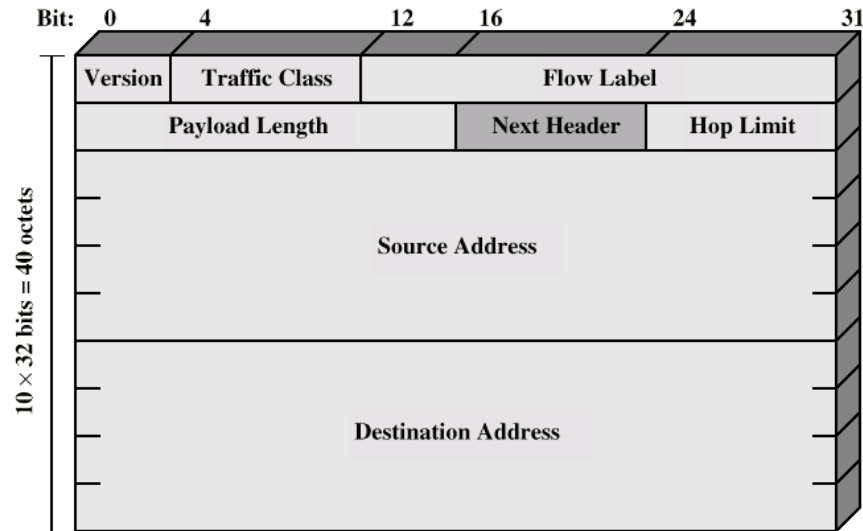


# IPv6



The New Internet Protocol and its  
Companion ICMP V6

# Outline

---

- IPv4 – Today's Internet - What's wrong?
- IPv6 – The Next Generation, (also new ICMPv6)
- Addressing and Routing (provider addressing)
- Autoconfiguration
- Security
- Support of Real-time Communication
- Deployment Strategy and Transition – How do we get there?

# IP v6 - Version Number

---

- IP v 1-3 defined and replaced
- IP v4 - current version
- IP v5 - streams protocol
- IP v6 - replacement for IP v4
  - During development it was called IPng
  - Next Generation

# Why Change IP?

---

- Address space 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
- Requirements for new types of service

# Expanded address space

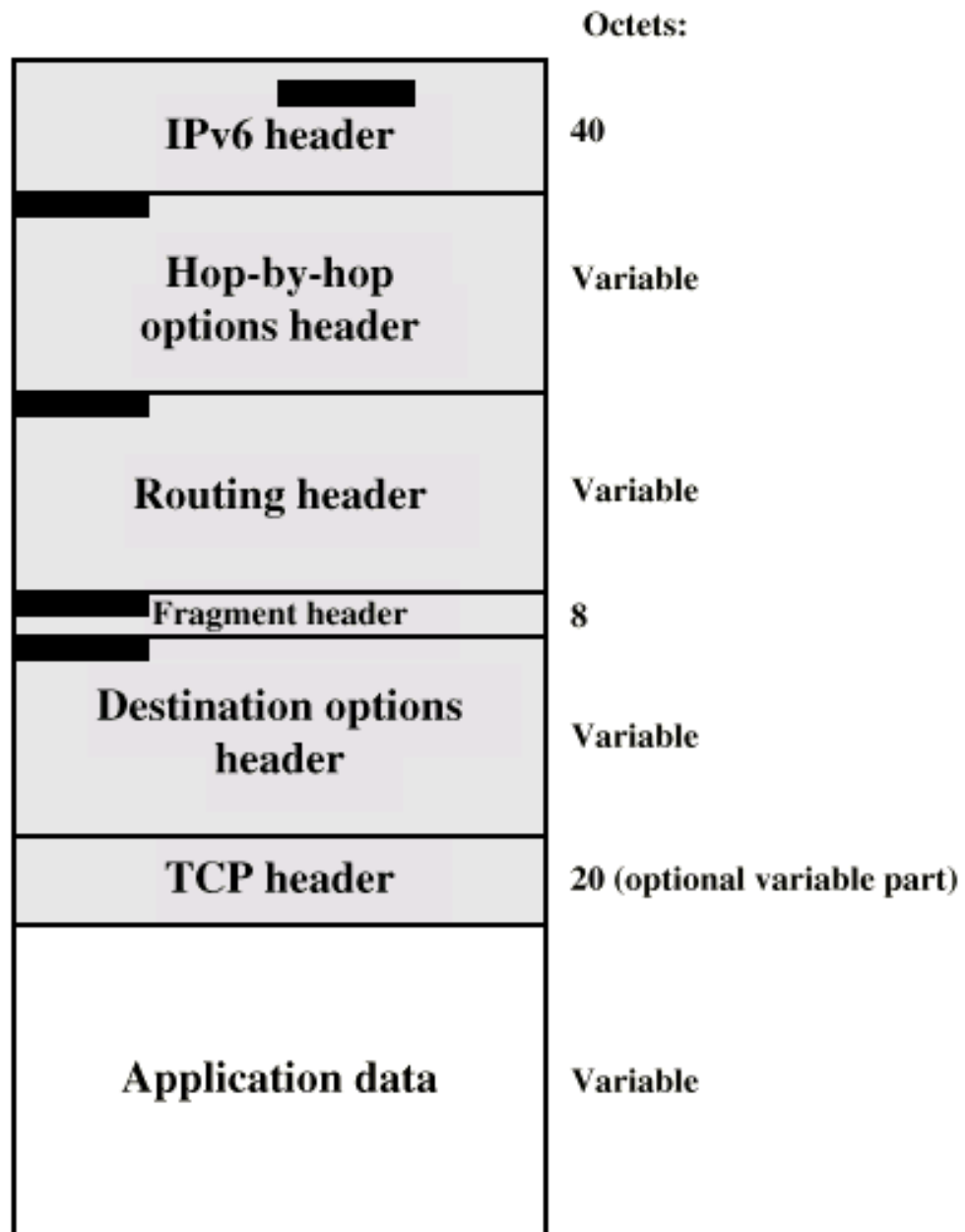
---

- Expanded address space
  - 128 bit
- 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

# IPv6 Enhancements (2)

---

- 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
  - Labeling of packets to particular traffic flow
  - Allows special handling
  - e.g. real time video



