Introduction to IPv6

IP v 1-3: defined and replaced

IP v4 - current version; 20+ years old

IP v5 - streams protocol

IP v6 - replacement for IP v4

During developments it was called IPng - Next Generation

Why Change IP?

32 bit Address space exhaustion

32 bit address space = millions of networks (could be enough?), BUT:

Two level addressing (network and host) wastes space: one network address used, even if not all possible associated hosts connected to Internet, or network connected to Internet

Growth of networks and the Internet (LANs, wireless LANs …)

2^{14} Class B network addresses already almost exhausted; class C networks too low size for most companies

Extended use of TCP/IP (new applications => requests for new IP addresses)

- Requirements for new types of services
  - Different applications have different requirements for delivery, reliability and speed
  - Current IP has *type of service* that's not often implemented
- Multicast transmissions

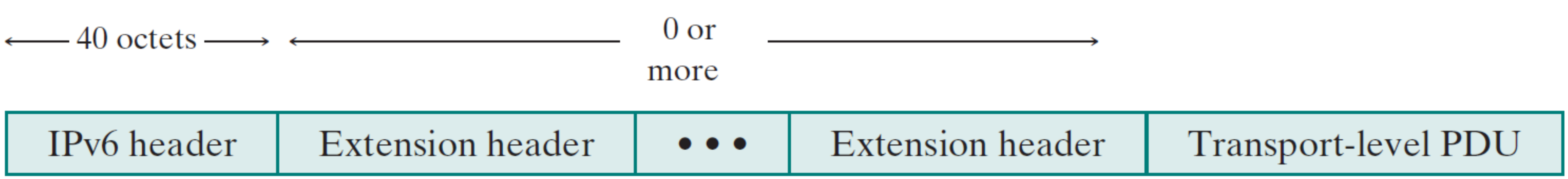
IPv6 RFCs

1752 - Recommendations for the IP Next Generation Protocol

2460 - Overall specification

4291 - addressing structure

….. Others



Enhancements over IPv4

Expanded address space: 128 bit

Improved option mechanism

- Separate optional headers between IPv6 header and Transport layer header
- Most are not examined by intermediate routers
  - Improved speed and simplified router processing of IPv6 datagrams
  - Easier to extend options

Address auto-configuration

- Dynamic assignment of addresses

Increased address flexibility & scalability

  - Anycast address : packet delivered to a set of hosts

Support for resource allocation

  - Allow packet labeling (those belonging to a traffic flow)

General considerations no broadcast, instead replaced with multicast

Not generally compatible with IPv4

- But compatible with higher-level protocols

Longer addresses: expanded address space, 128 bit

Address auto-configuration; dynamic assignment of addresses

Traffic Priorities: 0 – 7 for variable flow rate, 8 – 15 for real time traffic

Improved option mechanism

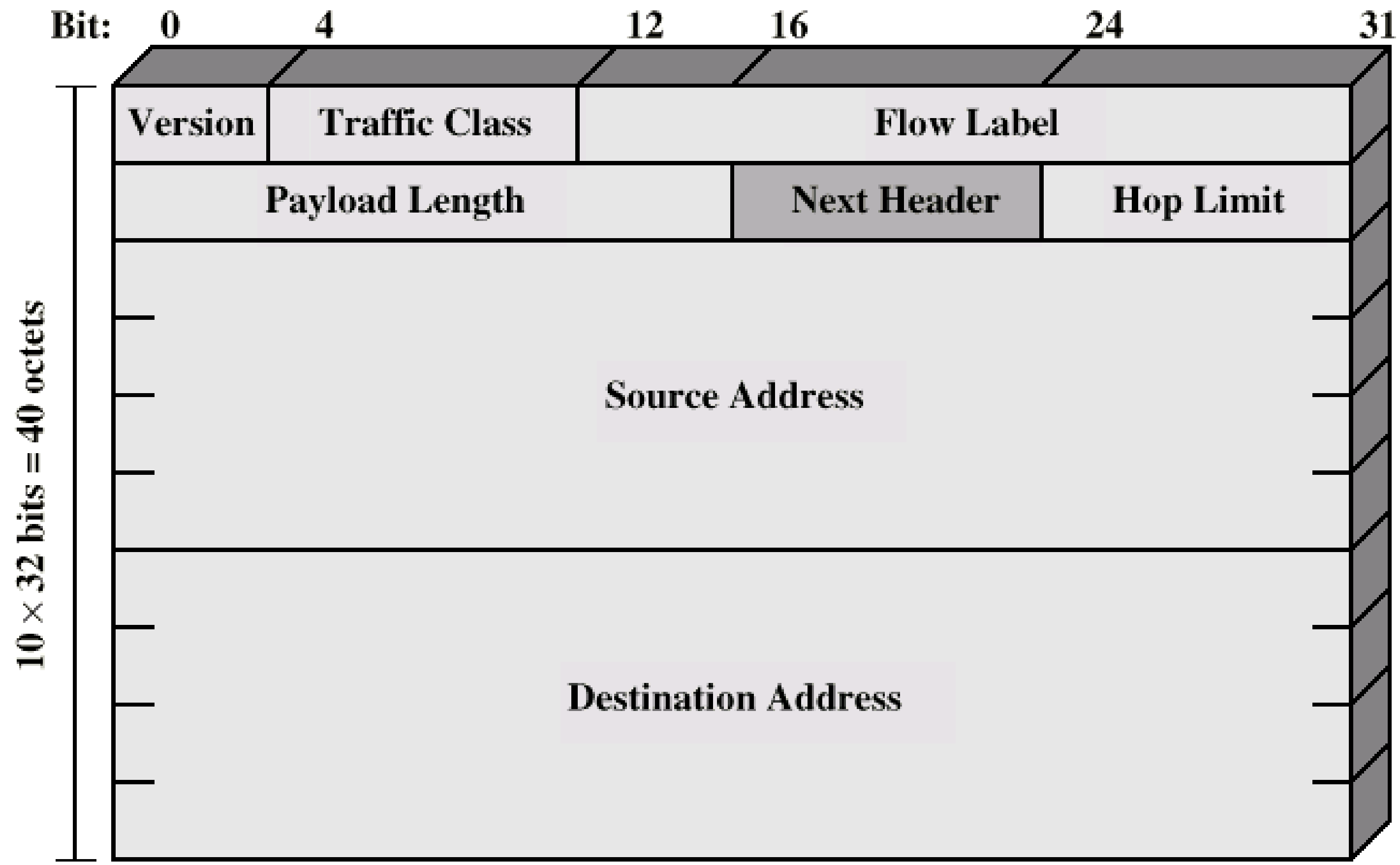
- Separate optional headers between IPv6 header and transport layer header
- Most are not examined by intermediate routers
  - Improved speed and simplified router processing
  - Easier to extend options

