Lecture 17

IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4).

Unicast: An identifier for a single interface. A packet sent a unicast address is delivered to the interface identified by that address.

Anycast: IP Version 6 (IPv6) defines a new type of address, known as an "anycast" address, that allows a packet to be routed to one of a number of different nodes all responding to the same address. The anycast address may be assigned to one or more network interfaces (typically on different nodes), with the network delivering each packet addressed to this address to the "nearest" interface based on the notion of "distance" determined by the routing protocols in use.

The uses of anycast addresses are still evolving, but such addresses offer the potential for a number of important services.

1. For example, an anycast address may be used to allow nodes to access one of a collection of servers providing a well-known service, without manual configuration in each node of the list of servers;

2. An anycast address may be used in a source route to force routing through a specific internet service provider, without limiting routing to a single specific router providing access to that ISP.

Multicast: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

There are no broadcast addresses in IPv6, their function being superseded by multicast addresses.

The changes from IPv4 to IPv6 fall primarily into the following categories:

Expanded Addressing Capabilities

IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. And a new type of address called an "anycast address" is defined, used to send a packet to any one of a group of nodes.

Header Format Simplification

Some of the IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.

Improved Support for Extensions and Options

Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

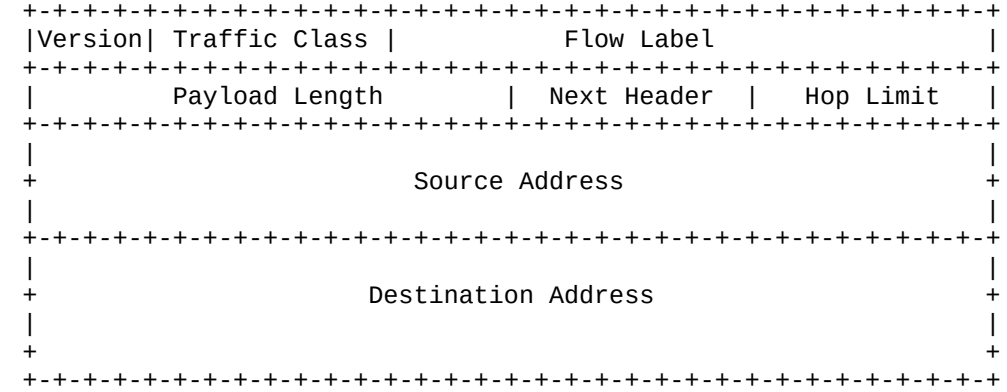
Flow Labeling Capability
A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.

Authentication and Privacy Capabilities
Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6.

Terminology

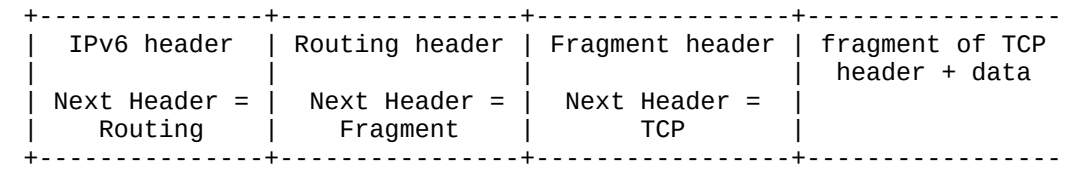
node	- a device that implements IPv6.
router	- a node that forwards IPv6 packets not explicitly addressed to itself.
host	- any node that is not a router.
upper layer	- a protocol layer immediately above IPv6. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF.
link	- a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6. Examples are Ethernets
neighbors	- nodes attached to the same link.
interface	- a node's attachment to a link.
address	- an IPv6-layer identifier for an interface or a set of interfaces.
packet	- an IPv6 header plus payload.
link MTU	- the maximum transmission unit, i.e., maximum packet size in octets, that can be conveyed over a link.
path MTU	- the minimum link MTU of all the links in a path between a source node and a destination node.