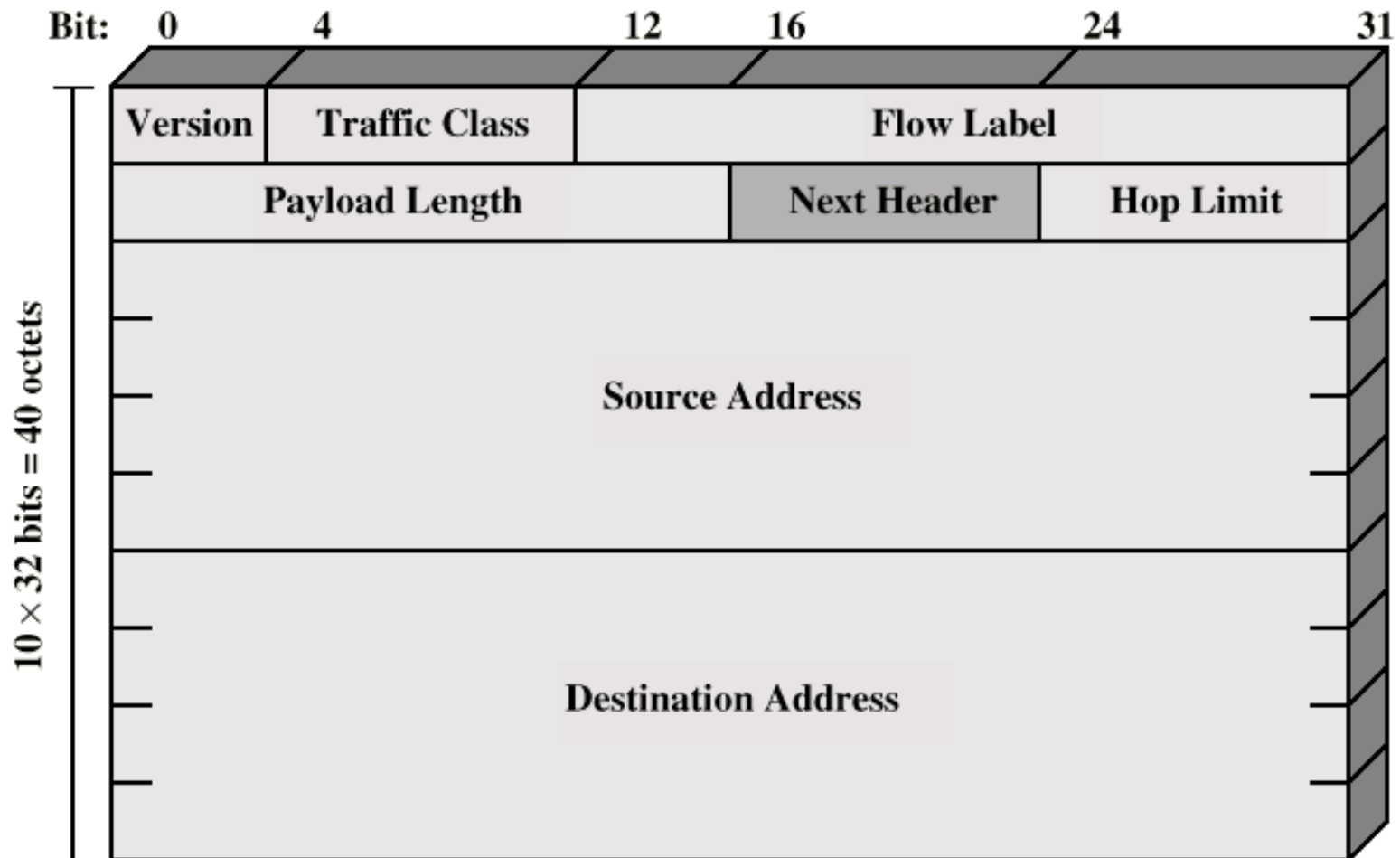
**Next Header field**

# Extension Headers

---

- Hop-by-Hop Options
  - Require processing at each router
- Routing
  - Similar to v4 source routing
- Fragment
- Authentication
- Encapsulating security payload
- Destination options
  - For destination node

# IP v6 Header



# IP v6 Header Fields (1)

---

- *Version* – 4 bit IP version (6)
- *Priority (Traffic Class)* – 4 bit priority value
  - Classes or priorities of packet
  - Still under development
  - See RFC 2460
  - Differentiates congestion-controlled traffic vs. non congestion-controlled traffic
- *Flow Label* – 24 bit value identifying flow requirements
  - Used by hosts requesting special handling
  - Used by routers to allocate resources or define routing

# IP v6 Header Fields (2)

---

- *Payload Length* – 16 bit length of packet
  - Includes all extension headers plus user data
  - Allows for  $2^{16} - 1$  (65,535) bytes
  - Optional Extension Headers allow for larger packet sizes
- *Next Header* – 8 bit identifier of next header
- *Hop Limit* – 8 bit value denoting number of hops left before packet is dropped
- *Source Address* – 128 bit address of sending host
- *Target Address* – 128 bit address of target host

# IPv6 Solutions

---

## ■ Addressing

- Addresses now 128 bits long ( $3.4 \times 10^{34}$  addresses)
  - Theoretically yields 665,570,793,348,866,943,898,599 IP addresses per square meter of the earth's surface.
  - Routing analysis shows practical values between 1564 and 3,911,873,538,269,506,102 IP addresses per square meter
- Address auto-configuration

## ■ Quality of Service

- Flow control and QoS options allow for better connections of high bandwidth and high reliability applications

## ■ Security

- Extension headers allow for standard encryption of data and standard authentication of users to hosts

## ■ Packet Size

- Extension headers allow for larger packets

# The Design of IPv6

---

- IPv4 design was very good IPv6 should keep most of it
- It could only increase the size of addresses and keep every thing the same
- Experience brought lessons for improvement

# IPv4 Packet Header

---

Version	IHL	Type of Service	Total packet length			
Identification			UU	DF	MF	Fragment Offset
Time to Live	Protocol		Header Checksum			
Source Address						
Destination Address						
Option Data (0 to 40 bytes)						