Increased addressing flexibility

- Anycast - delivered to one of a set of nodes
- Improved scalability of multicast addresses

- Support for resource allocation
    - Replaces *type of service* IPv4 field (most unused)
    - Labeling of packets to particular traffic flow
    - Allows special handling, e.g. real time video

IPv6 Header General format



IPv6 base header format

Contains less information than IPv4 header; header format - entirely different

Next Header field points to first extension header

Flow Label field used to associate datagrams belonging to a *flow* or communication between two applications (support for audio-video connections, with appropriate QoS)

Traffic class

Classes or priorities of current packet

Still under development, see RFC 2460

Advantages of the header structure

Efficiency - header only as large as necessary

Flexibility & extension - can add new headers for new features

Incremental development - can add processing for new features to testbed; other routers will skip those headers

Extension Headers

Additional information stored in optional extension headers, followed by data

Hop-by-Hop Options

Require processing at each router

Routing

Similar to IPv4 source routing

Fragment

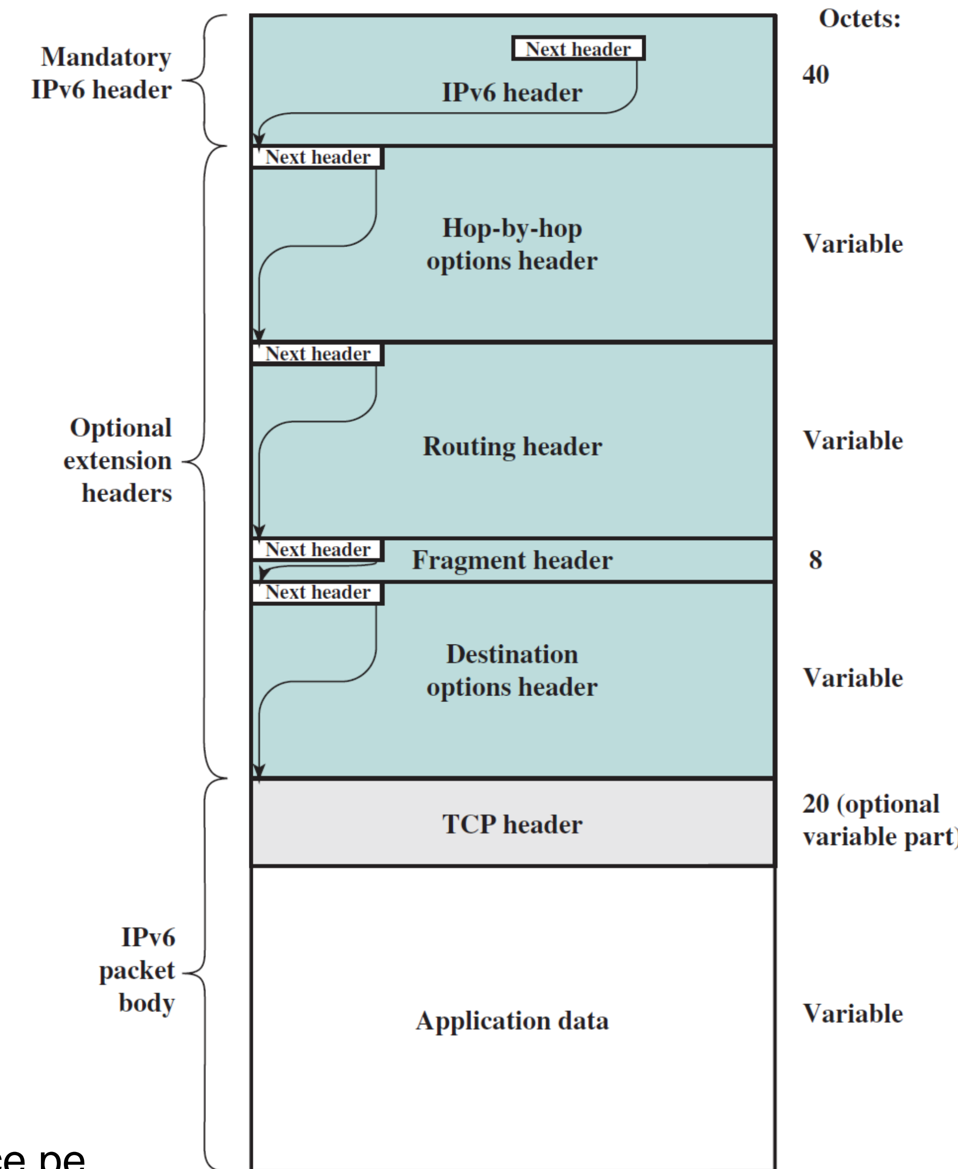
Authentication

Encapsulating security payload

Destination options

For destination node

fragmentarea se face doar de la sursa, nu pot face pe parcurs, deoarece la sfarsit se reasambleaza pachetele



IPv6 Packet with Extension Headers

IP v6 Header Fields (Basic Header)

Version: 6

Traffic Class (DS/ECN)

Classes or priorities of packets

Used by originating nodes and/or forwarding routers for differentiated services and congestion functions

Flow Label

Used by routers to label packets requesting special handling within the network

Payload length

Includes all extension headers plus user (application) data

Next Header

Identifies type of header immediate following

May have another extension header or next layer up protocol header

Source Address & Destination address (128 bits)

IPv6 Addresses

128 bits long

Assigned to node's interface, not to node

One single interface may have multiple unique unicast addresses

Three types of address:

Unicast

Single interface; packet delivered there

