Internet Services and Protocols

IPv6 over IPv4

Larger address space  
New options due to the new header format  
Support for resource allocation (allocation of resources for communication between transmitter and receiver)  
Support for more security  
Support for mobility

IPv6 is 4x larger than IPv4, but the header of an IPv6 address is only 2 times larger than that of the IPv4  
IPv6 headers have one fixed header and zero or more optional (Extension) headers. All the necessary information that is essential for a router is kept in the fixed header.  
extension header contains optional information that helps routers to understand how to handle a packet/flow

Version – version no of internet protocol used (e.g. IPv4)  
IHL – Internet Header Length (length of entire IP header)  
Type of Service – DSCP – Differentiated Services Code Point; type of service. DSCP packet header value that can be used to request high priority or best effort deliver for traffic  
ECN – Explicit Congestion Notification; Carries information about congestion seen in route.  
Total Length – Length of entire datagram (including IP header and IP payload)  
Identification – If IP packet is fragmented during the transmission, all the fragments contain same identification number, to identify original IP packet they belong to.  
Flags – As required by the network resource, if IP packet is too large to handle, these flags tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to 0  
Fragment Offset – This offset tells the exact position of the fragment in the original IP Packet  
Time to Live – To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded  
Protocol – Tells the network layer at the destination host, to which protocol this packet belong to. i.e. the next level Protocol, for example protocol number of ICMP is 1, TCP is 6 and UDP is 17  
Header Checksum – This field is used to keep checksum value of entire header which is then used to check if the packet is receiver error-free.  
Source address – 32-bit address of the Sender  
Destination address – 32-bit address of the receiver

IPv6  
Version(4-bit) – Represents version of Internet Protocol  
Traffic Class (8-bits) – 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the router know what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Ntification  
Flow label(20-bits) – This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router ifentify that particular packet belongs to a specific flow of information  
Payload length (16-bit) – This field is used to tell the routers how much information a particular packet contains in its payload  
Hop Limit (8-bit) – This field is used to stop packet to loop in the netwok infinitely. This is the same as the TTL  
Source Address(128-bits) – This field is used to describe the address of the sender  
Destination Address(128-bit)

Extension Headers  
In IPv6, Fixed header contains only that much information which is necessary.  
All extra information is put between the fixed header and the upper layer header in the form of extension headers. Each extension header is identified by a distinct value.   
Following eight fields of basic IPv6 packet header are optional extension headers and the data portion of the packet.  
If present, each extension header is aligned to 64 bits. There s no fixed number of extension headers in IPv6  
Extension headers form a chain of headers.  
Each extension header is identified by the Next Header field of the previous header.

Mobility ensures in IPv6

Encapsulation creates a PDU, each PDU has a header and a message(payload)

Internet is collection of autonomous systems  
Routing inside the AS is performed by Interior Gateway Protocols IGP  
Routing between AS is performed by Exterior Gateway Protocols EGP  
IGP – RIP, EIGRP, OSPF, IS-IS  
EGP – BGP

Routing is the building of maps  
Forwarding is passing the packet to the next hop device

Link State Protocol  
Each router contains a database containing a mpa of the whole topology  
 - Links  
 - State

All routers have the same information  
All routers calculate the best path to every destination  
Any link state changes are flooded across the network   
Automatic neighbour discovery  
Each route constructs a link state packet LSP  
each router computes its best path to every destination  
On network failure new LSPs are flooded & all routers recompute routing table

Dijkstra Algorithm