IPv4 Internet

- Too many connected systems
- Too many routing tables entries
- Response time, DNS resolution time increase progressive
Motivation for Developing IPv6

- To increase the IP addressing space from 32 bits to 128 bits
- To provide permanent IP addresses, instead of using dynamic IP address assignment or network address translation (NAT)
- To provide new functions at the IP layer: source routing, QoS, auto-configuration, security, etc.

Goals of IPv6

- Support billions of hosts, even with inefficient address space allocation
- Simplify the protocol, to allow routers to process packets faster
- Provide better security than current IP
- Pay more attention to type of services, particularly for real-time data
- Aid multicasting by allowing scopes to be specified
- Make it possible for a host to roam without changing its address
- Permit the old and new protocols to coexist
What good is IPv6?

- Bigger address space
- Support for mobile devices
- Built-in security

Bigger Address Space

- The bigger address space IPv6 offers is the most obvious enhancement it has over IPv4.
- While today's Internet architecture is based on 32-bit wide addresses, the new version has 128-bit technology available for addressing.
- Allow PDA, Cell phone to connect to Internet directly
Mobility

- "Mobile IP" is one of the requirements for every IPv6 stack.
- Support for roaming between different networks, with global notification when leaving one network and entering the other one.
- Support for roaming is possible with IPv4 too, but there are a number of hoops that need to be jumped in order to get things working.
- With IPv6, there's no need for this, as support for mobility was one of the design requirements for IPv6.

Security

- IPv6 protocol stacks are required to include IPsec.
- IPsec allows authentication, encryption, and compression of IP traffic.
- Except for application-level protocols like SSL or SSH, all IP traffic between two nodes can be handled without adjusting any applications.
- All applications on a machine can benefit from encryption and authentication, and that policies can be set on a per-host (or even per-network) basis, not per application/service.
Key functions provided by IPv6

- Powerful addressing capability:
  - Able to provide addresses for every mobile handset or Information appliance (IA) on the earth
  - Can provide unicast, anycast, and multicast
  - With anycast, the IP datagram can be routed to one destination with the shortest path

- To avoid IP fragmentation:
  - All fields in IPv4 related to IP fragmentation can be reduced.
  - Using path MTU discovery, select the most appropriate MTU size
  - Provide more efficient IP routing operations
  - Easy for IPv6 core network to provide QoS control
Key functions provided by IPv6

- Flexibility for IP QoS
  - Allow flow be classified by source address + flow label
  - Allow to be mixed with RSVP (ReSerVation Protocol)
- Auto-configuration
  - Stateless autoconfiguration
  - Statefull autoconfiguration (via DHCP v6)
- Tunneling Technique
  - Can be encapsulated in an IPv4 datagram
  - Can be carried in an IPv4 tunnel: host-to-host, router-to-router, or host-to-router
  - Allow smooth migration to co-existence of IPv4 and IPv6.
Format of IPv6 packets

- IPv4 (20 – 65535 bytes)

![IPv4 header](image)

- IPv6 (40- 65535 bytes)

![IPv6 base header](image) | IPv6 header extensions (0- more)

Fixed header: 40 octets   Header Extension: 0- more

Auto-configuration in IPv6

- Stateless Autoconfiguration
  - Host generates a unique Link-local address, add it with a  64 bits physical link interface identifier
  - The address will be verified by the router
  - No server is required.

- Statefull Autoconfiguration
  - Similar to the conventional DHCP operation, but under IPv6.
  - Require a DHCP server
Fields in IPv6 headers

- **Traffic class (8 bits)**
  - Indicates the class or priority of the IPv6 packet. The Traffic Class field provides similar functionality to the IPv4 Type of Service field.

- **Flow label (20 bits)**
  - Indicates that this packet belongs to a specific sequence of packets between a source and destination, requiring special handling by intermediate IPv6 routers.
  - The Flow Label is used for non-default quality of service connections, such as those needed by real-time data (voice and video).
  - For default router handling, the Flow Label is set to 0.

Fields in IPv6 headers (Continued)

- **Payload length (16 bits)**
  - Indicates the length of the IPv6 payload.
  - The Payload Length field includes the extension headers and the upper layer PDU.
  - With 16 bits, an IPv6 payload of up to 65,535 bytes can be indicated.
  - For payload lengths greater than 65,535 bytes, the Payload Length field is set to 0 and the Jumbo Payload option is used in the Hop-by-Hop Options extension header.