Anycast

Set of interfaces (typically belong to different nodes)

Delivered to any **one** interface, usual the "nearest"

Multicast

Packets delivered to all interfaces identified

Prefix (binary)	Usage	Fraction
0000 0000	Reserved (including IPv4)	1/256
0000 0001	Unassigned	1/256
0000 001	OSI NSAP addresses	1/128
0000 010	Novell NetWare IPX addresses	1/128
0000 011	Unassigned	1/128
0000 1	Unassigned	1/32
0001	Unassigned	1/16
001	Unassigned	1/8
010	Provider-based addresses	1/8
011	Unassigned	1/8
100	Geographic-based addresses	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1/16
1111 0	Unassigned	1/32
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
1111 1110 0	Unassigned	1/512
1111 1110 10	Link local use addresses	1/1024
1111 1110 11	Site local use addresses	1/1024
1111 1111	Multicast	1/256

IPv6 addresses

Address Type	Description
Unicast	One to One (Global, Link local, Site local) + An address destined for a single interface.
Multicast	One to Many + An address for a set of interfaces + Delivered to a group of interfaces identified by that address. + Replaces IPv4 “broadcast”
Anycast	One to Nearest (Allocated from Unicast) + Delivered to the closest interface as determined by the IGP

PREFIX	**Interface ID**

IPv6 Address Space Usage

Address Type	Binary Prefix	IPv6 Notation	Fraction of Address Space
Embedded IPv4 address	00…1111 1111 1111 1111 (96 bits)	::FFFF/96	2^{-96}
Loopback	00…1 (128 bits)	::1/128	2^{-128}
Link-local unicast	1111 1110 10	FE80::/10	1/1024
Multicast	1111 1111	FF00::/8	2/256
Global unicast	Everything else		

IPv6 addresses format:

•128-bit addresses, may use dotted decimal representation; requires 16 numbers

105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

•Groups of 16-bit numbers in hex, separated by colons - *colon hexadecimal* (or *colon hex*) representation (not case sensitive)

69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF

•Zero-compression - series of zeroes indicated by two colons

FF0C:0:0:0:0:0:0:B1 is equivalent with: FF0C::B1

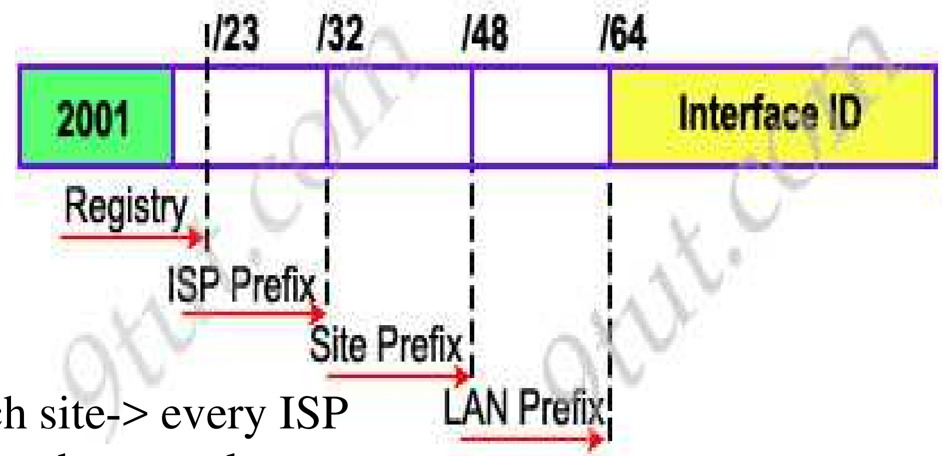
But once in an address

•IPv6 address with 96 leading zeros is interpreted to hold an IPv4 address

•Use of " / " notation to denote number of bits in address represent the subnet (prefix); rest of them represent interface ID);

