confirmed assignment of addresses and other configuration information.

IV. The server responds with a Reply message that contains the confirmed addresses and configuration.

(6) Multicast Listener Discovery (MLD)

- **RFC2710**：Multicast Listener Discovery (MLD) for IPv6
- Used by a router to discover the members of a particular multicast group.
- Provides the equivalent function of IGMP for IPv4
- There are three types of MLD message



(6) Multicast Listener Discovery (MLD)

- Multicast Listener Query
  - General query Used to find which multicast addresses are being listened for on a link.
  - Multicast-address-specific queryUsed to find if any nodes are listening for a specific multicast address on a link.
- Multicast listener report
  - Used by a node to report that it is listening to a multicast address.
- Multicast listener done
  - Used by a node to report that it is ceasing to listen to a multicast address.

(6) Multicast Listener Discovery (MLD)

- A router periodically sends a General Query on each of its links to the all nodes link-local address (FF02::1).
- When a node listening for any multicast addresses receives this query, it sets a delay timer(between 0 and maximum response delay) for each multicast address for which it is listening.
- As each timer expires, the node sends a *multicast listener report* message containing the appropriate multicast address.
- If a node receives another node's report for a multicast address while it has a timer still running for that address, then it stops its timer and does not send a report for that address.

(6) Multicast Listener Discovery (MLD)

- The router manages a list of, and sets a timer for, each multicast address it is aware of on each of its links.
- If one of these timers expires without a report being received for that address, the router assumes that no nodes are still listening for that address, and the address is removed from the list.
- Whenever a report *is* received, the router resets the timer for that particular address.

(6) Multicast Listener Discovery (MLD)

- When a node has finished listening to a multicast address,
  - if it was the last node on a link to send a report to the router then it sends a *multicast listener done* message to the router.
  - Else If the node *was* interrupted by another node before its timer expired, then it assumes that other nodes are still listening to the multicast address on the link and therefore does not send a done message.
- When a router receives a done message, it sends a multicast-address-specific message on the link.