IPv6 Header Format



Version	4-bit Internet Protocol version number = 6.
Traffic Class	8-bit traffic class field. See section 7.
Flow Label	20-bit flow label. See section 6.
Payload Length	16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header this IPv6 header, in octets. (Note that any of the extension headers present are considered part of the payload, i.e., included in the length count.
Next Header	8-bit selector. Identifies the type of header immediately following the IPv6 header.
Hop Limit	8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.
Source Address	128-bit address of the originator of the packet.
Destination Address	128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

In IPv6, optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. As illustrated in these examples, an IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the preceding header as shown below.



When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order:

IPv6 header
Hop-by-Hop Options header
Destination Options header
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Upper-layer header (here TCP header)

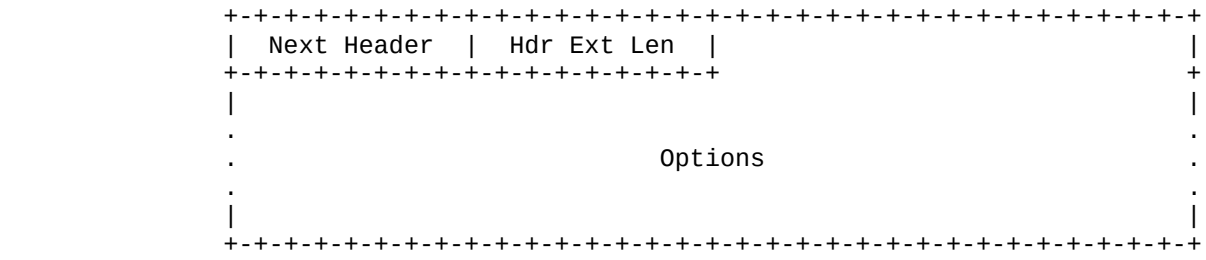
as shown in figure below

Figure 15.10 Page 553 Stalling

Each extension header should occur at most once, except for the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer header).

Hop-by-Hop Options Header

The Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet's delivery path. The Hop-by-Hop Options header is identified by a Next Header value of 0 in the IPv6 header, and has the following format:



Next Header is of 8-bit size. It identifies the type of header immediately following the Hop-by-Hop Options header.

Hdr Ext Len is 8-bit unsigned integer. Length of the Hop-by-Hop options header in 8-octet units.

Options is a variable length field consisting of one or more option definitions. Each definition is the form of three subfields.

- Option Type (8 bits) - which identifies the option
- Length (8 bits) - which specifies the length of option Data field in octets
- Option Data- which is a variable length specification of the option

The Option Type identifiers are internally encoded such that their highest-order two bits specify the action that must be taken if the processing IPv6 node does not recognize the Option Type:

00 - skip over this option and continue processing the header.

01 - discard the packet.

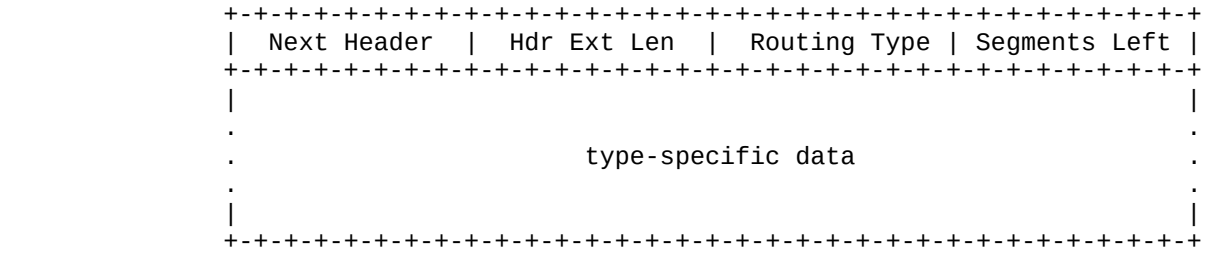
10 - discard the packet and, regardless of whether or not the packet's Destination Address was a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

11 - discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address pointing to the unrecognized Option Type.

The third-highest-order bit of the Option Type specifies whether or not the Option Data of that option can change en-route to the packet's final destination.