# IPv6 Packet Base Header

---

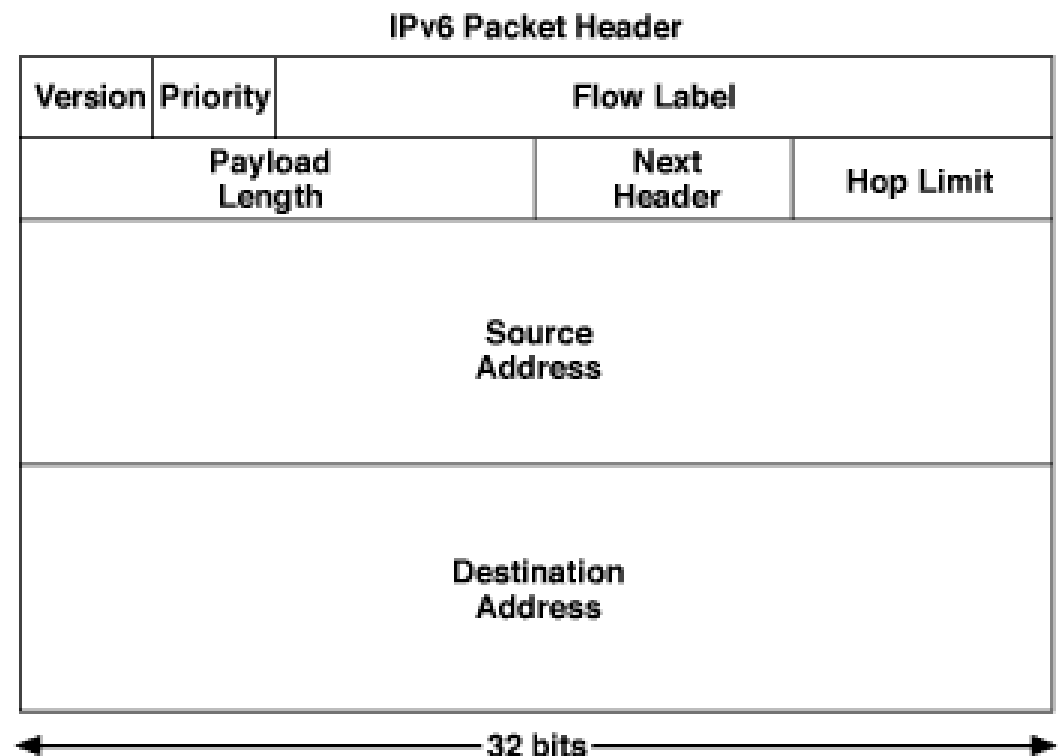
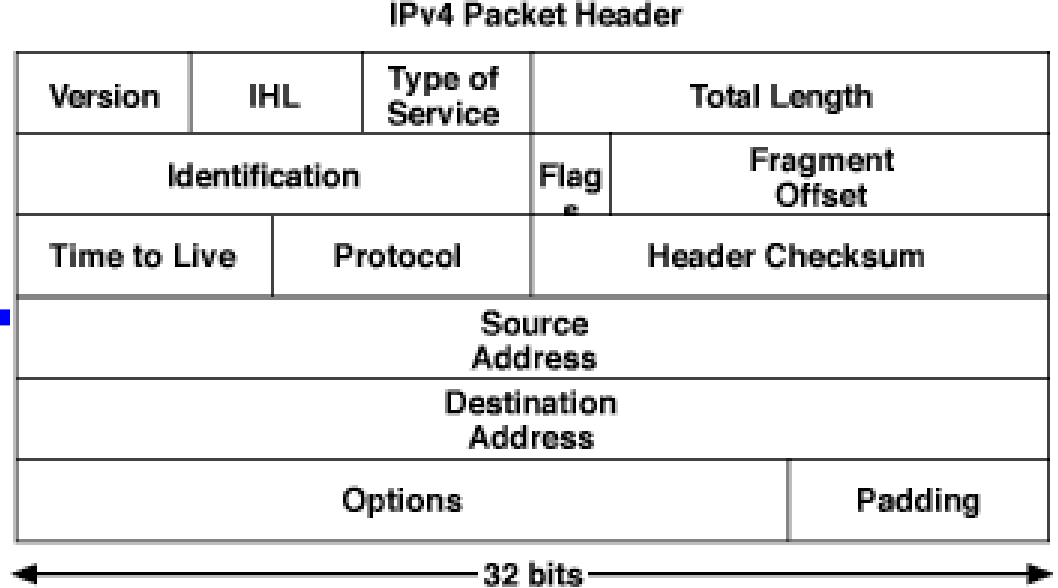
Version	Priority	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			

# Comparison of Headers

---

- V6: 6 fields + 2 addr
- V4: 10 fields + 2 addr + options
- Deleted:
  - Header length
  - type of service
  - identification, flags, fragment offset
  - Header Checksum
- Added:
  - Priority
  - Flow label
- Renamed:
  - length -> Payload length
  - Protocol -> Next header
  - time to live -> Hop Limit
- Redefined: Option mechanism

- Note that while the IPV6 address are four times as large as the IPV4 address, the header length is only twice as big.



# Simplifications

---

- Fixed format headers
  - no options -> no need for header length
  - options expressed as Extension headers
- No header checksum
  - reduce cost of header processing, no checksum updates at each router
  - minimal risk as encapsulation of media access protocols (e.g..., Ethernet, PPP) have checksum
- No fragmentation
  - hosts should use path MTU discovery
  - otherwise use the minimum MTU (536 bytes)

# Renaming

---

- Total Length → Payload Length
  - not include header length
  - max length 64Kbytes with provision for larger packets using “jumbo gram” option
- Protocol Type → Next header, can be set to:
  - Protocol type (UDP, TCP, etc..)
  - Type of first extension header
- TTL → Hop limit
  - “Truth in advertising!”,
  - number of hops NOT number of seconds

# New Fields

---

- Flow label & Priority
  - to facilitate the handling of real time traffic

# Options → Extension Headers

---

- Routers treat packets with options as “second class citizens” because it is slow to process, thus programmers tend not to use them and options almost became obsolete.

# Daisy Chain of Headers

---



# IPv6 Extension Headers

---

- Replace IPv4 Options field
- Used to define optional information about the packet or connection
- Generally not processed by the router, so they incur no overhead in the routers
- May be zero or more extension headers in a packet
  - The Next Header Id gives the id of the next header
  - Each extension header contains a length and Next Header Id field
  - Eventually, the Next Header Id will be the TCP header, which surrounds the data
- Ex. Encryption, authentication, fragmentation and routing information, and size extension

# Hop-by-Hop Options

---

- Next header
- Header extension length
- Options
  - Jumbo payload
    - Over  $2^{16} = 65,535$  octets
  - Router alert
    - Tells the router that the contents of this packet is of interest to the router
    - Provides support for RSVP (chapter 16)

# IPv6 extension headers

---

- Hop-by-hop options
- Routing
- Fragment
- Destination options
- Authentication
- Encryption Security Payload

# Protocol & Header Types

---

Decimal	Keyword	Header Type
0	HBH	hop-by-hop
3	ICMP	Inet Control
4	IP	v4 encapsul.
6	TCP	
17	UDP	
43	RH	Routing hdr