- **Next header (8 bits)**
  - Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6).
  - When indicating an upper layer protocol above the Internet layer, the same values used in the IPv4 Protocol field are used here.
Fields in IPv6 headers (Continued)

- Hop Limit (8 bits)
  - Time-to-live field in IPv4
- Source address (128 bits)
- Destination address (128 bits)

A Typical IPv6 Address

- 16-byte IPv6 address written as 8 groups of 4 hexadecimal digits with colons between groups
- 8000:0000:0000:0000:0123:4567:89AB:CDEF
- Since many addresses will have many zeros inside them,
  - Leading zeros with a group can be omitted
    - 0123 → 123
  - One or more groups with 0s can be replaced by a pair of colons.
    - 8000::123:4567:89AB:CDEF
  - IPv4 addresses can be written as a pair of colons and an old dotted decimal number
    - ::192.31.20.46
IPv6 Netmask and Hostmask

- IPv6 addresses are split in two parts
  - Network part (netbits)
  - Host part (hostbits)
- IPv4’s netmask is like 255.255.255.0 format
- The netmask for an IPv6 address is in 2001:638:A01:2::/64
  - 64 is the length of the netbits
  - The netbits are referred to as the “prefix”
  - Usually 48 netbits, 16 subnetbits, and 64 hostbits

| n netbits | 128-n hostbits |

Types of IPv6 Addresses

- Unicast
- Multicast
- Anycast
Unicast

- A unicast address identifies a single interface within the scope of the type of unicast address. With the appropriate unicast routing topology, packets addressed to a unicast address are delivered to a single interface.

Unicast IPv6 Addresses

- Aggregatable global unicast addresses
- Link-local addresses
  - those that are unique on the physical link/directly attached network
- Site-local addresses
  - those that are unique to a site
- Special addresses
Aggregatable Global Unicast

- TLA ID: Top-Level Aggregation Identifier
  - Identify the highest level in the routing hierarchy
- NLA ID: Next-Level Aggregation Identifier
- SLA ID: Site-Level Aggregation Identifier
- Interface ID: Indicate the interface on a specific subnet

Link-local Addresses

- Link-local addresses, identified by the FP of 1111 1110 10, are used by nodes when communicating with neighboring nodes on the same link.
- A link-local address is always automatically configured, even in the absence of all other unicast addresses.
Site-local Addresses

- The first 48-bits are always fixed for site-local addresses, beginning with FEC0::/48.
- After the 48 fixed bits is a 16-bit subnet identifier (Subnet ID field) that provides 16 bits with which you can create subnets within your organization.

Multicast

- A multicast address identifies multiple interfaces.
- With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address.
Multicast Addresses

- 4-bit flag field
  - 1-bit for distinguishing permanent groups from transient groups
- 4-bit scope field
  - Allows a multicast to be limited to the current link, site, organization, or planet
  - 14 for planetary scope
  - 15 is available to allow future expansion

Defined Values for the Scope

<table>
<thead>
<tr>
<th>Value</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
</tr>
<tr>
<td>1</td>
<td>Node-local scope</td>
</tr>
<tr>
<td>2</td>
<td>Link-local scope</td>
</tr>
<tr>
<td>5</td>
<td>Site-local scope</td>
</tr>
<tr>
<td>8</td>
<td>Organization-local scope</td>
</tr>
<tr>
<td>E</td>
<td>Global scope</td>
</tr>
<tr>
<td>F</td>
<td>Reserved</td>
</tr>
</tbody>
</table>
Anycast

- An anycast address identifies multiple interfaces.
- With the appropriate routing topology, packets addressed to an anycast address are delivered to a single interface, the nearest interface that is identified by the address.
- The “nearest” interface is defined as being closest in terms of routing distance.
- A multicast address is used for one-to-many communication, with delivery to multiple interfaces.
- An anycast address is used for one-to-one-of-many communication, with delivery to a single interface.

Anycast Address

- Anycast identifies the “nearest,” as measured by router’s metric of distance, interface of a set of interfaces
- Anycast could be used to provide one route entry for a particular ISP with multiple links
  - The anycast address, D, identifies both A and B
  - S can send to D and will reach the nearest router, A

D – anycast destination
Anycast Address (Continued)

- At present, anycast addresses are only used as destination addresses and are only assigned to routers.

