TCP/IP-1

The Internet Protocol (IP) enables communications across a vast and heterogeneous collection of networks that are based on different technologies. Any host computer that is connected to the Internet can communicate with any other computer that is also connected to the Internet. The Internet therefore offers ubiquitous connectivity and the economies of scale that result from large deployment.

The Internet offers two basic communication services that operate on top of IP: Transmission control protocol (TCP) reliable stream service and user datagram protocol (UDP) datagram service. Any application layer protocol that operates on top of either TCP or UDP automatically operates across the Internet. Therefore the Internet provides a ubiquitous platform for the deployment of network-based services.

3.1 THE TCP/IP ARCHITECTURE

The TCP/IP protocol suite usually refers not only to the two most well-known protocols called the Transmission Control Protocol (TCP) and the Internet Protocol (IP) but also to other related protocols such as the User Datagram Protocol (UDP), the Internet Control Message Protocol (ICMP) and the basic applications such as HTTP, TELNET, and FTP. The basic structure of the TCP/IP protocol suite is shown in Figure 3 .1. Application layer protocols such as SNMP and DNS send their messages using UDP. The PDUs exchanged by the peer TCP protocols are called TCP segments or segments, while those exchanged by UDP protocols are called UDP datagrams or datagrams. IP multiplexes TCP segments and UDP datagrams and performs fragmentation, if necessary, among other tasks to be discussed below. The protocol data units exchanged by IP protocols are called IP packets or packets.[1] IP packets are sent to the network interface for delivery across the physical network. At the receiver, packets passed up by the network interface are demultiplexed to the appropriate protocol (IP, ARP, or RARP). The receiving IP entity needs to determine whether a packet has to be sent to TCP or UDP. Finally, TCP (UDP) sends each segment (datagram) to the appropriate application based on the port number. The physical network can be implemented by a variety of technologies such as Ethernet, token ring, ATM, PPP over various transmission systems, and others.

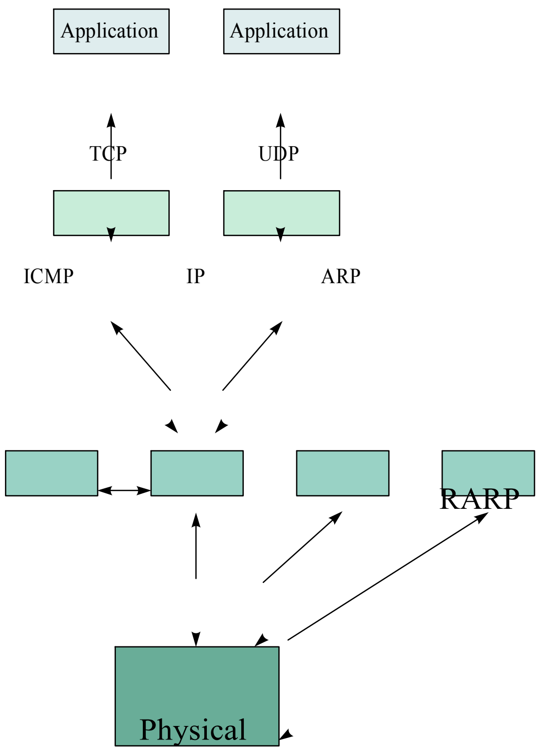


FIGURE 3.1 TCP/IP protocol suite

The PDU of a given layer is encapsulated in a PDU of the layer below as shown in Figure 8.2. In this figure an HTTP GET command is passed to the TCP layer, which encapsulates the message into a TCP segment. The segment header contains an ephemeral port number for the client process and the well-known port 80 for the HTTP server process. The TCP segment in turn is passed to the IP layer where it is encapsulated in an IP packet. The IP packet header contains an IP network address for the sender and an IP network address for the destination. IP network addresses are said to be logical because they are defined in terms of the logical topology of the routers and end systems. The IP packet is then passed through the network interface and encapsulated into a PDU of the underlying network. In Figure 2.2 the IP packet is encapsulated into an Ethernet LAN frame. The frame header contains physical addresses that identify the physical endpoints for the sender and the receiver. The logical IP addresses need to be converted into specific physical addresses to carry out the transfer of bits from one device to the other. This conversion is done by an address resolution protocol.

Each host in the Internet is identified by a globally unique IP address. An IP address is divided into two parts: a network ID and a host ID. The network ID

