IPv6 is a new version of the internetworking protocol designed to address the shortcomings of the current standard, IPv4. The address space is limited to only 32-bits in IPv4 whereas IPv6 has 128-bits address in addition to mobility constraint and network layer security. The main problem is that IPv4 and IPv6 are not directly compatible. So programs and systems designed to one standard cannot communicate with those designed to the other.

This work presents a comprehensive explanation of the various transition mechanisms and brings about the prospects of an Address Translation Technique and a Tunnel Broker Mechanism. A solution for transition mechanism which includes conversion of IPv4 to IPv6 and vice versa and a mechanism for an efficient router design is proposed. With focus to a longest prefix matching lookup algorithm, it uses a small amount of memory.

Address translation is trivial when using IPv4-mapped and IPv4-compatible IPv6 addresses. For the IPv6-to-IPv4 direction, the translator simply extracts the lower 32-bits of an IPv6 address to obtain an IPv4 address. For the opposite direction the translator sets the lower 32-bits of the IPv6 source/destination addresses to the IPv4 source/destination addresses, and sets the upper 96-bits of the IPv4 source and destination addresses to the IPv4-mapped and IPv4-compatible prefix, respectively. It is preferred to use IPv6-only addresses to refer to IPv4 nodes, which requires the translator to maintain an explicit mapping between IPv4 and IPv6 addresses.

Tunnelling mechanism is one of the mechanisms developed for managing the transition from IPv4 to IPv6 and vice versa. This mechanism will be used when two hosts that are located in two different IPv6-only zones
want to communicate with each other by passing their packets through IPv4-only zones.

This mechanism enables the island IPv6 end systems and routers to communicate through an existing IPv4 infrastructure. The tunneling mechanism encapsulates IPv6 packets in IPv4 packets and can be used by two IPv6 nodes to communicate with each other over an IPv4 network.

The address transition mechanisms are designed and implemented in Java. A virtual environment is developed for IPv4 and IPv6 network with different machines. To verify address translation, connection is established between the two different networks and communication between nodes in both the directions is made. Few analyses are carried out during runtime.

A mechanism to perform fast longest-matching-prefix route lookups in hardware in an IP router is presented here. Since the advent of Classless Inter Domain Routers (CIDR) IP routes have been identified by a <route prefix, prefix length> pair where the prefix length is between 0 and 128 bits. For every incoming packet, a search must be performed in the router’s forwarding table to determine which next hop the packet is destined for. First the set of routes with prefixes that match the beginning of the incoming IP destination address is found. Then, among this set of routes, the one with the longest prefix is selected. This is the route that is used to identify the next hop. This work is motivated by the need for faster route lookups; in particular, a fast, hardware implementable lookup algorithms is presented.

Regarding the implementation of the routing table in VLSI, the search algorithm is run on practical routing tables. This routing table VLSI design is written in VHDL code and synthesized by Xilinx and downloaded into Spartan 2E. About 1,20,000 prefixes are taken for the experiment to put into memory and consumed 750kB. The designed forwarding table is carried
out into post-layout simulation, using Active VHDL, which shows that the design correctly worked at 30 MHz. Consequently, the design furnished approximately 85 lookups/sec.

The three mobility implementing protocols are studied and compared. The purpose of the comparison is to determine which protocol will be best suited for mobility. The chosen protocols are Mobile IPv4 (MIPv4), Host Identity Payload (HIP), and Mobile IPv6 (MIPv6). To eliminate Triangular Routing, Route Optimization technique is used. During Route Optimization threats like Man-in-the Middle, Denial of Service, attack against secrecy and integrity and Flooding used to occur. In this work, these threats are eliminated and security is provided by using Return Routability mechanism. Some of the key features are compared.

The factors compared in different protocols are security, mode of operation, architecture, mobility, usability and bandwidth and so on. Addressing is 32 bits in IPv4, 128 bits in IPv6 and for HIP it depends on public key. Security is a built in feature of IPv6 and HIP is more secured than IPv4 and IPv6.

This work has presented some of the issues related to IPv6. Out of many mechanisms for transition from IPv4 to IPv6, study is made for address translation and tunneling mechanisms. Typical analysis for different scenario is a possible future work. Again performance measures of the different methods can be measured and optimization techniques can be used to pick up the best approach. Then a novel algorithm is developed for the routing table of IPv6 in VLSI. Finally the three internet protocols are compared and the key features are tabulated. Much challenges are available for the researchers in this IPv6 area for their intellectual contributions.