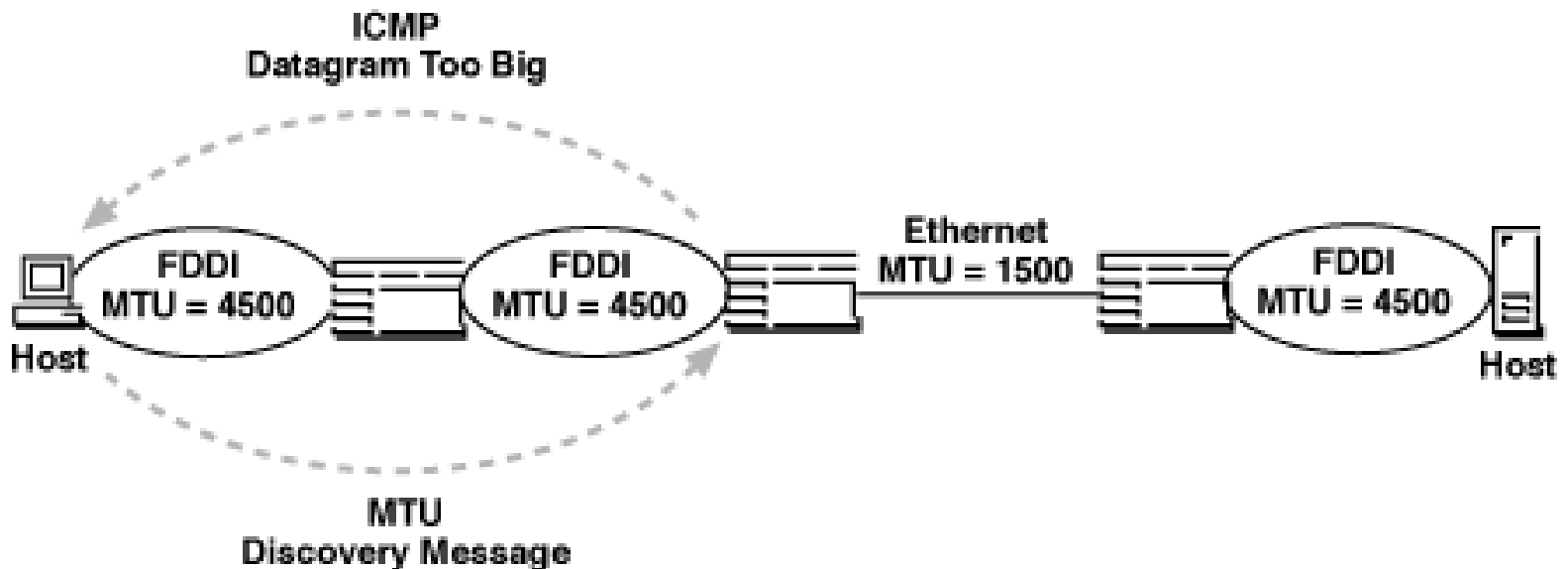
# IPv6 Optional Headers

---

- Extension Header Order
  - IPv6 Header
  - Hop by Hop Options Header
  - Destination Options Header 1
  - Source Routing Header
  - Fragmentation Header
  - Authentication Header
  - Encryption Header
  - Destination Options Header 2

# IPv6 Fragmentation Header

- IPv6 only allows fragmentation at source and destination nodes (IPv4 had the ability to fragment packets at any point in path). The header contains fields that identify a group of fragments as a packet and assign them sequence number



# IPv6 Fragmentation Header

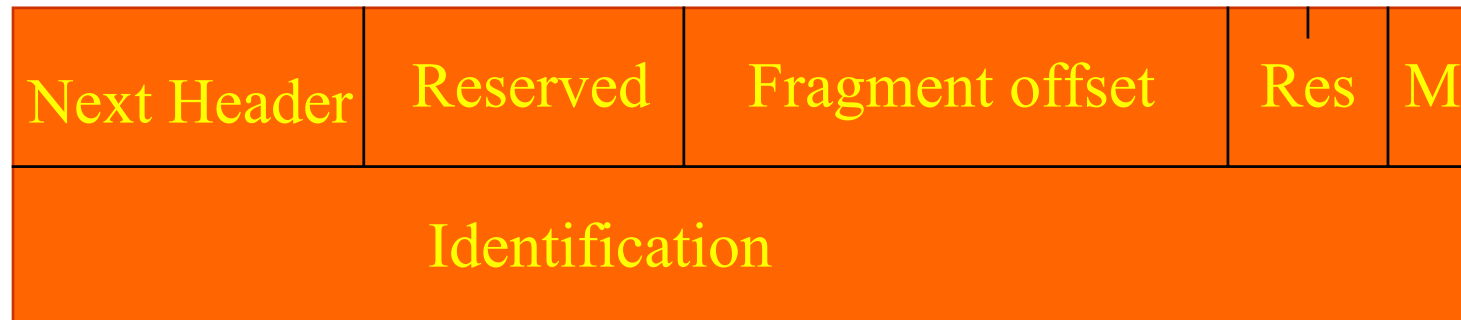
---

- Fragmentation only allowed at source
- No fragmentation at intermediate routers
- Node must perform path discovery to find smallest MTU of intermediate networks
- Source fragments to match MTU
- Otherwise limit to 1280 octets

# Fragmentation Header Fields

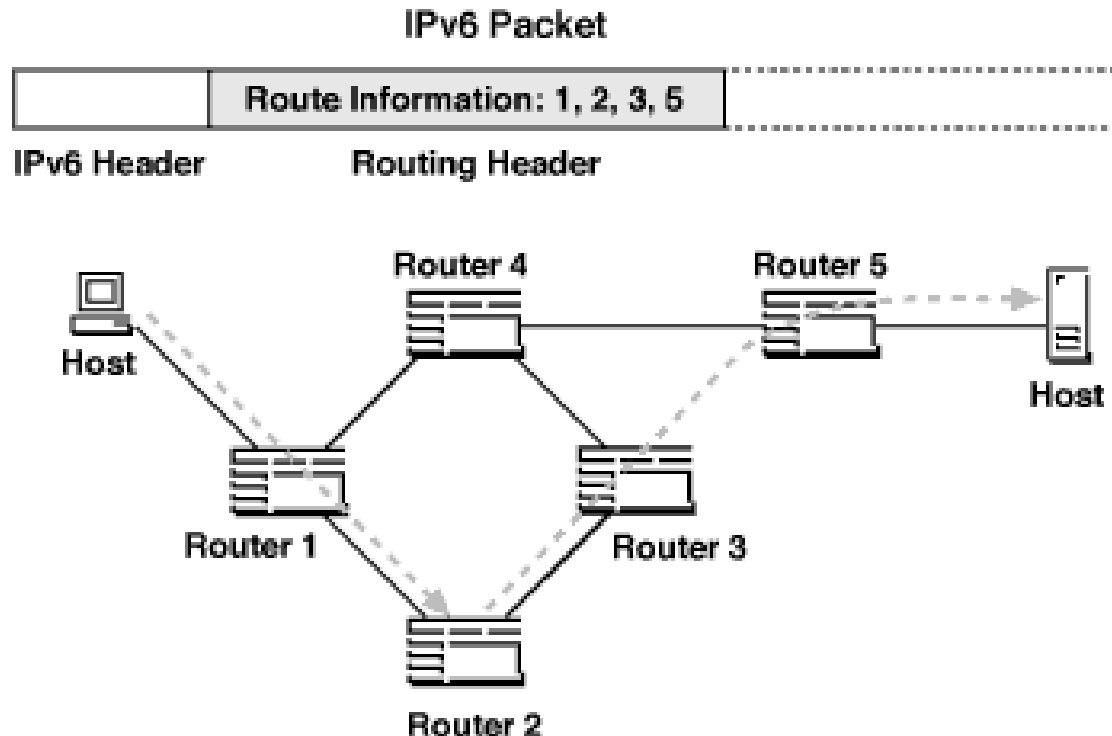
---

- Next Header
- Reserved
- Fragmentation offset
- Reserved
- More flag
- Identification



# Routing Header

- Allows a source node to specify a list of IP addresses that dictate what path a packet will traverse



# Routing Header

---

- Next Header
- Header extension length
- Routing type
- Segments left
  - i.e. number of nodes still to be visited

# Routing Header

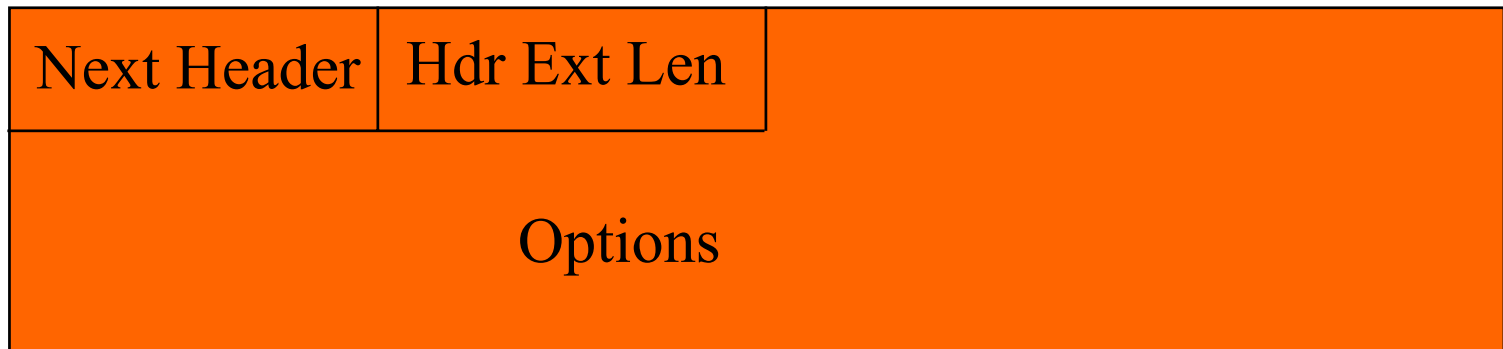
Next Header	0	Num addrs	Next Addr
Reserved	strict/loose bit mask (24)		
Address[0]			
.....			
Address[Num Addrs -1]			