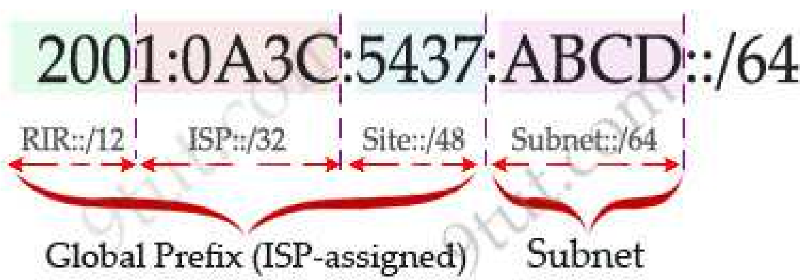
- /64 is common prefix length

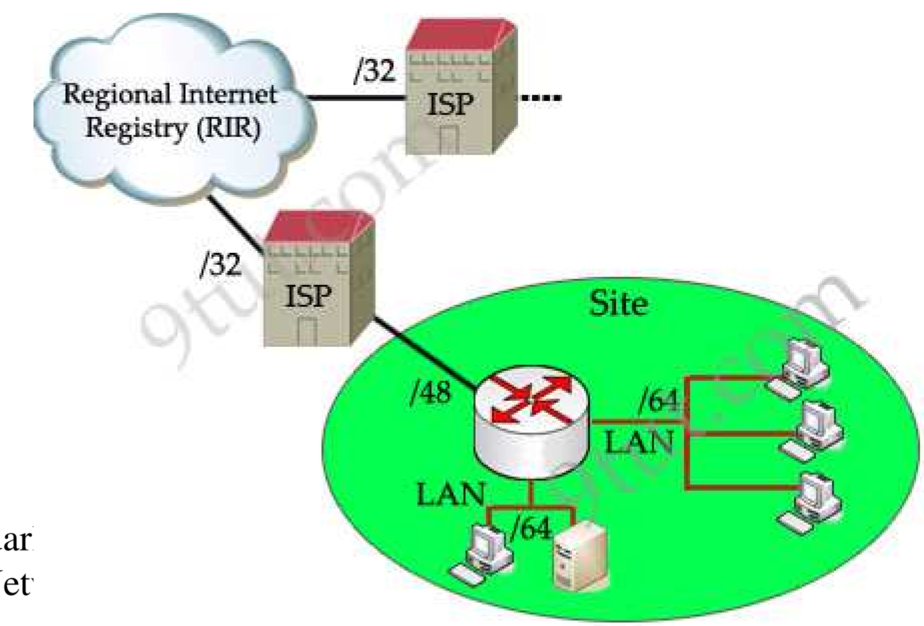
ICANN assigns a range of IP addresses to Regional Internet Registry (RIR) organizations. The size of address range assigned to the RIR may vary but with a minimum prefix of /12 and belong to the following range: 2000::/12 to 200F:FFFF:FFFF:FFFF::/64.



Each ISP receives a /32 and provides a /48 for each site-> every ISP can provide $2^{(48-32)}$ = 65,536 site addresses (note: each network organized by a single entity is often called a site).
Each site provides /64 for each LAN -> each site can provide $2^{(64-48)}$ = 65,536 LAN addresses for use in their private networks.
So each LAN can provide 2^{64} interface addresses for hosts.

EXAMPLE:





IPv6 Address Scopes	*Description*
Link-local address	+ only used for communications within the local subnetwork (automatic address configuration, neighbor discovery, router discovery, and by many routing protocols). Only valid on the current subnet. + routers do not forward packets with link-local addresses. + are allocated with the FE80::/64 prefix -> can be easily recognized by the prefix FE80. + is usually created dynamically using a link-local prefix of FE80::/10 and a 64-bit interface identifier (based on 48-bit MAC address).
Global unicast address	+ unicast packets sent through the public Internet + globally unique throughout the Internet + starts with a 2000::/3 prefix (this means any address beginning with 2 or 3). But in the future global unicast address might not have this limitation
Site-local address	+ allows devices in the same organization, or site, to exchange data. + starts with the prefix FEC0::/10. They are analogous to IPv4′s private address classes.

PREFIX	**Interface ID**

Options Headers

Carry optional information, not necessary examined by all routers or hosts

Hop-by-Hop Options Header

Consists of the following:

- *Next header*
- *Header extension length*
- *Options*
  - One or more option definitions
  - Options definition contains the following sub-fields:
    - *Option Type* – identifies option
    - *Length* – length in octets of the option's data field
    - *Option Data* – option specification

Examples for such options:

Jumbo payload option

Over 2^{16} = 65,535 octets in an IPv6 packet

Router alert option

Tells the router that the contents of this packet is of interest to the router (to handle data accordingly)

Provides support for RSVP (Reservation Protocol), used in multimedia transmissions, for flow control

Fragmentation Header

Fragmentation only allowed at source node, no fragmentation at intermediate routers

Node must perform path discovery operation, to find the smallest MTU (Maximum Transmission Unit) of intermediate networks

Source fragments IPv6 packets to match MTU

Otherwise limits to 1280 octets, that must be supported by any network

Fragmentation Header Fields:

Next Header – type of following header

Reserved

Fragmentation offset – any fragment data is multiple of 64bits; this field indicates where in the original packet this fragment's payload belongs

Reserved

More flag – more fragments or last fragment

Identification – identify the original packet (now fragmented)

Routing Header

List of one or more intermediate nodes to be visited

Structure (see next):

Next Header

Header extension length – length of this header

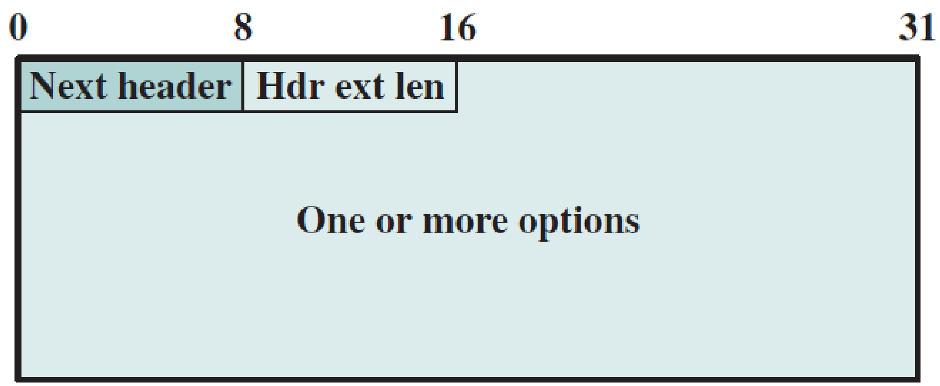
Routing type – identifies a routing protocol header variant

Segments left - number of nodes still to be visited

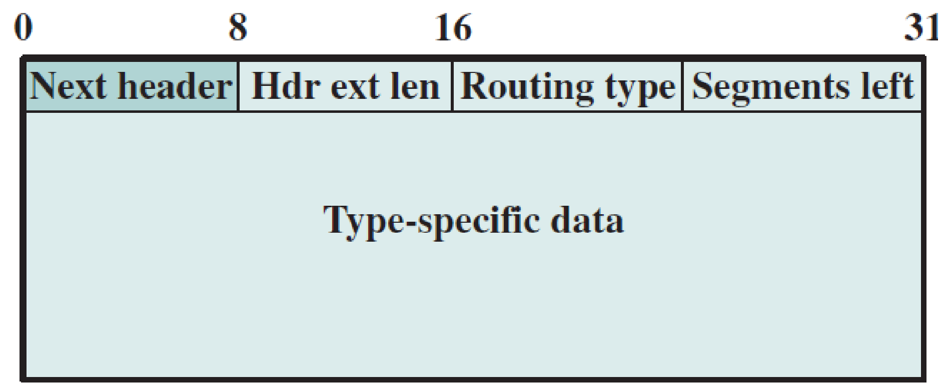
Destination Options Header

Information examined by the destination node

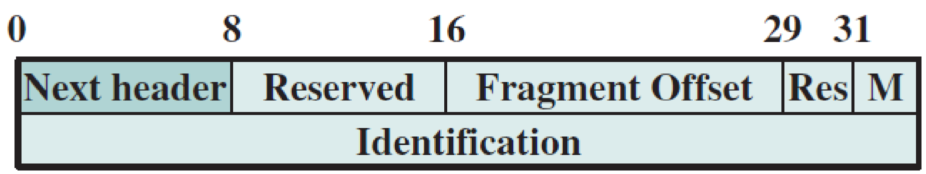
Same format as Hop-by-Hop options header



