Hello Everyone! In this video, you will understand the IP protocol, its functions, and the IP addressing scheme.

IP stands for Internet Protocol. It is the carrier protocol of the Internet working on the IP or Network layer. It specifies the format and route of the packets, also called datagrams, and the addressing scheme used by it is called IP addressing for carrying the data across networks. IP works in coordination with UDP or TCP (Transport layer protocols) to transmit the data for various applications.

The IP packets encapsulate the TCP segments or UDP datagrams (coming from the transport layer) and flow through a number of networks(internetwork) to reach the destination.

Inspiration for the IP packet has been taken from the postal system. A postal service is a connectionless service, in which letters may be transmitted through multiple routes to reach the destination without setting up a connection between them. Here, the sender and receiver are not sure about each other's presence, as well as, the sender does not know whether the letter has reached to destination or not.

IP does not provide guaranteed services. Therefore, It's services are called Best Effort services. It means that the IP tries its best to deliver the data but with no guarantee to deliver it. No acknowledgment is sent to the sender after receiving the data on the receiver side.

Copyrighted Content

IP protocol is also media independent. It does not depend on any transmission media, it can carry data on any medium such as twisted pair cable, fiber optics, co-axial cable as well as a wireless medium. This enables IP packets to move through a long route encompassing different types of networks.

IPv4 is the current version of the IP protocol. **Let's understand the IPv4 packet header.**
As shown in the figure, different fields in an IP packet header contain various important information.
VER field is used to mention the current version of the protocol being used. IHL mentions the header length and Service type field defines the type of service, used for providing quality of service. Packet length describes the length of the IP packet. Identification, flag, and Fragment offset fields are meant for IP fragmentation, which allows IP packets to move through different networks with different MTUs where MTU stands for Maximum Transmittable Unit. The time to live field mentions the lifetime of the packet and the protocol provides the information related to transport layer protocols. Header checksum Is used for error control. The source address and destination address identify the sender and receiver machines. There are some options defined in Ipv4 to make it more usable. Padding is used for checksum calculation.

The IP addresses defined by the IPv4 protocol are used to identify the machines globally. These are 32-bit numbers represented in a dotted decimal notation by dividing the complete address into 4 eight-bit blocks and separating by

Copyrighted Content

dots. The IP Address can be divided in two parts: first part as Network ID and second as a Host ID.

Based on the first few bits, and the size of a Network ID and host ID, the IP addresses have been divided into five classes A, B, C, D, and E. These classes facilitate the management and distribution of IP addresses to various users, organizations and groups. Addresses starting with 0 and one byte of network id are class A addresses. Class B addresses start with 1 0 and have a network id of two bytes. similarly, class C starts with 1 1 0 and has 3 bytes of network id. Classes A, B and C are used to assign IP addresses to users or organizations while Class D and E do not have network id and host id distribution. Addresses from these classes have special purposes. Class D addresses, which start with 1110, are used in multicasting, while class E addresses starting with 1111 are reserved for future use.

IPv4 addresses can be unicast, multicast, or broadcast. Unicast addresses identify a single machine and allow one-to-one communication, found normally on the Internet. Multicast addresses identify a group of machines, represented by class D addresses, and allow communication from one to many. Broadcast addresses represent all the machines in a network and allow one to all communication normally used in a local area network.

Copyrighted Content

The current version of the IP protocol (version 4), which is acting as a backbone of the Internet, has some issues associated with it. Let's understand. The available IP addresses are definite and short. We are going to consume them shortly. The IPv4 has some least necessary fields which increase the load over the routers to process. The IPv4 protocol does not focus on the quality of service of the communication instead the data from an interactive communication and email is forwarded with the same priority.

To address the issues of IPv4 protocol, IPv6, the latest version of IP protocol has been developed with an improved packet header and Large size addresses for increasing the number of addresses.

IPv6 addresses are 128-bit in size, a very large number. It allows more addresses available for Internet devices. As the address size is very large, they are represented in a colon hexadecimal notation to easily manage them.

As, for IPv4 addresses, the IPv6 addresses have also been divided into three categories, but with a difference. These categories are unicast, multicast, and anycast.

A unicast address uniquely identifies an interface of an IPv6 node. A packet sent to a unicast address is delivered to the interface identified by that address. A multicast address

Copyrighted Content

identifies a group of IPv6 interfaces. A packet sent to a multicast address is processed by all members of the multicast group. An anycast address is assigned to multiple interfaces. A packet sent to an anycast address is delivered to only one of these interfaces, usually the nearest one.

Let's discuss the improved header of the IPv6 protocol. In this header, the fields like header length, fields related to fragmentation, etc. have been removed to make it smaller in size. Version, payload length, and hop limit have usual meanings and traffic class and flow label are used for providing various quality of service to various applications. In TCP the base header contains only the mandatory information required for communication. The rest of the optional functionality has been represented as extension headers. The next header field points to the next header being carried by the IP packet or behaves in a similar way as a protocol in IPv4 if no extension header is available. The source address and destination address are 128 bits each, representing the sender and receiver of the packet.

Ipv4 and IPv6 protocols have various differences between them. Let's understand them. IPv4 came in 1981, fully deployed now while IPv6 has been introduced in 1998, and is still in the deployment phase. IPv4 addresses are 32-bit while IPv6 addresses are 128-bit in length. IPv6 has a very large address base compared to ipv4.IPv4 addresses are represented in dotted decimal notation, while IPv6 addresses are represented in colon hexadecimal notation.

Copyrighted Content

IPv4 addresses are configured manually by the administrator or DHCP protocol, while IPv6 allow machines to auto configure themselves by creating their own IP addresses.

Thank You.

Copyrighted Content