Routers will only look at the routing header if they recognize one of their addresses in the destination field of the main header

# Destination Option Header

---

- Will only be examined by the station specified in the destination address.

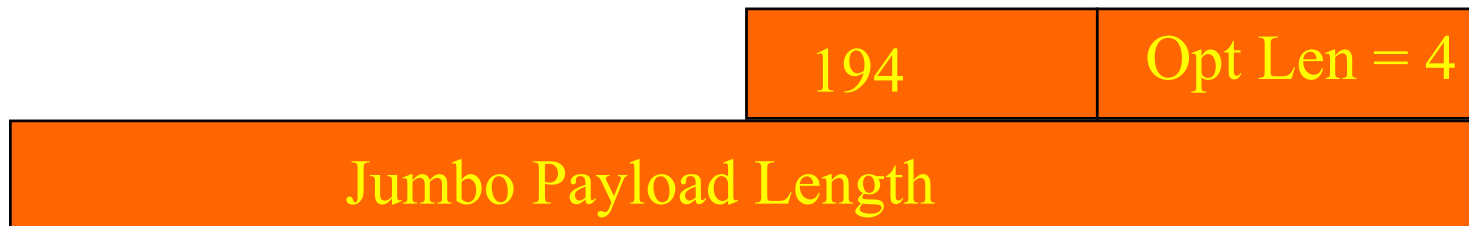


# Hop-by-Hop Option Header

---

- Will be examined by each router.
- Has same form as destination options hdr.

To satisfy networking requirement of supercomputers, the Jumbo payload option is used to send very large packets (the IPv6 length field is set to zero):



# IPv6 Enhancements

---

## ■ Flow Labeling Capability

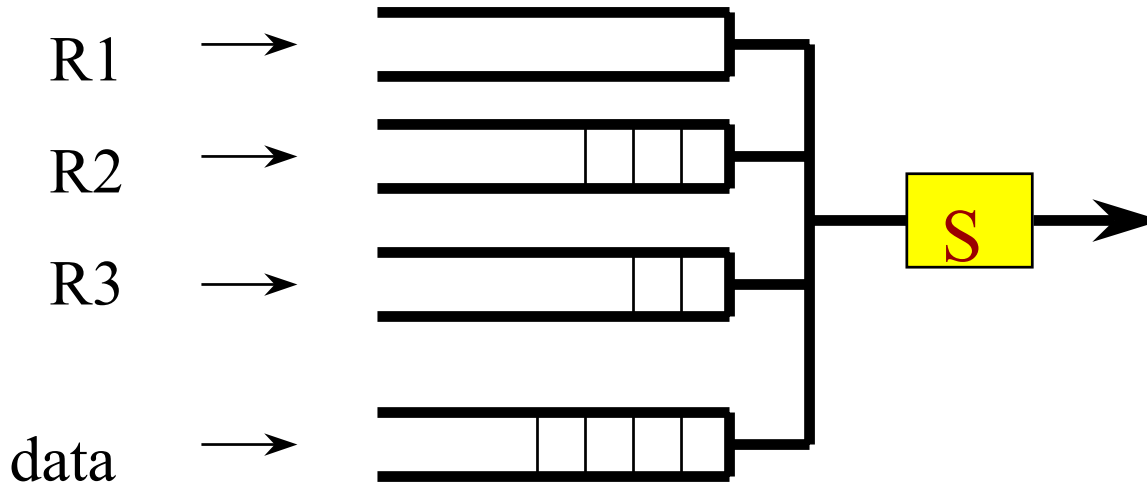
- A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service (for applications such as videoconferencing).

# Real-time Support & Flows

---

- A proper handling of flows is required for high-quality multimedia communications in the new Internet
- A flow is a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers.

# Real-time flows & Data Queues



The *flow label & source address* are used to assert which packets belong to what flows

In IPv6 *port numbers* deep inside due to *daisy chaining*

Even may not be visible due to *encryption*

# Security

---

- If security is provided at the IP level it becomes standard service that all applications can use
- It is absolutely necessary to implement if we want to develop of commercial use the Internet, e.g...., to deter sniffing attacks on passwords and credit card numbers.

# IPv6 Authentication Header

---

- Gives network application a guarantee that packet did in fact come from an authentic source.
- the packet has not been altered during transmission.
- Extremely easy to spoof data streams in IPv4.

# IPv6 Encryption Header

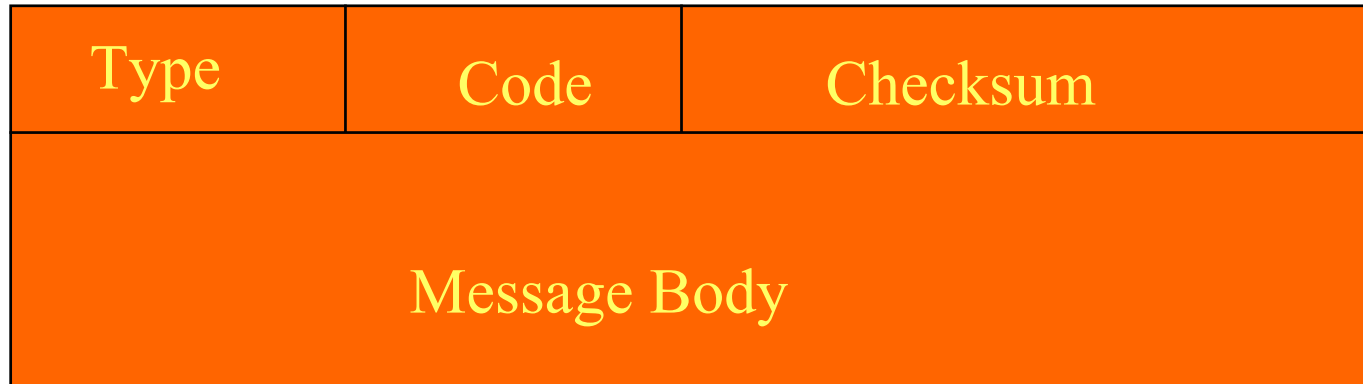
---

- Encryption header
  - Guarantee that only legitimate receivers
  - will be able to read the content of the packet
- Encapsulating Security Payload service is used to encrypt the entire datagram, transport-layer header and payload.