(a) Hop-by-Hop Options header;
Destination Options header



(c) Generic Routing header

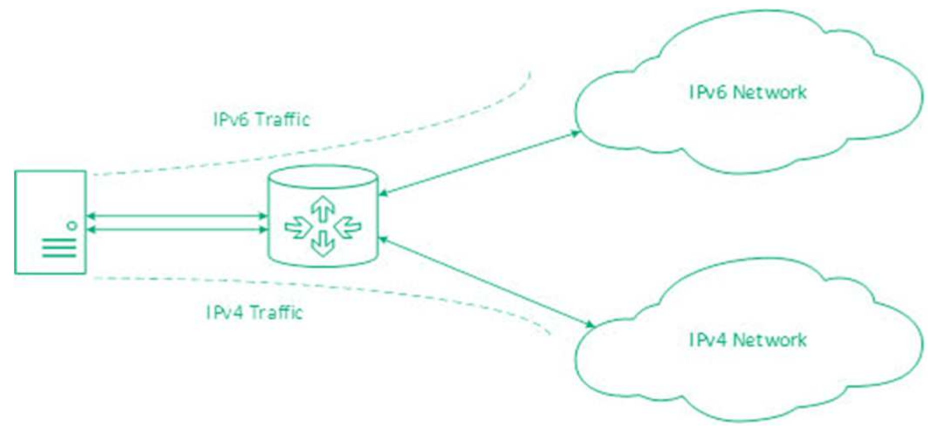


(b) Fragment header

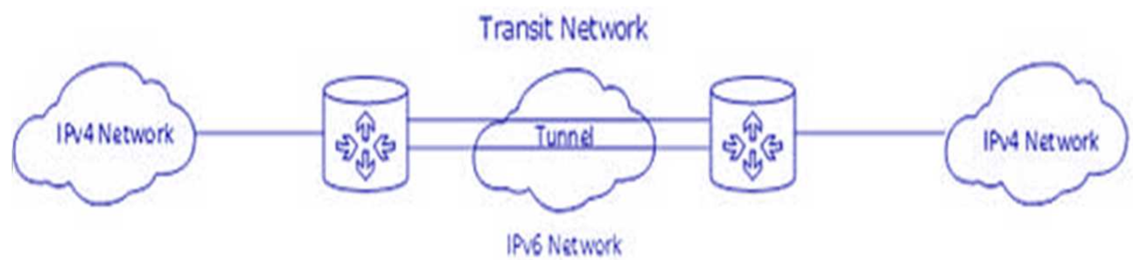
IPv6 Extension Headers

Technologies can be used in transition from IPv4 to IPv6

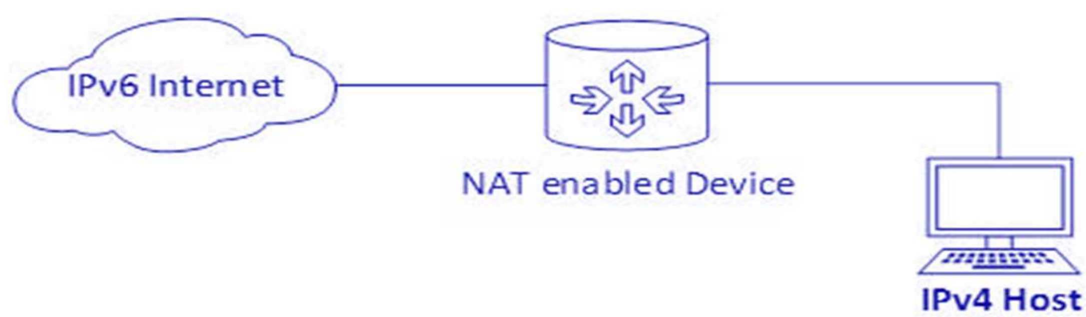
Dual Stack Routers



Tunneling



NAT Protocol Translation



Multicasting

Addresses that refer to group of hosts on one or more networks

Used in:

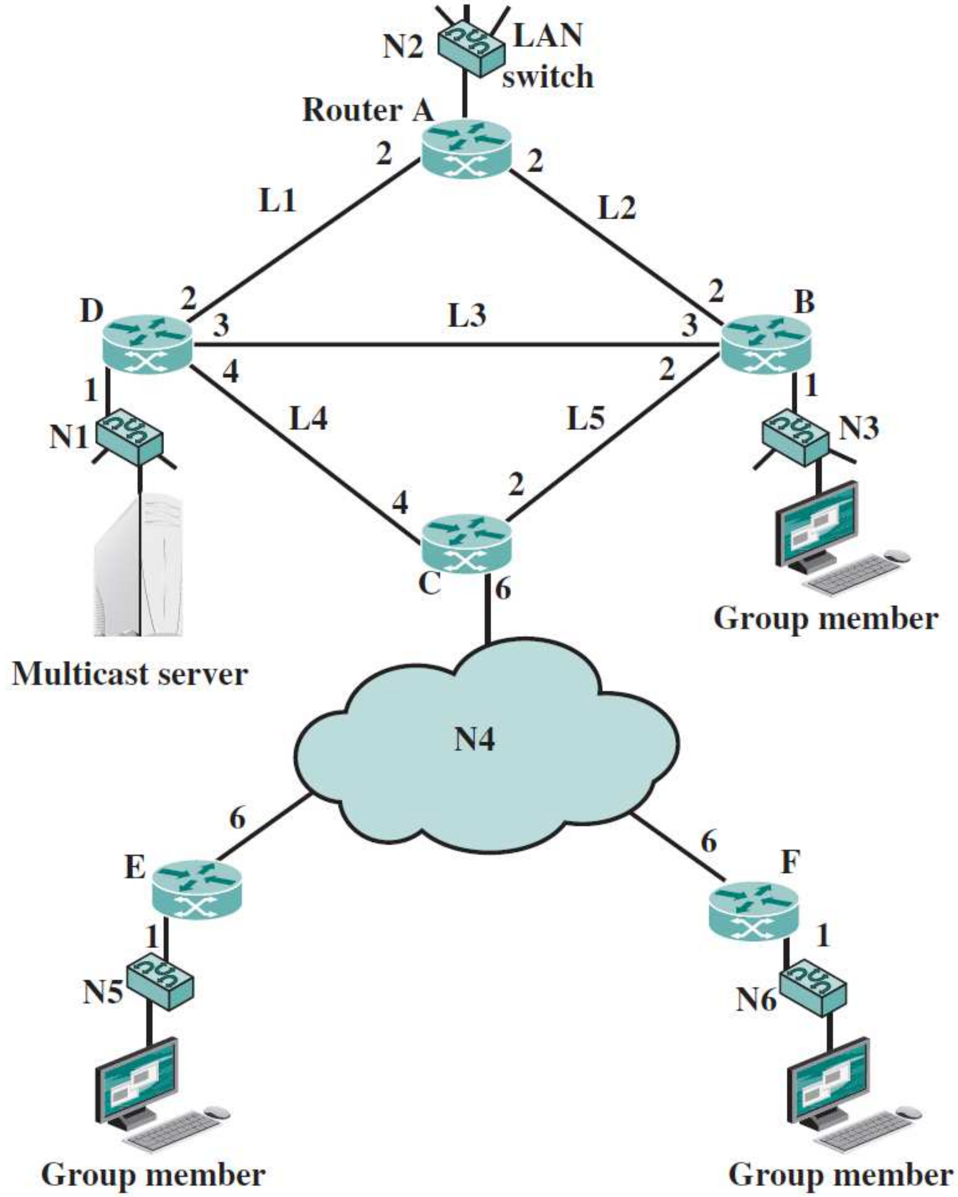
Multimedia stream "broadcasts"