5. Internet transition - Migrating from IPv4 to IPv6

I. RFC4213：Basic Transition Mechanisms for IPv6 Hosts and Routers

II. RFC2893： Transition Mechanisms for IPv6 Hosts and Routers

III. RFC2185：Routing Aspects Of IPv6 Transition

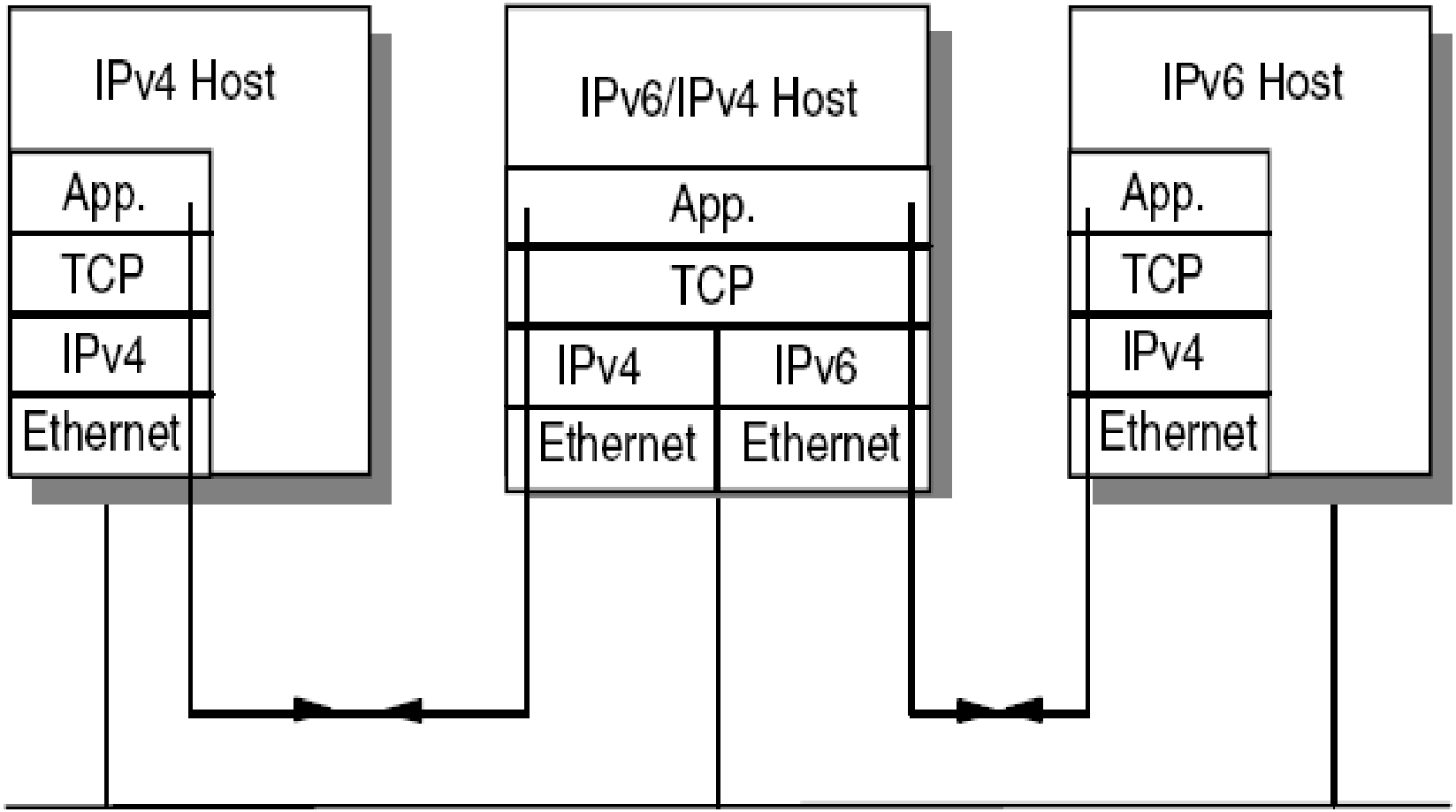
Internet transition - Migrating from IPv4 to IPv6

- If the Internet is to realize the benefits of IPv6, then a period of transition will be necessary when new IPv6 hosts and routers deployed alongside existing IPv4 systems.
- Define a number of mechanisms to be employed to ensure both compatibility between old and new systems and a gradual transition that does not impact the functionality of the Internet.

Internet transition - Migrating from IPv4 to IPv6

- The transition employs the following techniques:
  - Dual-stack IP implementations for hosts and routers that must interoperate between IPv4 and IPv6.
  - Imbedding of IPv4 addresses in IPv6 addresses. IPv6 hosts will be assigned addresses that are interoperable with IPv4, and IPv4 host addresses will be mapped to IPv6.
  - IPv6-over-IPv4 tunneling mechanisms for carrying IPv6 packets across IPv4 router networks.
  - IPv4/IPv6 header translation.This technique is intended for use when implementation of IPv6 is well advanced and only a few IPv4-only systems remain.

Dual IP stack implementation



Dual IP stack implementation

- An IPv6/IPv4 node can send and receive either IPv6 packets or IPv4 datagrams, depending on the type of system with which it is communicating.
- The node will have both a 128-bit IPv6 address and a 32-bit IPv4 address, which do not necessarily need to be related.

Dual IP stack implementation

- When an IPv6/IPv4 node wishes to communicate with another system, it needs to know the capabilities of that system and which type of packet it should send.
- The records found in the DNS for a node depend on which protocols it is running:
  - IPv4-only nodes only have **A** records containing IPv4 addresses in the DNS.
  - IPv6/IPv4 nodes that can interoperate with IPv4-only nodes have **AAAA** records containing IPv4-compatible IPv6 addresses and A records containing the equivalent IPv4 addresses.
  - IPv6-only nodes that cannot interoperate with IPv4-only nodes have only **AAAA** records containing IPv6 addresses.

