What’s wrong?

- Addressing
  - Current addressing scheme allows for over 2 million networks, but most are Class “C” which are too small to be useful
  - Most of the Class “B” networks have already been assigned
- Quality of Service
  - IPv4 does not implement QoS functionality

IPv6 Solutions

- Addressing
  - Addresses now 128 bits long (3.4 x 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

IPv6 Solutions Cont.

- 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

<table>
<tr><td>Version</td><td colspan="2">IHL</td><td>Type of Service</td><td colspan="4">Total packet length</td></tr>
<tr><td colspan="4">Identification</td><td>UU</td><td>DF</td><td>MF</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="8">Source Address</td></tr>
<tr><td colspan="8">Destination Address</td></tr>
<tr><td colspan="8">Option Data (0 to 40 bytes)</td></tr>
</table>

IPv6 Packet Base Header

Version	Priority	Flow label

Payload length	Next header	Hop limit

Source address

Destination address

IPv6 Base Header Cont.

- *Version* – 4 bit IP version (6)
- *Priority* – 4 bit priority value
  - Differentiates congestion-controlled traffic vs. non congestion-controlled traffic
- *Flow Label* – 24 bit value identifying flow requirements
  - Used by routers to allocate resources or define routing

IPv6 Base Header Cont.

- *Payload Length* – 16 bit length of packet
  - 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

IPv6 Base Header Cont.

- *Source Address* – 128 bit address of sending host
- *Target Address* – 128 bit address of target host

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

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

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

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

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 segmentation
  - hosts should use path MTU discovery
  - otherwise use the minimum MTU (536 bytes)

Renaming

- Total Length $\rightarrow$ Payload Length
  - not include header length
  - max length 64Kbytes with provision for larger packets using "jumbo gram" option
- Protocol Type $\rightarrow$ Next header, can be set to:
  - Protocol type (UDP,TCP, etc..)
  - Type of first extension header
- TTL $\rightarrow$ 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 treats packets with options as "second class citizens" because it is slow to process, thus programmers tend not use them and options almost became obsolete.

Daisy Chain of Headers

IPv6 Header Next Header= TCP	TCP Header + Data

IPv6 Header Next Header= Routing	Routing Header Next Header= TCP	TCP Header + Data