Teleconferencing – a transmission from a station sent to all members

Database updating – for all copies of replicated files or databases

Distributed computing – resource sharing

Real time workgroups – real time exchange of information



Multicast Configuration

Multicast over a single Ethernet LAN segment is straightforward; provision for MAC multicast addresses, due to the broadcast nature of LAN

For Internet environment, more approaches:

Broadcast and Multiple Unicast

Broadcast a copy of packet to each network, even if does not contain group members

For figure behind, multicast server sends a packet to group hosts from networks N3, N5, N6: requires 13 copies of the packet

Multiple Unicast

Send packet only to networks that have hosts in group

Source knows location for each group member

11 packets

True Multicast

Use of following algorithm:

Determine least cost path to each network that has host in group

Gives spanning tree configuration containing networks with group members

Transmit single packet along spanning tree

Routers replicate packets at branch points of the spanning tree

8 packets required for above example

	Broadcast					Multiple Unicast				Multicast
	S → N2	S → N3	S → N5	S → N6	Total	S → N3	S → N5	S → N6	Total	
N1	1	1	1	1	4	1	1	1	3	1
N2										
N3	1	1	1					1	1	
N4			1	1	2		1	1	2	2
N5			1		1		1		1	1
N6			1	1			1	1	1	
L1	1			1						
L2										
L3		1			1	1			1	1
L4			1	1	2		1	1	2	1
L5										
Total	2	3	4	4	13	3	4	4	11	8

<u>Multicast problems:</u>

Router may have to forward more than one copy of packet (multiple output branches)

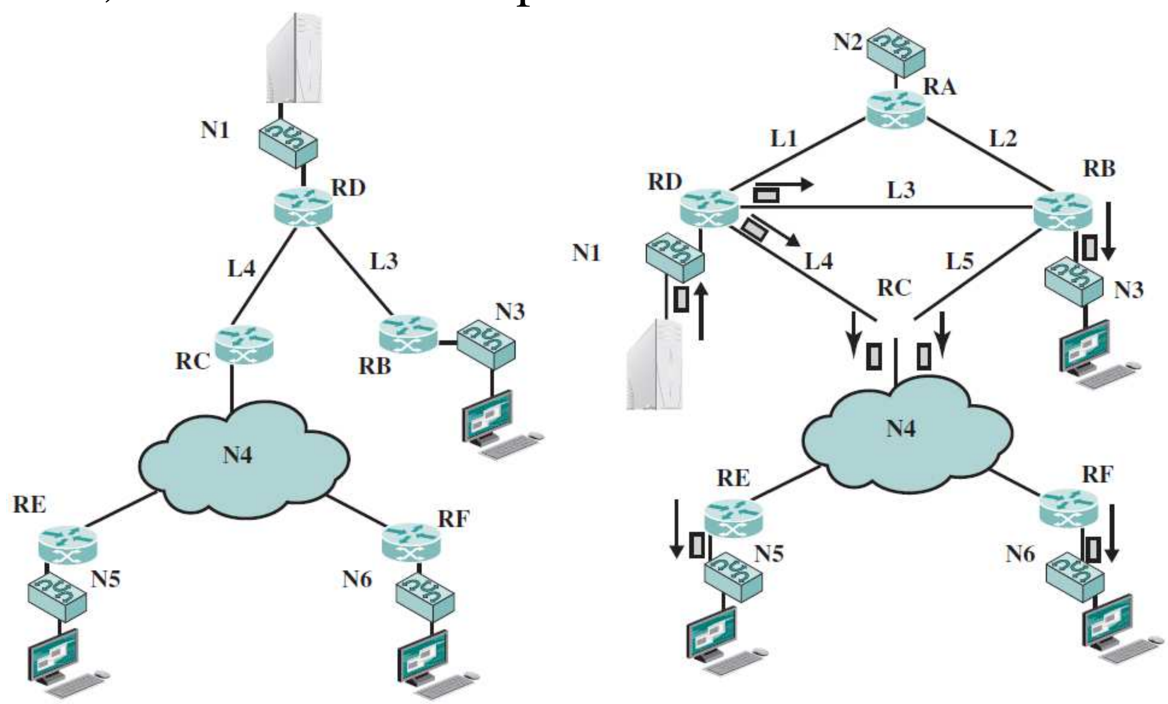
Convention needed to identify multicast addresses

IPv4 - Class D – starts with 1110 …

IPv6 - 8 bit prefix, all 1s, 4 bit flags field, 4 bit scope field, 112 bit group ID

Nodes (routers & source) must translate between IP multicast addresses and a list of networks containing group members; allows tree development

Multicast transmission example



(a) Spanning tree from source to multicast group

(b) Packets generated for multicast transmission

Router must translate between IP multicast address and a network LAN multicast address (at the MAC level) in order to deliver packet to that LAN