Dual IP stack implementation

- Because IPv6/IPv4 nodes make decisions about which protocols to use based on the information returned by the DNS, the incorporation of AAAA records in the DNS is a prerequisite to interoperability between IPv6 and IPv4 systems.
- Name servers do not necessarily need to use an IPv6-capable protocol stack, but they must support the additional record type.

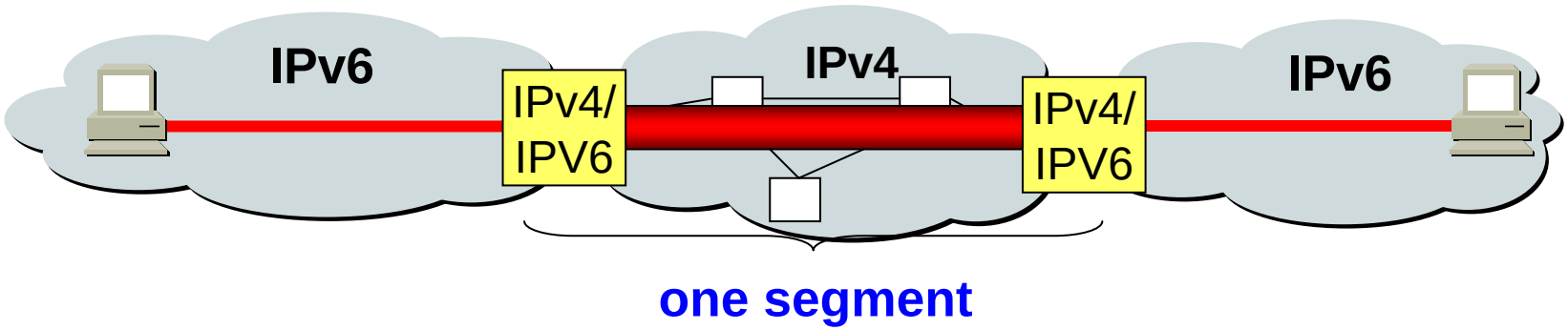
Common Tunneling Mechanisms

- The IPv6 routing infrastructure will be built up over time.
- The existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic.
- Tunneling provides a way to utilize an existing IPv4 routing infrastructure to carry IPv6 traffic.
- IPv6/IPv4 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets.