IPv6 Addresses

<table>
<thead>
<tr>
<th>Address Type</th>
<th>Prefix</th>
<th>Prefix Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0000 0000</td>
<td>1/256</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0000 0001</td>
<td>1/256</td>
</tr>
<tr>
<td>Reserved for NSAP allocation</td>
<td>0000 001</td>
<td>1/128</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0000 010</td>
<td>1/128</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0000 011</td>
<td>1/128</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0000 10</td>
<td>1/32</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0001</td>
<td>1/16</td>
</tr>
<tr>
<td>Aggregatable global unicast addresses</td>
<td>001</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>010</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>011</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>100</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>101</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>110</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1110</td>
<td>1/16</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1111 0</td>
<td>1/32</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1111 10</td>
<td>1/64</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1111 110</td>
<td>1/128</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1111 110 0</td>
<td>1/512</td>
</tr>
<tr>
<td>Link-local unicast addresses</td>
<td>1111 1110 10</td>
<td>1/1024</td>
</tr>
<tr>
<td>Site-local unicast addresses</td>
<td>1111 1110 11</td>
<td>1/1024</td>
</tr>
<tr>
<td>Multicast addresses</td>
<td>1111 1111</td>
<td>1/256</td>
</tr>
</tbody>
</table>
Link Layer Address and IPv6 address

- Link layer address is used to identify the final destination of a packet within a physical network.
- Layer 3 address is used to identify the final destination of a packet within the whole network.

Link Layer Address and IPv6 address (Continued)
Neighbor Solicitation

- This message is sent by a node to discover the link layer address of another node or to check whether another node is still reachable through the address.
- Neighbor Solicitation and Neighbor Advertisement together replace the IPv4 ARP protocol.

Neighbor Advertisement

- A Neighbor advertisement is the response to a Neighbor Solicitation message.
- A node can periodically send this message as well.
- When a node receives this type of message, it updates its Neighbor Cache, which contains the mapping between IPv6 and layer 2 addresses.
EUI64 for Hostbits

- IPv6 hostbits are recommended to be built using EUI64 addresses
- EUI64 addresses are derived from MAC addresses of the network interface
- 6-byte MAC address is filled with the "fffe" in the middle.
- As a result, the IPv6 addresses could be assigned automatically

IEEE 802 address to EUI-64 address
URL in IPv6

- 1020::8:800:200D:4567
  - http://[1020::8:800:200D:4567]:80/index.html
- fffe:3d00:f100:7031:2003::2
  - http://[ffe:3d00:f100:701:2003::2]/default.asp

How many IPv6 Addresses

- 16-byte address → $2^{128}$ different addresses
- A 128-bit address space allows for $2^{128}$ or 340,282,366,920,938,463,463,374,607,431,768,211,456 (or $3.4 \times 10^{38}$) possible addresses.
- IPv6 would allow $7 \times 10^{23}$ IPv6 addresses per square meter
- Huitema calculated there will be 1000 IPv6 addresses per square meter of the earth’s surface in the most pessimistic way.
- Only 28% of the address space has been allocated so far.
Consideration of Fragmentation

- The IPv6 takes a different approach to fragmentation
- The fields relating to fragmentation were removed
- All IPv6 conformant hosts and routers must support packets of 1280 bytes
- When a host sends a large IPv6 packet, the router that is unable to forward it sends back an error message telling the host to break up all future packets to that destination
- It is no need for routers to fragment packets on the fly

No Checksum

- IPv6 has no checksum field
- The reliable networks now are available
- Data link layer and transportation layer have their own checksums
- It seems no need to checksum of IP header
Values of the Next Header Field

<table>
<thead>
<tr>
<th>Value (in decimal)</th>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Hop-by-Hop Options Header</td>
</tr>
<tr>
<td>6</td>
<td>TCP</td>
</tr>
<tr>
<td>17</td>
<td>UDP</td>
</tr>
<tr>
<td>41</td>
<td>Encapsulated IPv6 Header</td>
</tr>
<tr>
<td>43</td>
<td>Routing Header</td>
</tr>
<tr>
<td>44</td>
<td>Fragment Header</td>
</tr>
<tr>
<td>46</td>
<td>Resource ReSerVation Protocol</td>
</tr>
<tr>
<td>50</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>51</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>58</td>
<td>ICMPv6</td>
</tr>
<tr>
<td>59</td>
<td>No next header</td>
</tr>
<tr>
<td>60</td>
<td>Destination Options Header</td>
</tr>
</tbody>
</table>