# ICMP.... Streamlined

---

- Removed unused functions in ICMP of v4
- Incorporate IGMP of v4



# ICMP Error Messages

---

## 1 Destination Unreachable. Codes:

- 0 No route to destination
- 1 destination prohibited
- 3 Address unreachable
- 4 Port unreachable

## 2 Packet Too Big

contain next hop MTU.  
used for path MTU discovery

## 3 Time Exceeded. Codes:

- 0 Hop limit exceeded
- 1 Fragment reassembly time exceed

## 4 Parameter Problem

No error message in response to multicast or ICMP packets

# Other ICMP messages

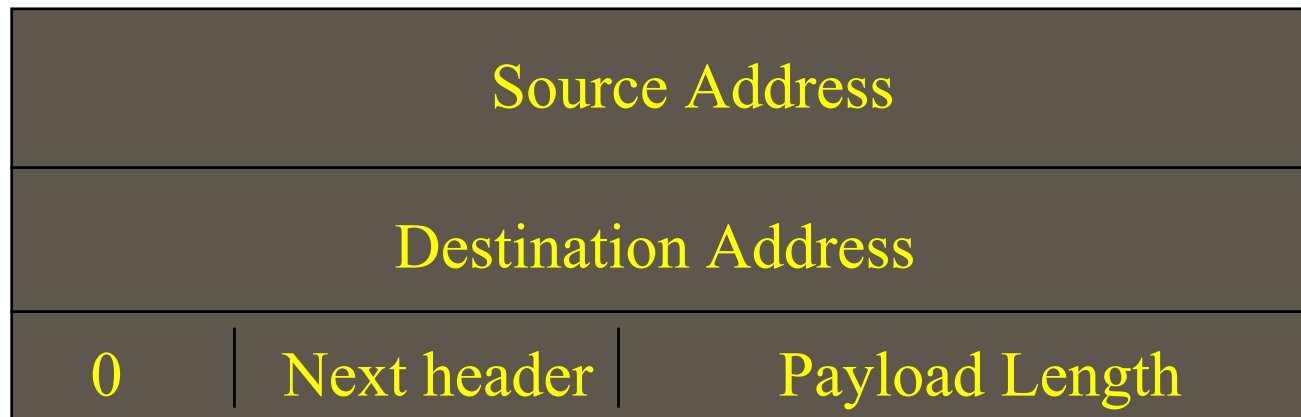
---

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

# Impact on Upper Layers

---

Upper-layer Checksums : Mandatory (even UDP)



# Impact on Upper Layers

---

## Domain Name Service

32-bit address to 128-bit address

## Programming interface

Address data structures

`AF_INET6, PF_INET6, in_addr6, sockaddr_in6`

Name-to-address translation functions

Address conversion functions

# IPv6 DNS

---

- Current 32-bit name servers cannot handle 128 bit addresses
- IETF designers have defined an IPv6 DNS standard (RFC 1886, DNS Extension to Support IPv6).
- Domain name lookups (reverse lookups) are also defined.

# Points of Controversy

---

- Do we need more than 255 Hops?
  - allowing hop count to be very large, looping packets will be relayed many times before being discarded
- Should packets be larger than 64K?
  - allowing very large packets increase the size of queues and the variability of queuing delays
- Can we live without checksum?
  - Some IPv4 routers started to cut corners by not verifying checksums to gain advantage over competition. By removing checksum altogether offers all routers the same advantage.

# IPv6 Addresses

---

- 128 bits long
- Assigned to interface
- Single interface may have multiple unicast addresses
- Three types of address
- Unicast – A single address on a single interface
  - A packet sent here arrives here
- Multicast – A set of interfaces
  - Interfaces may be configured to recognize multiple addresses
  - All interfaces associated with the multicast address receive the packet
- Anycast – A set of interfaces
  - Only one of the interfaces associated with the address receives the packet (the closest one)
  - Set of interfaces (typically different nodes)
  - Delivered to any one interface
  - the “nearest”

# IPv6 Addressing Cont.

---

## ■ IPv6 Address

- X:X:X:X:X:X:X:X

- X is a 16 bit value written in hex (leading zeros may be omitted)
- Ex. 1025:1ab6:0:0:0:87:a76f:1234

- The first sequence of zeros may be replaced by two colons

- Ex. 1025:1ab6::87:a76f:1234

# Notations of IPv6 Addresses

---

- 128 bit is represented as:
  - 8 integers (16-bit) separated by colons
    - each integer is represented by 4 hex digits

**Example:**

FEDC:BA98:7654:3210:FEDC:BA98:7664:3210

# Simplifications

---

- Skip leading zeros
  - Example: 1080:0000:0000:0000:0008:0800:200C:417A
  - is reduced to: 1080:0:0:0:8:800:200C:417A
- A set of consecutive nulls is replaced by :: (at most one :: inside an address)
  - the above address is reduced to:
    - 1080::8:800:200C:417A

# IPv6 Address Format

---

- Due to method of allocating certain styles of IPv6 addresses, it will common for addresses to contain long string of zero bits. In order to make writing addresses containing zero bits easier, a special syntax “::” is available to suppress zeros.
- For example  
1080:0:0:0:0:800:200C:417A  
can be represented as  
1080::800:200C:417A

# IPv6 Address Format

---

- An alternative form, which is convenient when dealing with mixed environment of IPv4 and IPv6 is

x:x:x:x:x:d.d.d.d.

where x = hexadecimal value of six high-order 16 bits

d = four low-order 8 bit pieces of addresses

for example:

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

::FFFF.129.144.52.38 (in compressed form)

# Unicast Address

---

- Aggregatable Global Unicast Address
- Address Hierarchy
  - IPv6 was designed from the ground up to provide a highly scalable address space that can be partitioned into a flexible and efficient global routing hierarchy.
  - At the top of the hierarchy, several international registries assign blocks of addresses to top level aggregators (TLA)
  - TLAs allocate block of addresses to Next Level Aggregators (NLA) which represent large provider and corporate networks.

# Aggregation Based IPv6 Address

- NLA can divide the address so to create their own hierarchy, one that maps to current ISP industry, in which smaller ISP subscribe to higher level ISP
- When an NLA is a provider, it further allocates address to its subscribers.

3	13	32 bits	16 bits	64 bits
001	TLA	NLA	SLA	Interface ID
Public Topology			Site Topology	Local Interface

# IPv6 Addressing Cont.

---

FP	Registry-id	Provider-id	Subscriber-id	Subnet-id	Interface-id
----	-------------	-------------	---------------	-----------	--------------

## ■ Unicast addresses

- FP – Format Prefix (001 = Global Unicast)
- Registry-id – ID assigned to address registry organization
  - InterNIC
- Provider-id – ID assigned to the ISP
- Subscriber-id – ID assigned to the user/business
- Subnet-id – ID assigned to a physical LAN by User (subnet)
- Interface-id – ID assigned to interface
  - MAC address

# IPv6 Addressing Cont.

---

1111111010	00	Interface-id
------------	--	--------------

## ■ Link-local unicast address

- Used to address a host on the local network (subnet)
- Routers will not forward these packets

1111111011	000	Subnet-id	Interface-id
------------	---	-----------	--------------

## ■ Site-local unicast address

- Used to address hosts within the site only

# Unicast Addresses

---

- Two Types of Local-Use Addresses defined.

