the ISP's service is provided. Now a point-to-point physical connection is established but to transmit independent IP packets necessary data link layer functions have to be implemented.

IP packets are transmitted every now and then and in the meantime errors on the line could be interpreted as IP packets if no framing and error control is implemented. To solve this problem, PPP uses the data link layer protocol, called *Link Control Protocol* (LCP), which performs framing of IP packets and error control. LCP also defines a negotiation mechanism, which is used in the beginning and end of the data link layer connection. End systems may, for example, agree to use frame numbering, acknowledgments and retransmission for error recovery. They are needed in wireless connections but not typically used in PSTN or ISDN connections.

Another problem is that the user's computer has no permanent IP address and before any communications an address has to be assigned. Typically each ISP has a much smaller number of IP addresses than customers. For dynamic IP address assignment, a Network Control Protocol (NCP) is used after data link layer connection is established by LCP. NCP assigns one of the ISP's IP addresses for the customer at the beginning of the connection and releases it at the end [3].

6.6.4 Internet Protocol

The IP is the core protocol of the Internet. It provides a service for the transfer of data units, datagrams, between the host computer and the router as well as between routers. At the IP level, each datagram is handled as a separate transfer and not as part of a larger data set.

The main task of the IP layer is addressing, which requires global Internet addresses, and routing of the IP packets from the source computer to their destination via a number of interconnected networks. The basic network elements in the IP network are routers and permanently connected computers (hosts) with different application protocols that provide services for Internet users. Each such element has at least one Internet address. They are different from the addresses used in the PSTN. The Internet addresses are global and their usage is internationally controlled by the NIC.

6.6.4.1 IP Addresses

Every host and router in the Internet has a unique fixed-length IP address, that defines the network and the host. No two machines connected to the global Internet have the same IP address. All IP addresses are 32 bits long and are used in source and destination address fields of IP packets. Figure 6.38 shows the format of an IP address.

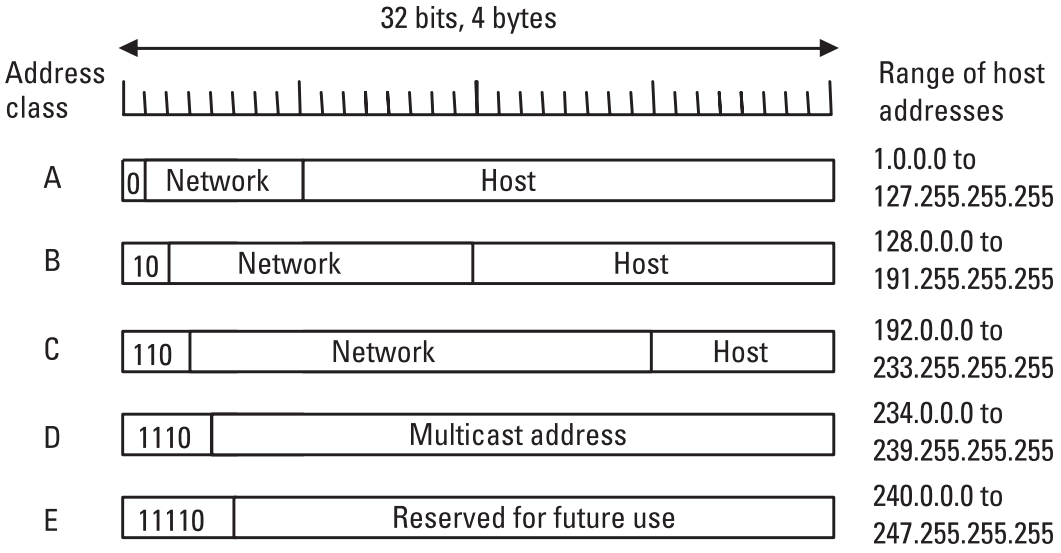

Figure 6.38 IP address format (IPv4).

Machines connected to multiple networks have different addresses on each network [3]. NIC assigns the network part, and the administrator of each network assigns the host part of addresses. IP addresses, which are 32-bit numbers, are usually written in dotted decimal notation as shown in Figure 6.38. For example, class C binary address 11000000 00101001 00000111 00110100, which is in hexadecimal form C0290734, is written as 192.41.7.52. Some addresses, such as lowest 0.0.0.0 and highest 255.255.255.255, have special uses, as shown in Figure 6.39 [3, 4]. Because

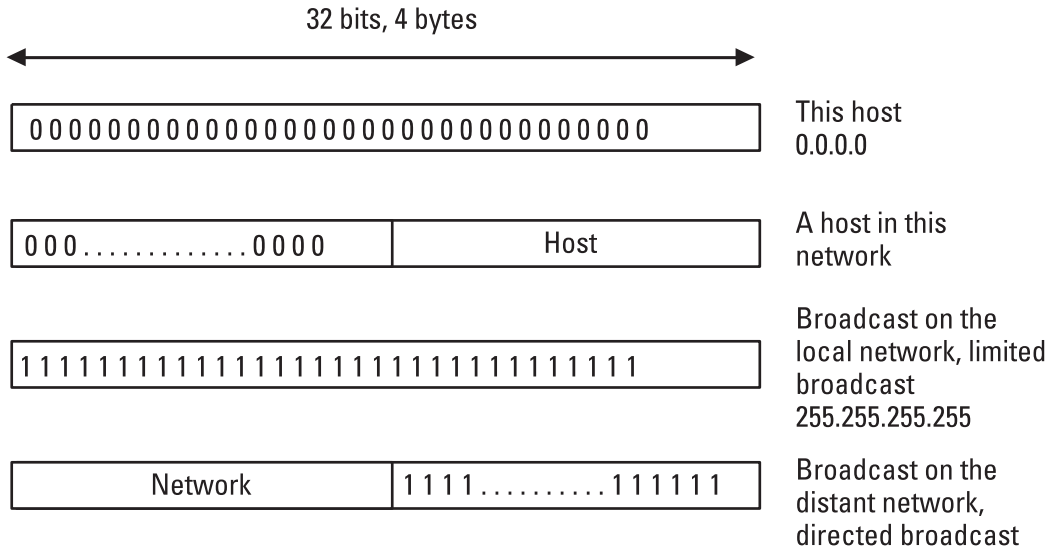

Figure 6.39 Special IP addresses.