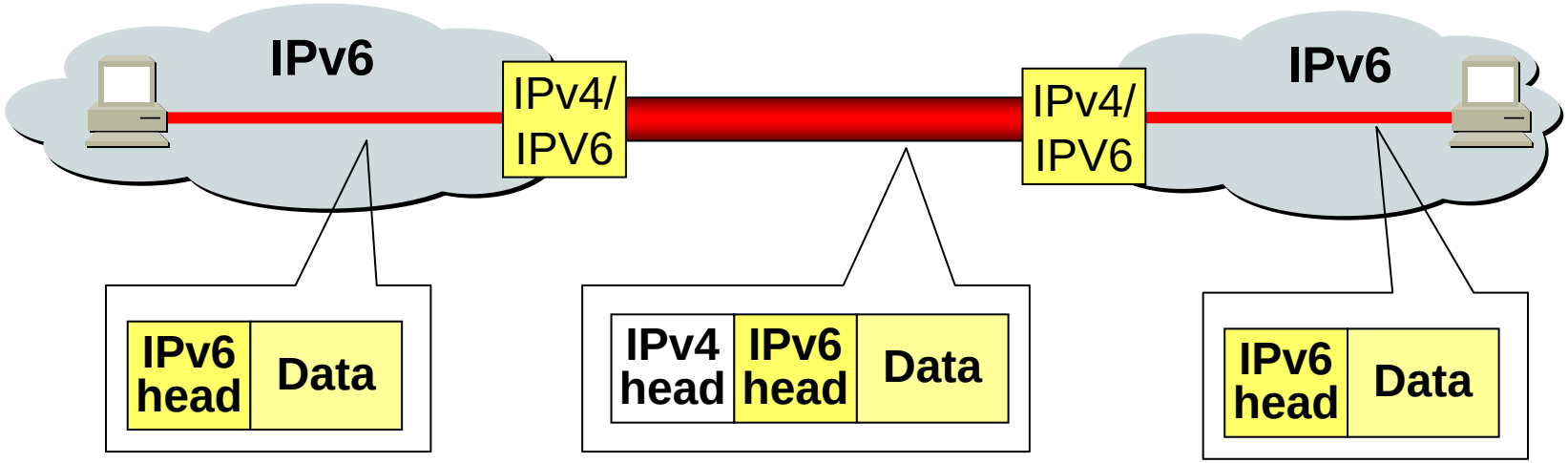
Common Tunneling Mechanisms

Tunneling can be used in a variety of ways:

- Router-to-Router
  - IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves.
  - In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes.