Mechanism required for hosts to dynamically join and leave multicast groups

Routers must exchange info

- Which networks include members of given group
- Sufficient info to work out shortest path to each network (spanning tree)
- Routing algorithm to work out shortest path
- Routers must determine routing paths based on source and destination addresses, for avoiding packet duplication

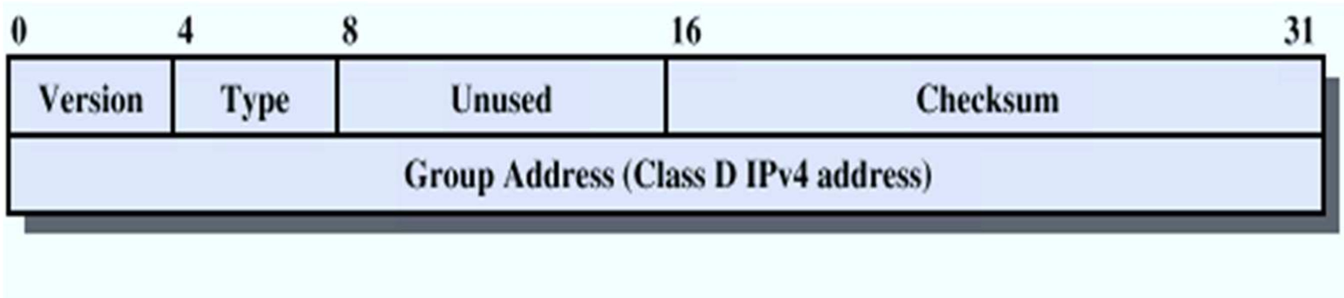
IGMP (Internet Group Management Protocol)

RFC 1112, initial developed for IPv4, but incorporated also in ICMPv6

Host and router exchange of **multicast group information**

Use broadcast LAN to transfer information among multiple hosts and routers

IGMP Fields



Version - 1

Type

- 1 - query sent by a multicast router
- O - report sent by a host

Checksum – 16 bit ones complement addition of all the 16-bit words in the message

Group address

- Zero value in a request message
- Valid group address in a report message

IGMP Operation

To join a group, hosts sends report message

- Group address of group to join
- Sent in a IP datagram with the same multicast destination address
- All hosts in group receive message and learn new member
- Routers listen to all multicast addresses to hear all reports

Routers periodically issue request messages (queries)

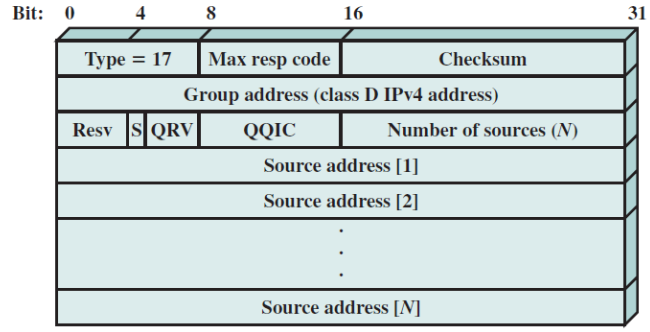
- Sent to *all-hosts* multicast address
- Host that want to stay in groups must read *all-hosts* messages and respond with report for each group it is in

Group Membership with IPv6

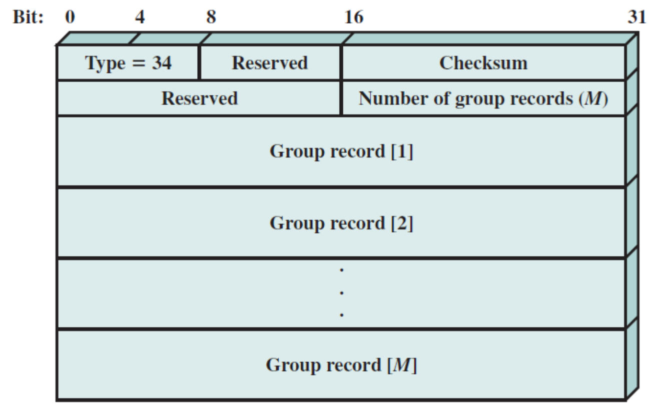
Function of IGMP included in ICMP v6; ICMPv6 contains a new type of message: group membership **termination** message, to allow host to leave the group

IGMP v3

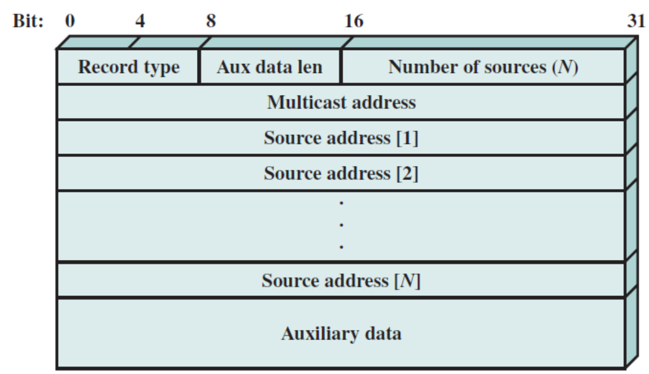
RFC 3376



(a) Membership query message



(b) Membership report message



(c) Group record