Routing Header

The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. This function is very similar to IPv4's Loose Source and Record Route option. The Routing header is identified by a Next Header value of 43 in the immediately preceding header, and has the following format:



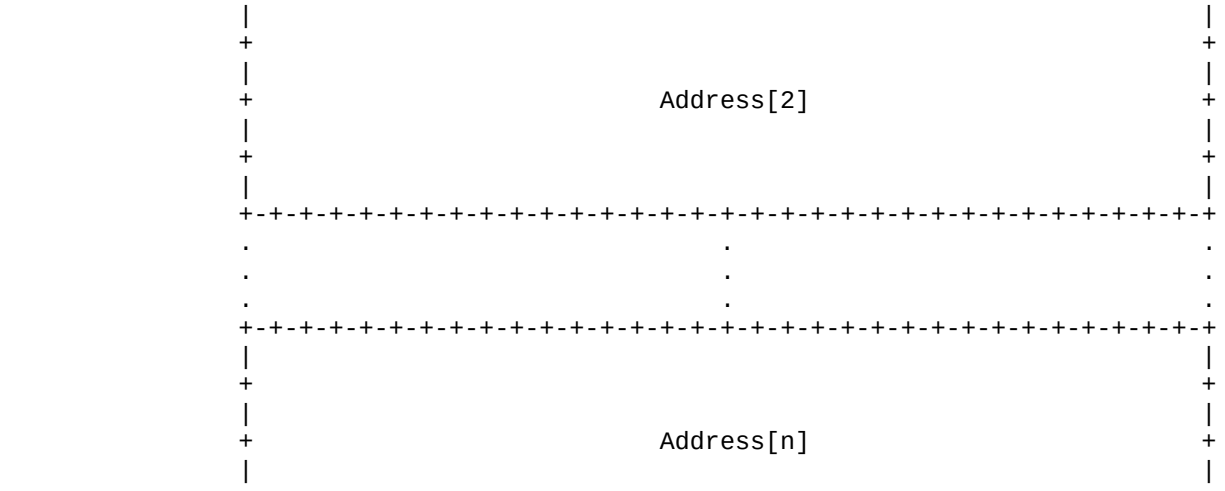
Next Header: It is 8-bit selector. It identifies the type of header immediately following the Routing header.

Hdr Ext Len: It is 8-bit unsigned integer. The Length of the Routing header in 8-octet units, not including the first 8 octets.

Routing Type: It is 8-bit identifier of a particular Routing header variant.

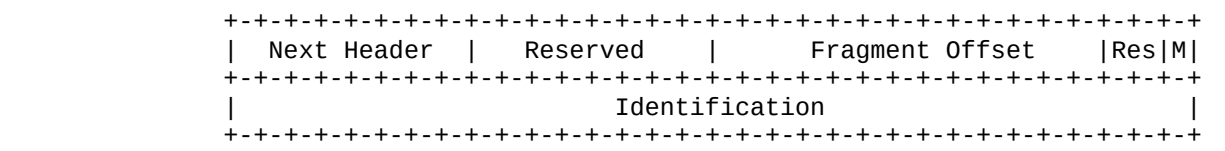
Segments Left: It is 8-bit unsigned integer specifying number of route segments remaining, i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination.

The Type 0 Routing header has the following format:



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. (Note: unlike IPv4, fragmentation in IPv6 is performed only by source nodes). The Fragment header is identified by a Next Header value of 44 in the immediately preceding header, and has the following format:



Next Header: It is 8-bit selector. It identifies the type of header immediately following this header.

Reserved: It is 8-bit reserved field, which is initialized to zero for transmission and ignored on reception.

Fragment Offset: It is 13-bit unsigned integer. It indicates where in the original packet, the payload of this fragment belongs.

Res: It is 2-bit reserved field, which is initialized to zero for transmission and ignored on reception.

M flag 1 = more fragments; 0 = last fragment.

Identification: It is a 32 bit field that uniquely identifies the original packet.

In order to send a packet that is too large to fit in the MTU of the path to its destination, a source node may divide the packet into fragments and send each fragment as a separate packet, to be reassembled at the receiver.

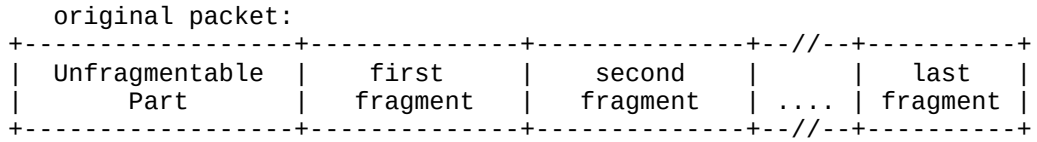
For every packet that is to be fragmented, the source node generates an Identification value. The Identification must be different than that of any other fragmented packet sent recently* with the same Source Address and Destination Address.