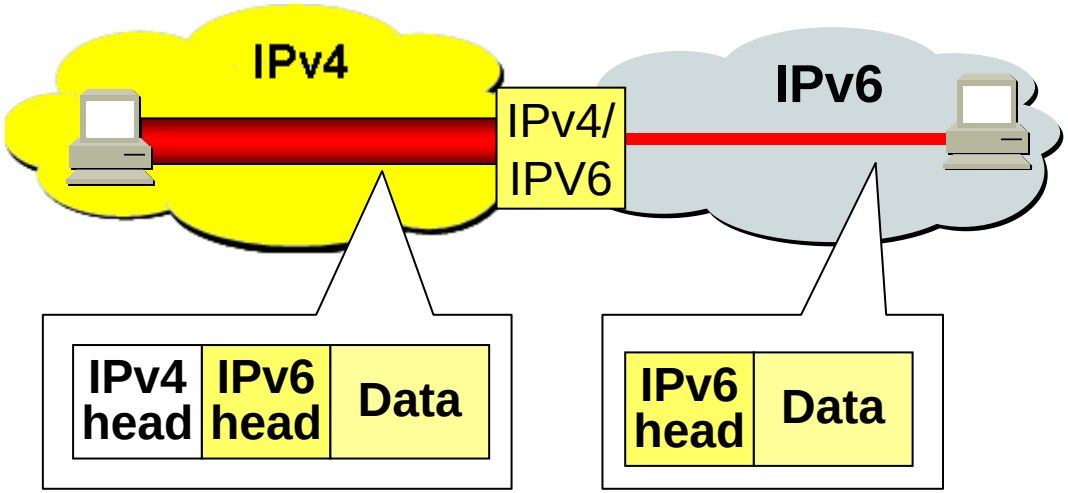


Common Tunneling Mechanisms



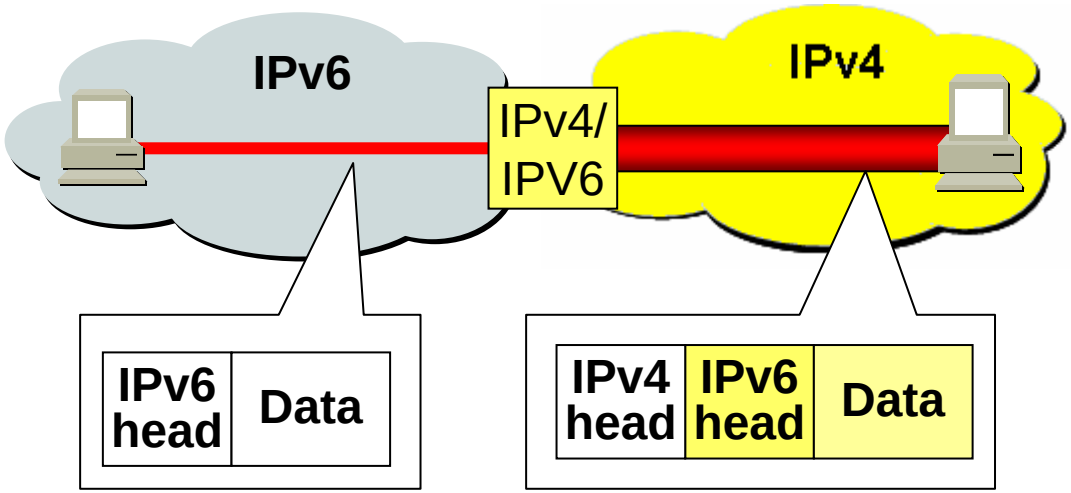
Common Tunneling Mechanisms

- Host-to-Router
  - IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that is reachable via an IPv4 infrastructure.
  - This type of tunnel spans the first segment of the packet's end-to-end path.



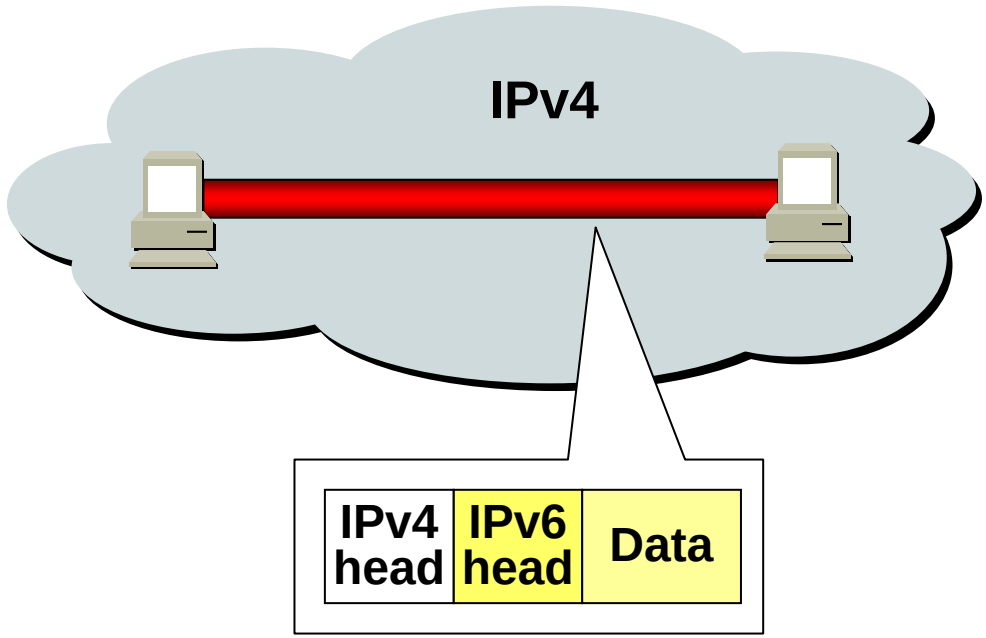
Common Tunneling Mechanisms

- Router-to-Host
  - IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 host.
  - This tunnel spans only the **last segment** of the end-to-end path.