Extension Headers

- Some of the missing fields are occasionally still needed
- IPv6 introduces extension headers

<table>
<thead>
<tr>
<th>Extension header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hop-by-hop options</td>
<td>Miscellaneous information for routers</td>
</tr>
<tr>
<td>Routing</td>
<td>Full or partial route to follow</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>Management of datagram fragments</td>
</tr>
<tr>
<td>Authentication</td>
<td>Verification of the sender’s identity</td>
</tr>
<tr>
<td>Encrypted security payload</td>
<td>Information about the encrypted contents</td>
</tr>
<tr>
<td>Destination options</td>
<td>Additional information for the destination</td>
</tr>
</tbody>
</table>
### Extension Headers (Continued)

<table>
<thead>
<tr>
<th>IPv6 Header Next Header = TCP</th>
<th>TCP Header</th>
<th>Data</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IPv6 Header Next Header = Routing</th>
<th>Routing Header Next Header = TCP</th>
<th>TCP Header</th>
<th>Data</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IPv6 Header Next Header = Routing</th>
<th>Routing Header Next Header = Fragmentation</th>
<th>Fragmentation Header Next Header = TCP</th>
<th>TCP Header</th>
<th>Data</th>
</tr>
</thead>
</table>

---

### Extension Headers (Continued)

<table>
<thead>
<tr>
<th>IPv6 Header Next Header = 6 (TCP)</th>
<th>TCP Segment</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IPv6 Header Next Header = 43 (Routing)</th>
<th>Routing Header Next Header = 6 (TCP)</th>
<th>TCP Segment</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IPv6 Header Next Header = 43 (Routing)</th>
<th>Routing Header Next Header = 44 (Fragment)</th>
<th>Fragment Header Next Header = 6 (TCP)</th>
<th>TCP Segment fragment</th>
</tr>
</thead>
</table>
Hop-by-Hop Extension Header

- The 8-bit Next Header field
- The 8-bit Hdr Ext Len (Header Extension Length) field contains the length of the Hop-by-Hop Options header in 8-byte units (64 bits), not including the first 8 bytes.
- The 8-bit Option Type field contains the value 194, which indicates the Jumbo Payload option.
- The 8-bit Option Data Length field contains the value 4, which indicates that 4 bytes of data will follow—that is, the Jumbo Payload Length field.
- Jumbo payload length

Routing Header

- Routing header lists one or more routers that must be visited on the way to the destination
- Strict routing -- full path is supplied
- Loose routing -- only selected routers are supplied
Fields in Routing Header

The 8-bit Next Header field uses the same values as the field with the same name in the IPv6 header.

The 8-bit Hdr Ext Len (Header Extension Length) field contains the length of the Routing header in 8-octet (64-bit) units, not including the first 8 octets. In the case of a Type 0 Routing header, the Hdr Ext Len value must be less than or equal to 46, equal to twice the number of addresses in the header itself.

The 8-bit Routing Type field always contains, in this case, the zero value. Different values can be used in the future to support new types of Routing headers.

Fields in Routing Header (Continued)

The 8-bit Segments Left field contains the number of explicitly listed intermediate nodes still to be visited on the path to the destination— that is, the number of addresses not yet used. The maximum legal value for this field is 23.

The 24-bit Strict/Loose Bit Map field is a mask containing a Strict/Loose bit for each address.

If the Strict/Loose bit associated with an address is zero, then the address must be treated as Loose; if equal to 1, the address must be treated as Strict.
Example of Routing

Node $S$ transmits to Node $D$ by using a Routing header that forces the packet being routed through intermediate nodes $I_1$, $I_2$, and $I_3$.

As the packet travels from $S$ to $I_1$:
- Source Address = $S$
- Destination Address = $I_1$
- Hdr Ext Len = 6
- Segments Left = 3
- Address[1] = $I_2$
- (if bit 0 of the Bit Map is 1, $S$ and $I_1$ must be neighbors; this is checked by $S$)
- Address[2] = $I_3$
- Address[3] = $D$

As the packet travels from $I_1$ to $I_2$:
- Source Address = $S$
- Destination Address = $I_2$
- Hdr Ext Len = 6
- Segments Left = 2
- Address[1] = $I_1$
- (if bit 1 of the Bit Map is 1, $I_1$ and $I_2$ must be neighbors; this is checked by $I_1$)
- Address[2] = $I_3$
- Address[3] = $D$