- Link-Local - used on a single network

- Format :

10 bits	54 bits	64 bits
1111111110	0	interface ID

- Site-Local - for use on a single site

- Format :

10 bits	38 bits	16 bits	64 bits
1111111011	0	Subnet ID	Interface ID

# Unicast Addresses

---

## ■ Unicast Address

- **0:0:0:0:0:0:0:0** - **unspecified address**. Indicates absence of address and must never be assigned to node.
- One possible use is in the Source Address field of an IPv6 packets sent by an initializing host before it has learned its own address.
- **0:0:0:0:0:0:0:1** - **loopback address**. It may be used to send an IPv6 packet to itself. Must not be used as Source Address in IPv6 packet.

# Unicast Address

---

- IPv6 Addresses with Embedded IPv4 Addresses
  - IPv4 Compatible IPv6 address
    - Low order 32 bits - IPv4 address
    - Next 16 bits - 0000
  - IPv4 Mapped IPv6 address
    - Used to represent the addresses of IPv4-only nodes.  
(those that DO NOT support IPv6)
    - Low order 32 bits - IPv4 address
    - Next 16 bits - FFFF

# IPv6 Addressing Cont.

---

- Link-local and Site-local addresses allow easy integration to global Internet
  - Private networks will only use the subnet-id and interface-id to address their network
  - When they are ready to connect to the Internet, they obtain a global prefix (Registry-id + Provider-id + Subscriber-id), and prefix it to their existing Subnet-id to form a global IP address

# IPv6 Addressing Cont.

---

1111111111	Flags (4 bits)	Scope-id (4 bits)	Group-id (112 bits)
------------	----------------	-------------------	---------------------

## ■ Multicast addresses

- Used to send a single message to multiple machines
- An interface may belong to any number of multicast groups
- Flags
  - First 3 bits are reserved and must be 0
  - Fourth bit (T) defines transient (0) vs. permanent (1) multicast addresses
- Scope defines scope of group
  - Node-local, link-local, site-local, org-local, global

# IPv6 Addressing Cont.

---

- Anycast address
  - Looks like any other unique address
  - Cannot be used as a source address
  - Generally to be used only on routers
  - Identifies a group of interfaces
    - Usually each interface is on a separate machine
    - Only one will receive the packet, typically the closest
  - One form already predefined – subnet-router
    - Defined as an interface address of all zeros
    - All routers are required to support it
    - Used to address the closest router that is connected to a subnet

# IPv6 Addressing Cont.

---

## ■ Unspecified address

- 0:0:0:0:0:0:0:0
- Used when sending host does not know its IP address
  - Ex. – During startup before IP address has been assigned
- May never be used as destination address

# IPv6 Addressing Cont.

---

- Loopback address
  - 0:0:0:0:0:0:0:1
  - Never leaves the interface card

# Anycast Addresses

---

- Conceptually, anycast is a cross between unicast and multicast.
- Two or more interfaces on an arbitrary number of nodes are designated as anycast group.
- A packet addresses to group's anycast address is delivered to only one of the interfaces on the group, typically the “nearest” interface, according to the current routing protocol metrics

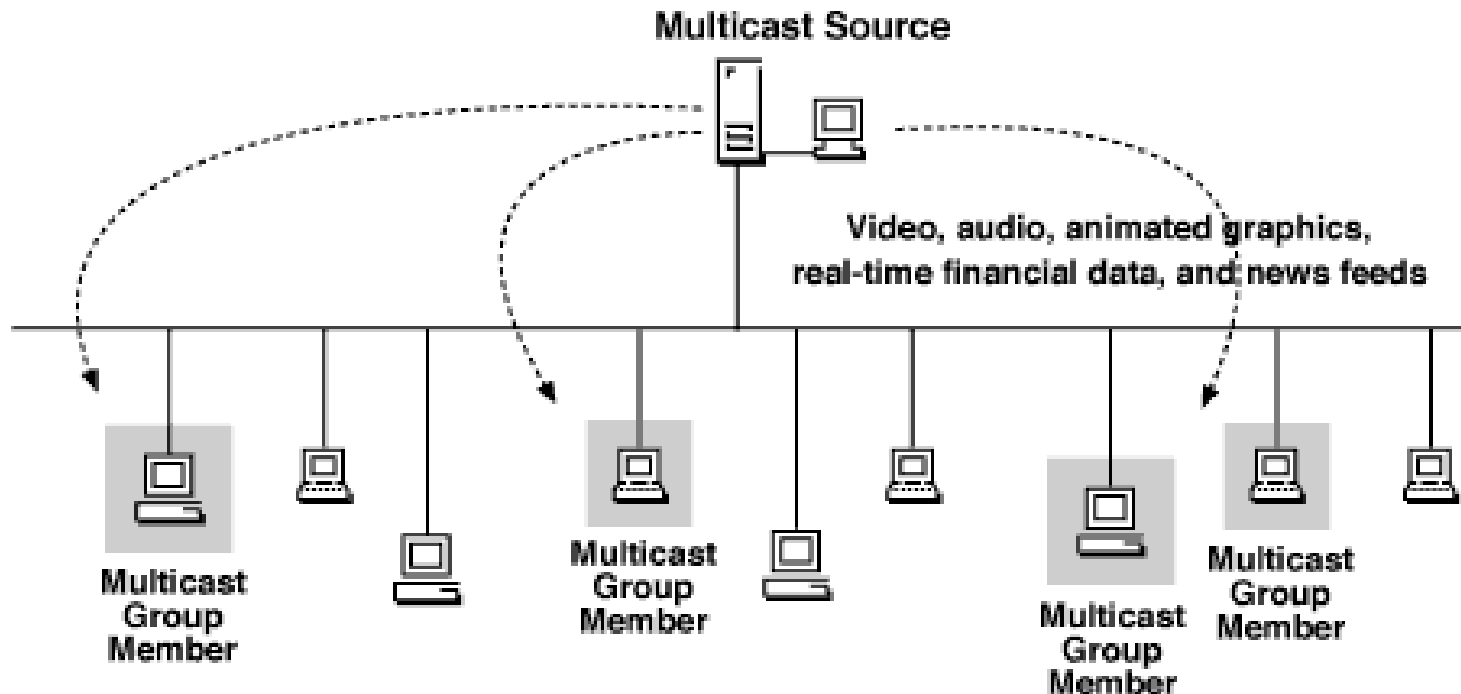
# Anycast Addresses

---

- Anycast is a new service, and its implications not envisioned fully.
- One use is to have provider's routers have the same anycast address. If one of the routers goes down, the next nearest device will receive the traffic.
- Anycast addresses are allocated from the unicast address space, using any of the defined unicast address format.

# Multicast Addresses

- Multicast Addressing : The address is for a set of interfaces. A packet sent to mulitcast address is delivered to all interfaces identified by that address.