IPv6 extension headers

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

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

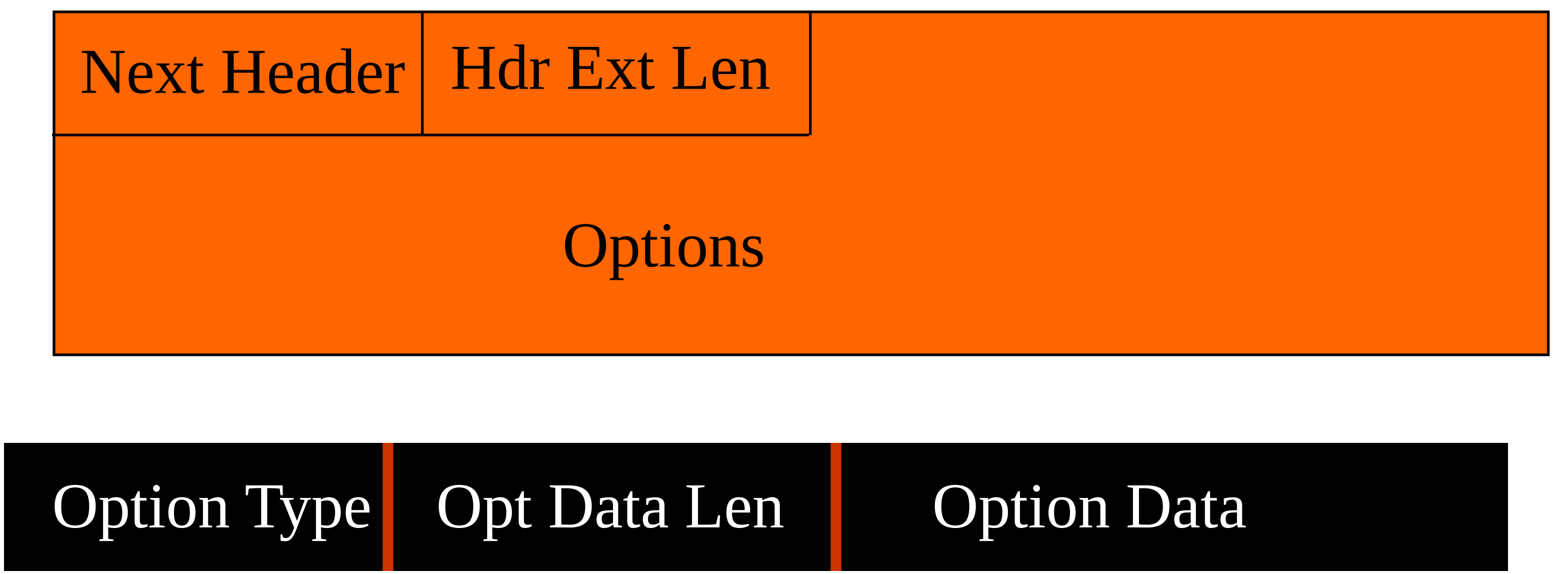
Fragment Header

- Routers do not fragment oversized packets
- Sender is to fragment &
- Receiver is to reassemble

Next Header	Reserved	Fragment offset	Res	M
Identification				

Destination Option Header

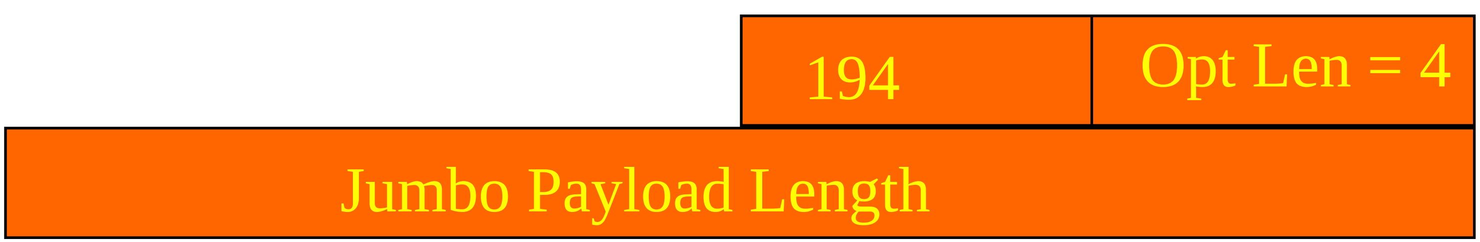
- ⌘Will only be examined by the station
- ⌘specified in the destination address.



Hop-by-Hop Option Header

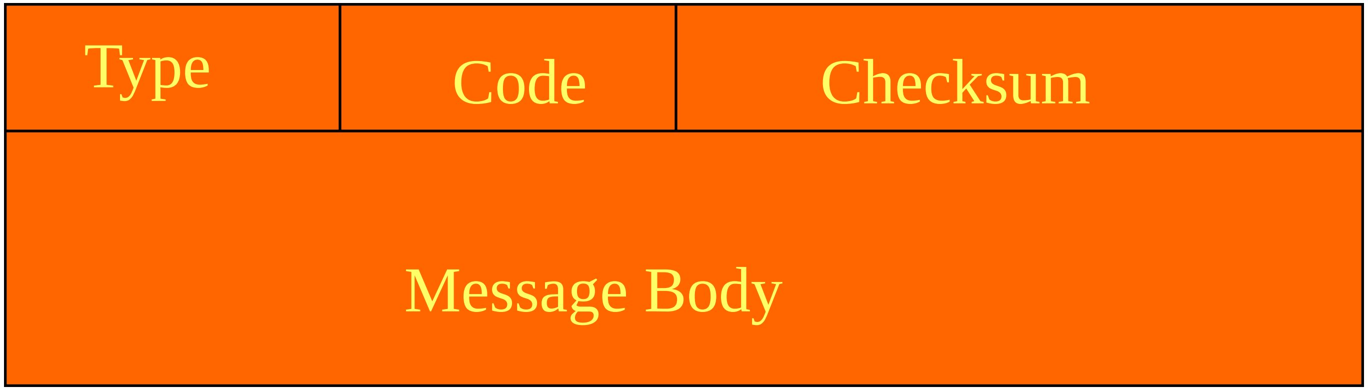
- Will be examined by each router.
- Has same form as destination options hdr.