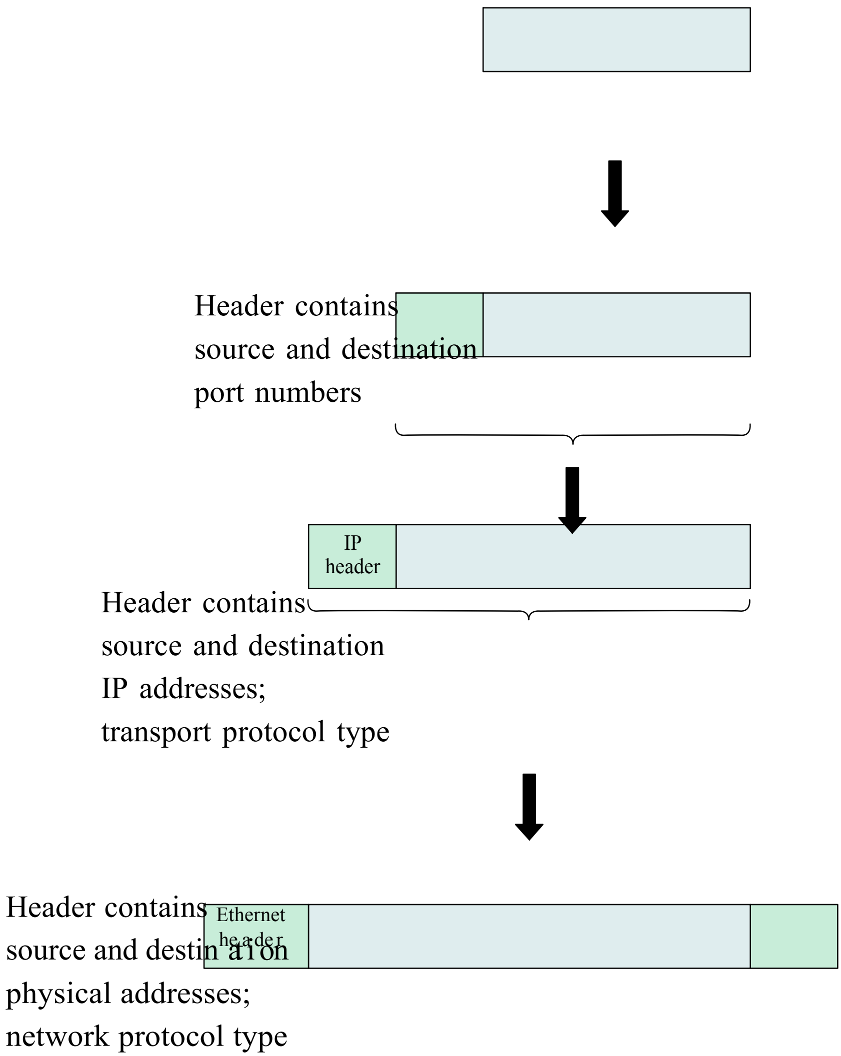


FIGURE 3.2 Encapsulation of PDUs in TCP/IP and addressing information in the headers

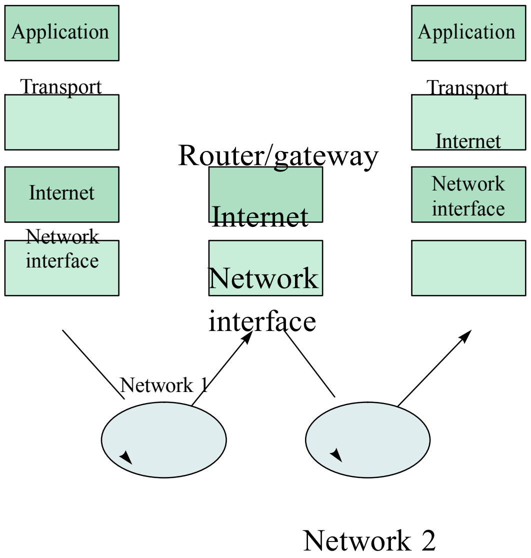
must be obtained from an organization authorized to issue IP addresses. The Internet layer provides for the transfer of information across multiple networks through the use of routers, as shown in Figure 2.3. The Internet layer provides a single service, namely, best-effort connectionless packet transfer. IP packets are exchanged between routers without a connection setup; they are routed indepen- dently, and may traverse different paths. The gateways that interconnect the intermediate networks may discard packets when they encounter congestion. The responsibility for recovery from these losses is passed on to the transport layer.

The network interface layer is particularly concerned with the protocols that are used to access the intermediate networks. At each gateway the network protocol is used to encapsulate the IP packet into a packet or frame of the underlying network or link. The IP packet is recovered at the exit router of the given network. This router must determine the next hop in the route to the destination and then encapsulate the IP packet or frame of the type of the next network or link. This approach provides a clear separation of the Internet layer from the technology-dependent network interface layer. This approach also allows the Internet layer to provide a data transfer service that is transparent in the sense of not depending on the details of the underlying networks. Different network technologies impose different limits on the size of the blocks that they can handle. IP must accommodate the maximum transmission unit of an under-

lying network or link by implementing segmentation and reassembly as needed.

To enhance the scalability of the routing algorithms and to control the size of the routing tables, additional levels of hierarchy are introduced in the IP

FIGURE 3.3 The Internet and network interface layers



addresses. Within a domain the host address is further subdivided into a subnet- work part and an associated host part. This system facilitates routing within a domain, yet can remain transparent to the outside world. At the other extreme, addresses of multiple domains can be aggregated to create supernets.

Source : http://elearningatria.files.wordpress.com/2013/10/cse-vi-computer-networks-ii-10cs64-notes.pdf