As the packet travels from $I_2$ to $I_3$:
- Source Address = $S$
- Destination Address = $I_3$
- Hdr Ext Len = 6
- Segments Left = 1
- Address[1] = $I_1$
- (if bit 2 of the Bit Map is 1, $I_2$ and $I_3$ must be neighbors; this is checked by $I_2$)
- Address[2] = $I_2$
- Address[3] = $D$

As the packet travels from $I_3$ to $D$:
- Source Address = $S$
- Destination Address = $D$
- Hdr Ext Len = 6
- Segments Left = 0
- Address[1] = $I_1$
- (if bit 3 of the Bit Map is 1, $I_3$ and $D$ must be neighbors; this is checked by $I_3$)
- Address[2] = $I_2$
- Address[3] = $I_3$
Fragment Header

- The Fragment header is processed only by destination.
- Fragment Offset field contains the offset of the data following this header relative to the start of the original packet, in 8-octet (64-bit) units.
- The 1-bit M (More fragments) field indicates whether a fragment is the last in a packet (M = 0) or not (M = 1).
- The 32-bit Identification field contains a unique identification of the packet generated by the node.

<table>
<thead>
<tr>
<th>Next Header (8 bits)</th>
<th>Reserved (8 bits)</th>
<th>Fragment Offset (13 bits)</th>
<th>Res</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification (32 bits)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fragmentation

<table>
<thead>
<tr>
<th>Unfragmentable Part</th>
<th>Fragmentable part</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unfragmentable Part</th>
<th>Fragment Header</th>
<th>Fragment 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unfragmentable Part</td>
<td>Fragment Header</td>
<td>Fragment 2</td>
</tr>
<tr>
<td>Unfragmentable Part</td>
<td>Fragment Header</td>
<td>Fragment 3</td>
</tr>
</tbody>
</table>
Name Resolution in IPv6

- A simple table in /etc/hosts
- Network Information Service (NIS)
- Domain Name Service/System (DNS)
  - noon IN AAAA 3ffe:400:430:2:240:95ff:fe40:4385
  - /etc/named.conf
    zone "0.3.4.0.0.4.0.e.f.f.3.IP6.INT" {
      type master;
      file "db.reverse";
    };
  - db.reverse
    5.8.3.4.0.4.e.f.f.5.9.0.4.2.0.2.0.0.0 IN PTR noon.ipv6.example.com.

Differences of IPv4 and IPv6 (1/3)

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source and destination addresses are 32 bits (4 bytes) in length.</td>
<td>Source and destination addresses are 128 bits (16 bytes) in length.</td>
</tr>
<tr>
<td>IPsec support is optional.</td>
<td>IPsec support is required.</td>
</tr>
<tr>
<td>No identification of packet flow for QoS handling by routers is present within the IPv4 header.</td>
<td>Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.</td>
</tr>
<tr>
<td>Fragmentation is done by both routers and the sending host.</td>
<td>Fragmentation is not done by routers, only by the sending host.</td>
</tr>
<tr>
<td>Header includes a checksum.</td>
<td>Header does not include a checksum. For more information</td>
</tr>
</tbody>
</table>
### Differences of IPv4 and IPv6 (2/3)

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.</td>
<td>ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.</td>
</tr>
<tr>
<td>ARP Request frames are replaced with multicast Neighbor Solicitation messages.</td>
<td>ARP Request frames are replaced with multicast Neighbor Solicitation messages.</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.</td>
<td>Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.</td>
</tr>
<tr>
<td>Header includes options.</td>
<td>All optional data is moved to IPv6 extension headers</td>
</tr>
</tbody>
</table>

### Differences of IPv4 and IPv6 (3/3)

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.</td>
<td>Broadcast addresses are used to send traffic to all nodes on a subnet.</td>
</tr>
<tr>
<td>Must be configured either manually or through DHCP.</td>
<td>Must be configured either manually or through DHCP.</td>
</tr>
<tr>
<td>Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.</td>
<td>Uses pointer (PTR) resource records in the IP6.INT DNS domain to map IPv6 addresses to host names.</td>
</tr>
<tr>
<td>Must support a 576-byte packet size (possibly fragmented).</td>
<td>Must support a 1280-byte packet size (without fragmentation).</td>
</tr>
</tbody>
</table>