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):



ICMP…. Streamlined

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



Impact on Upper Layers

Upper-layer Checksums : Mandatory (even UDP)

pseudoheader	transport header	transport data

Source Address		
Destination Address		
0	Next header	Payload Length

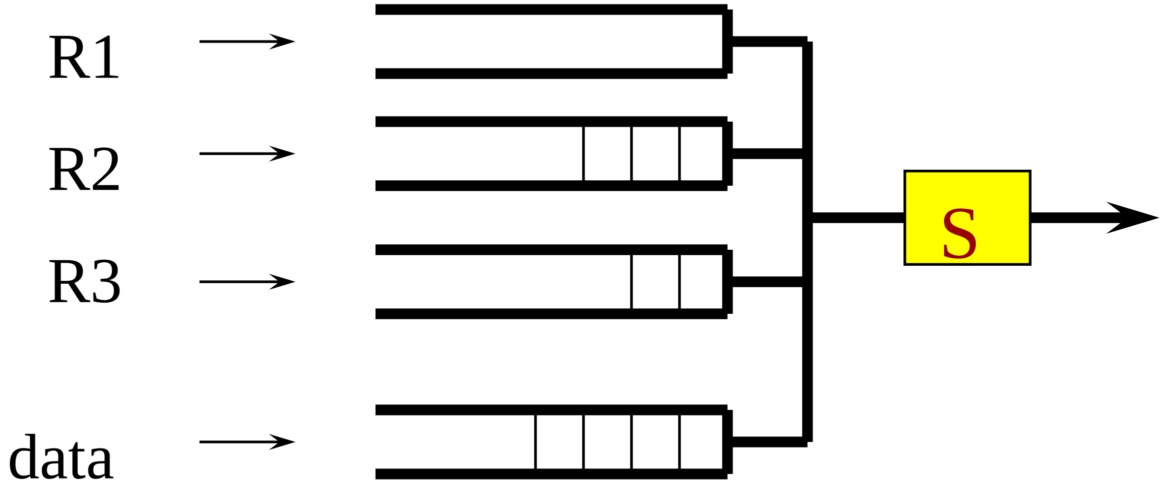
Points of Controversy

- 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.

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.

Headers

- Authentication header
  - Guarantee that the source address is authentic &
  - the packet has not been altered during transmission.
- Encryption header
  - Guarantee that only legitimate receivers
  - will be able to read the content of the packet

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.

IPv6 Addressing

- Three types of network addresses
  - 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)

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

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	000000000000000000000000000000000000000000000000000000000000	Interface-id

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

1111111011	0000000000000000000000000000000000000000	Subnet-id	Interface-id

- Site-local unicast address
  - Used to address hosts within the site only

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

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?

0000000000000000 – 80 bits – 0000000000000000	0000000000000000	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?

0000000000000000 – 80 bits – 0000000000000000	1111111111111111	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

- IP version 6 – new version of Internet Protocol, designed as successor to IP version 4.
- Improvements
  - Expanded addressing capability. IPv6 increases the address size from 32 bits to 128 bits.
  - Larger, flexible address space enable the definition of flexible, hierarchical global routing architecture with many levels.

IPv4 vs. IPv6

- Expanded Addressing Capability
  - IPv6 increase the IP address size from 32 bits to 128 bits.
  - This increases the available addresses from

    4,294,967,296

    to

    340,282,366,920,938,463,463,374,607,431,768,211,456

IPv6 Enhancements

- In a theoretical sense this is approximately 665,570,793,348,866,943,898,599 addresses per square meter of the surface of the planet Earth (assuming the earth surface is 511,263,971,197,990 square meters).
- In more practical terms the assignment and routing of addresses requires the creation of hierarchies which reduces the efficiency of the usage of the address space.
- Christian Huitema performed an analysis in which evaluated the efficiency of other addressing architecture's. Even his most pessimistic estimate this would provide 1,564 addresses for each square meter of the surface of the planet Earth.

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