Original packet:

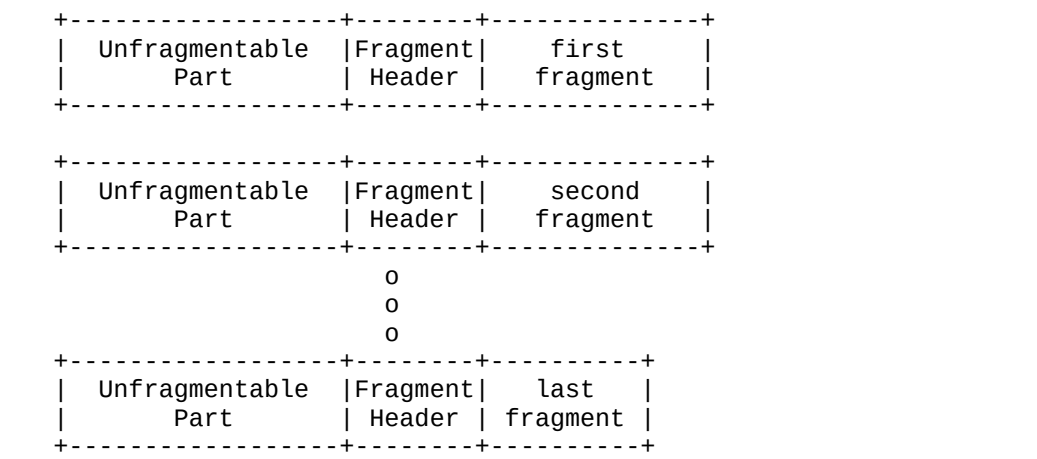
The Unfragmentable Part consists of the IPv6 header plus any extension headers that must be processed by nodes en route to the destination, that is, all headers up to and including the Routing header if present, else the Hop-by-Hop Options header if present, else no extension headers.

The Fragmentable Part consists of the rest of the packet, that is, any extension headers that need be processed only by the final destination node(s), plus the upper-layer header and data.

The Fragmentable Part of the original packet is divided into fragments. The fragments are transmitted in separate "fragment packets" as illustrated:

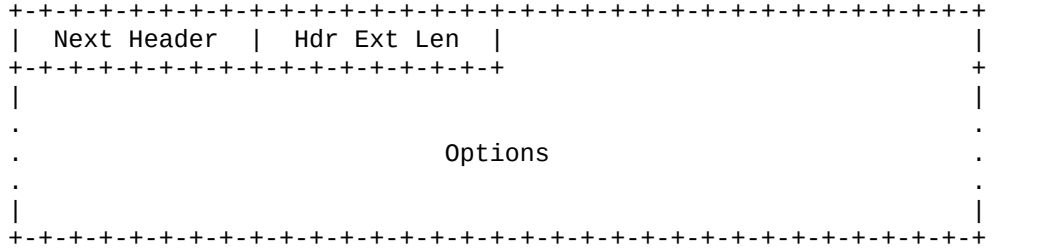


fragment packets:



Destination Options Header

The Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s). The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header, and has the following format.



Next Header: It is 8-bit selector. It identifies the type of header immediately following the Destination Options header.

Hdr Ext Len: It is 8-bit unsigned integer. It contains the length of the Destination Options header in 8-octet units, not including the first 8 octets.

No Next Header

The value 59 in the Next Header field of an IPv6 header or any extension header indicates that there is nothing following that header. If the Payload Length field of the IPv6 header indicates the presence of octets past the end of a header whose Next Header field contains 59, those octets must be ignored, and passed on unchanged if the packet is forwarded.

Flow Labels

The 20-bit Flow Label field in the IPv6 header may be used by a source to label sequences of packets for which it requests special handling by the IPv6 routers, such as non-default quality of service or "real-time" service.

Traffic Classes

The 8-bit Traffic Class field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.