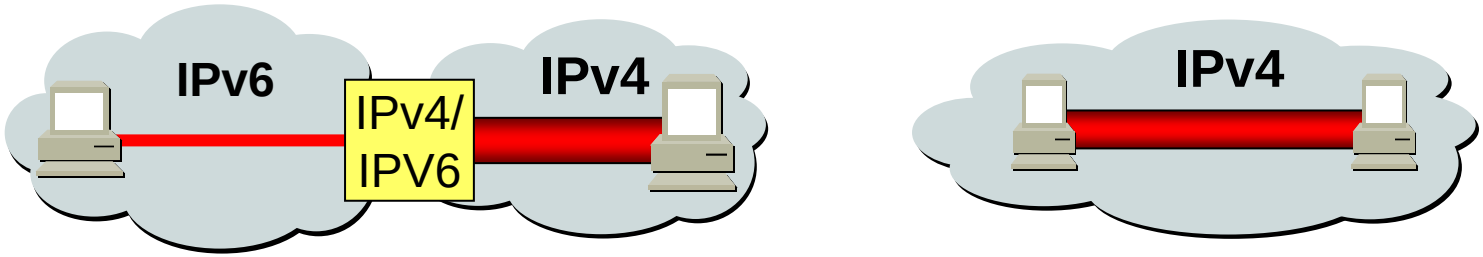


Common Tunneling Mechanisms

- Host-to-Host
  - IPv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves.
  - In this case, the tunnel spans the entire end-to-end path that the packet takes.



Automatic Tunneling

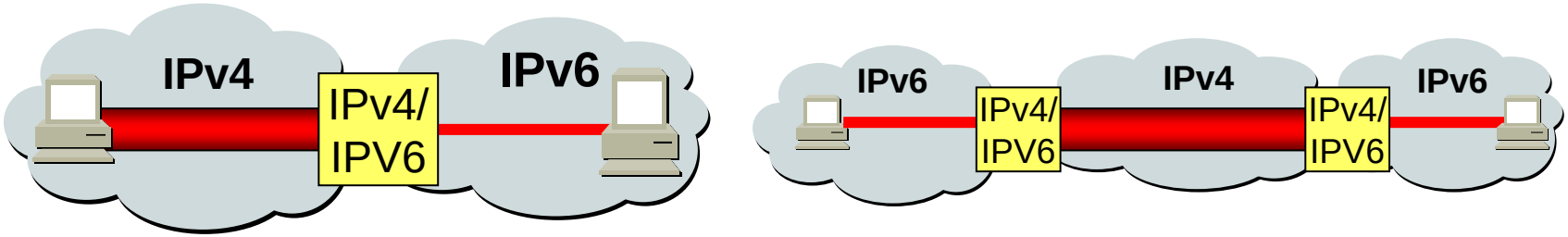


- In Router-to-Host and Host-to-Host situation the destination host's IPv6 address is known.
- The destination has a IPv4 compatible IPv6 address.
- The tunnel endpoint address is determined automatically from the packet being tunneled (the destination has a IPv4-compatible IPv6 address.).
- This is called **automatic tunneling**.

96-bits	32-bits
0:0:0:0:0:0	IPv4 Address

IPv4-Compatible IPv6 Address Format

Configured Tunneling



- In configured tunneling, the tunnel endpoint address is determined from configuration information in the encapsulating node.
- For each tunnel, the encapsulating node must store the tunnel endpoint address.
- When an IPv6 packet is transmitted over a tunnel, the tunnel endpoint address configured for that tunnel is used as the destination address for the encapsulating IPv4 header.

Configured Tunneling

- IPv6/IPv4 hosts that are connected to datalinks with no IPv6 routers MAY use a configured tunnel to reach an IPv6 router.
- If the IPv4 address of an IPv6/IPv4 router bordering the IPv6 backbone is known, this can be used as the tunnel endpoint address.
- This tunnel can be configured into the routing table as an IPv6 "default route".
- That is, all IPv6 destination addresses will match the route and could potentially traverse the tunnel.
- Since the "mask length" of such a default route is zero, it will be used only if there are no other routes with a longer mask that match the destination.

References of Internet transition - Migrating from IPv4 to IPv6

I. RFC4213：Basic Transition Mechanisms for IPv6 Hosts and Routers

II. RFC2893： Transition Mechanisms for IPv6 Hosts and Routers

III. RFC2185：Routing Aspects Of IPv6 Transition

IV. Silvaco Gai, Internetworking IPv6 with Cisco Routers, McGraw-Hill, 1998. (**IPv6** 网络互联与**Cisco**路由器，机械工业出版社，**1999**。)

Exercises

- 18.11
- 18.12
- 8.13*
- 18.16