of special use of all zero and all ones addresses a host address, where all bits in the host part are either zero or one, must not be used.

The IP address 0.0.0.0 is used by hosts being booted, but not afterward. IP addresses for later use may be assigned by the network for the host while it is booted. An address where all bits in the network part are zero refers to the current network, typically a LAN. All hosts in the network receive the IP packet with address consisting of all 1's. If only the host part is all 1's the packet is received by all hosts in the network identified by the network address.

6.6.4.2 Subnetworks

As seen earlier, all hosts in the network must have the same network number. A company that has one class C can have up to 254 hosts in its network and the use of these addresses have to be controlled over whole network, which may consist of multiple LANs. This could become a serious headache for network managers as the network grows and hosts are added and relocated. For easier management, a network can be divided into subnets so that a company's network still acts like a single network to the outside world. The network manager can decide to use, for example, two first digits in the host address section as a subnet address, as shown in Figure 6.40.

Now he or she may divide his or her network into four subnets, each containing up to 62 (0 and 63 are not used) hosts. If, for example, the class C network address is 221.109.65.0, the hosts are numbered from 1 to 254 (excluding 0 and 255). The 2 bits in Figure 6.40 identify four subnets and their host address ranges are 1 to 63. With subnet digits a whole 8-bit host part has values 1 to 63 (subnet 0), 65 to 127 (subnet 1), 129 to 191 (subnet 2), and

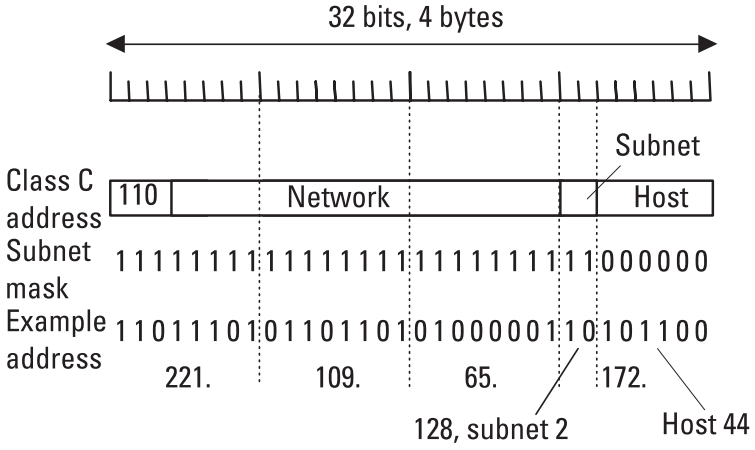

Figure 6.40 Example of subnet and subnet mask.

193 to 254 (subnet 3). Actually a few more addresses could be used without including hosts with all host part bits 0's or 1's, for example, 64 in subnet 1. However, in practice, it is probably better to follow the same addressing principles in all subnetworks. From the outside world, IP packets are routed with the help of a network number section and it is a matter for the company's internal staff to determine how host numbers are divided into subnets.

When an IP packet arrives at the router, it detects the address class from the first digits to see what section in the address represents the network. If it identifies its own network, the packet is forwarded to the host identified by the host part; otherwise, it is forwarded to the next router according to the stored routing table. If subnets are implemented, a subnet mask (shown in Figure 6.40) is defined and stored in the router. Now the received packet contains the router's network address and it performs a Boolean AND operation with the subnet mask to get rid of the host section. In our example, the result of this operation could give subnet address 221.109.65.0, 221.109.65.64, 221.109.65.128, or 221.109.65.192. This address is then looked up in the routing tables to find out how to get to hosts in a given subnet. The example address in Figure 6.40 is 221.109.65.172, which gives subnet address 112.109.65.128 as a result of an AND operation with a subnet mask and this indicates that the destination host is located in subnet 2.

Classless interdomain routing (CIDR) is a technique that divides network addresses into smaller address ranges in the same way subnets are divided as explained earlier. With the help of CIDR, for example, an ISP can split up its address range for assignment to its customers. For example, CIDR notation 128.211.176.112/30 defines a subnet mask of 30 bits and a four-address block with highest address 128.211.176.115.

6.6.4.3 IP Header

Each IP packet contains a header, as shown in Figure 6.41. *Version* specifies the IP protocol version being used, in this case, version 4. The *Internet header length* (IHL) specifies header length as a number of 32-bit words. The minimum value of IHL is 5 and the maximum is 15. With the *type of service* field the host may specify the datagram priority. It also contains flag bits D (Delay), T (Throughput), and R (Reliability), which the host can set to 1 to indicate about which feature it cares most. In practice, most routers ignore the type of service field altogether.

The *total length* field tells the length of the IP packet including the header and user data. It gives the total number of bytes or octets and its maximum value is 65,535 bytes. The IP layer may divide long datagrams into shorter fragments, which is necessary, for example, when the data are