# Multicast Addresses

---

## ■ Multicast addresses

- A packet address to a multicast address is delivered to all the interfaces assigned with that multicast address. IPv6 addressing doesn't include a broadcast address
- Format
  - First 8 bits - 1111 1111
  - Next 4 bits - Flags
    - First 3 bits of Flag are set to zero
    - Fourth bit (T) indicates if the multicast address is permanent (T = 0) or non-permanent (T=1)

# Multicast Addresses

---

- Next 4 bits - scope field.
  - used to limit the scope of the multicast group
  - 0 = reserved
  - 1 = node-link scope
  - 2 = link-local scope
  - 5 = site-local scope
  - 8 = organizational-local scope
  - 3,4,6,7,9,A,B,C = unassigned
- Remaining 112 bits - Group ID

# Transitioning the Internet

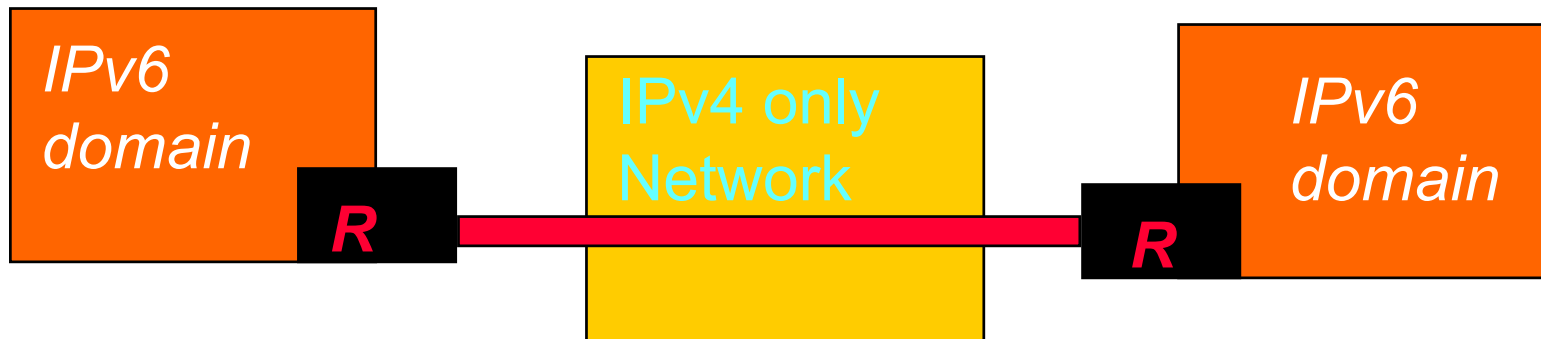
---

- At the beginning, all IPv6-capable hosts will also be IPv4-capable so as to retain connectivity with the existing Internet.
- To transform IPv4 into a dual-stack IPv6-capable host, it should include:
  - The IPv6 basic code
  - Handling IPv6 within TCP & UDP
  - Modify socket interface to support new addresses
  - Handling the interface with the name service

# The 6-Bone

---

- The Similar to the M-Bone, Initially the connectivity is achieved by tunneling
- IPv6 packet will be encapsulated within IPv4 packets.



# Transition: How do we get there?

---

- IPv6 will be implemented slowly
- Multiple IPv6 networks will need to communicate, but will have only IPv4 networks connecting them
- IPv6 systems will have to be able to talk to IPv4 systems

# Transition: How do we get there?

---

- Two new address types defined:
  - IPv4-compatible
  - IPv4-mapped
- IPv6 routers at the boundary between an IPv4 network and an IPv6 network will convert the IPv6 packets to IPv4 packets

# Transition: How do we get there?

---

000000000000000000000000 – 80 bits – 00000000000000000000	00000000000000000000	IPv4 address
---	----------------------	--------------

## ■ IPv4-compatible address

- Last 32-bits are a valid IPv4 address
- Assigned to IPv6 systems communicating via an intermediate IPv4 network

# Transition: How do we get there?

---

00000000000000000000 – 80 bits – 000000000000000000	11111111111111111111	IPv4 address
---	----------------------	--------------

## ■ IPv4-mapped address

- Again, last 32 bits are a valid IPv4 address
- Used by IPv6 systems to communicate with IPv4 systems (does not yet support IPv6)

# IPv6 Related RFCs and References

---

- **RFC1809** - Using the Flow Label Field in IPv6. C. Partridge. June 1995. (Format: TXT=13591 bytes) (Status: INFORMATIONAL)
- **RFC1881** - IPv6 Address Allocation Management. IAB & IESG. December 1995. (Format: TXT=3215 bytes) (Status: INFORMATIONAL)
- **RFC1887** - An Architecture for IPv6 Unicast Address Allocation. Y. Rekhter & T. Li, Editors. December 1995. (Format: TXT=66066 bytes) (Status: INFORMATIONAL)
- **RFC1924** - A Compact Representation of IPv6 Addresses. R. Elz. April 1996. (Format: TXT=10409 bytes) (Status: INFORMATIONAL)

# IPv6 Related RFCs and References

---

- **RFC1933** - Transition Mechanisms for IPv6 Hosts and Routers. R. Gilligan & E. Nordmark. April 1996. (Status: PROPOSED STANDARD)
- **RFC2080** - RIPng for IPv6. G. Malkin, R. Minnear. January 1997. (Status: PROPOSED STANDARD)
- **RFC2081** - RIPng Protocol Applicability Statement. G. Malkin. January 1997. (Status: INFORMATIONAL)
- **RFC2133** - Basic Socket Interface Extensions for IPv6. R. Gilligan, S. Thomson, J. Bound, W. Stevens. April 1997. (Status: INFORMATIONAL)

# IPv6 Related RFCs and References

---

- **RFC2147** - TCP and UDP over IPv6 Jumbograms. D. Borman. May 1997. (Status: PROPOSED STANDARD)
- **RFC2185** - Routing Aspects of IPv6 Transition. R. Callon, D. Haskin. September 1997. (Status: Informational)
- **RFC2292** - Advanced Sockets API for IPv6. W. Stevens, M. Thomas. February 1998. (Status: Informational)
- **RFC2374** - An IPv6 Aggregatable Global Unicast Address Format. R. Hinden, M. O'Dell, S. Deering. July 1998. (Obsoletes RFC2073) (Status: PROPOSED STANDARD)
- **RFC2375** - IPv6 Multicast Address Assignments. R. Hinden, S. Deering. July 1998. (Status: Informational)

# IPv6 Related RFCs and References

---

- Semaria, Chuck, “Understanding IP Addressing: Everything You Ever Wanted To Know”, April 26, 1996
- Network Working Grouping, RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification, December 1998
- Network Working Grouping, RFC 2373 - Internet Protocol, Version 6 - Addressing architecture, July 1998
- University of Southern California, RFC 791 - Internet Protocol, DARPA Internet Program, Protocol specification, September 1981
- Bay Network, “White Paper- IPv6”,  
<http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/BayNetwroks/>  
1997

# IPv6 Related RFCs and References

---

- RFC1597 - Address Allocation for Private Internets
- RFC1700/STD2 – Assigned Numbers
- Tanenbaum, Andrew S., Computer Networks, Third Edition, ISBN 0-13-349945-6, p. 412-419
- Mbogho, Audrey, “The New Internet Protocol (Ipng)”, <http://www.nycinteractive.com/Ingenuity/Articles/tcp-ip/>, Summer 1997
- Robert M. Hinden. *IP Next Generation Overview*. <http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html>, May 14, 1995.