# NETWORK-LAYER PROTOCOLS

## INTERNET PROTOCOL (IP)

The protocol, Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer. IP layer position is shown in figure 2.7.1.

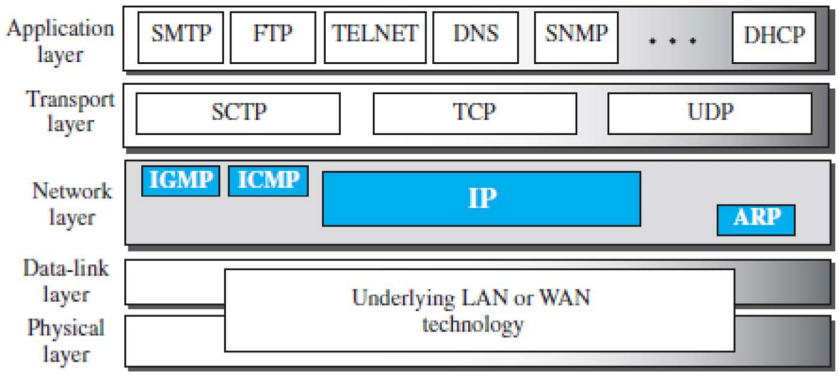


**Fig2.7.1: Position of IP and other layers .**

*[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-562]*

IPv4 is also a connectionless protocol that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order.

### Datagram Format

Packets used by the IP are called datagrams.

Figure 2.7.2 shows the IPv4 datagram format. A datagram is a variable length packet consisting of two parts: header and payload (data). The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

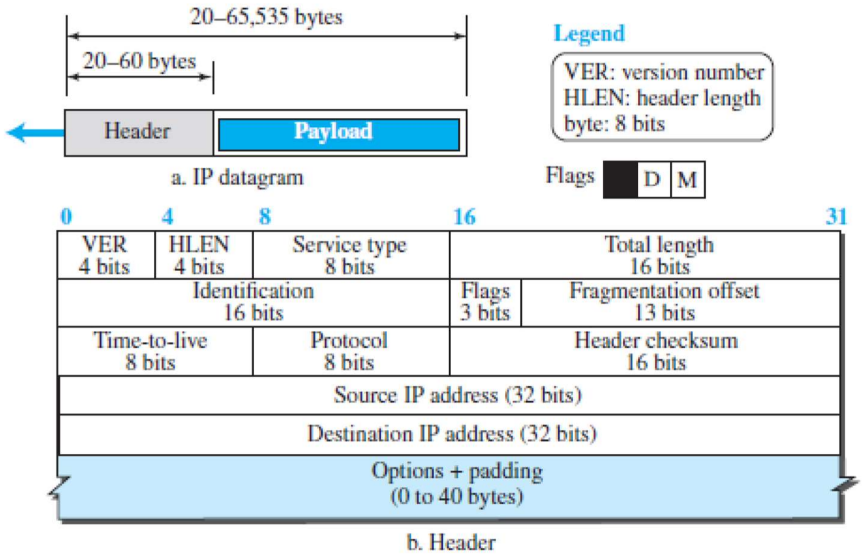


**Fig2.7.2: IP datagram.**

*[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-563]*

Version Number.The 4-bit version number (VER) field defines the version of theIPv4 protocol, which, has the value of 4.

Header Length.The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header.

Service Type. This field is called as type of service (TOS), which defined how the datagram should be handled.

Total Length.This 16-bit field defines the total length (header plus data) of the IP datagram in bytes. A 16-bit number can define a total length of up to 65,535 (when all bits are 1s).

Identification, Flags, and Fragmentation Offset. These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.

Time-to-live.Due to some malfunctioning of routing protocols a datagram may be circulating in the Internet, visiting some networks over and over without reaching the destination.

This may create extra traffic in the Internet.

The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram.

Protocol.In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol.

A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP. A datagram can also carry a packet from other protocols that directly use the service of the IP.

Header check sum.IP is not a reliable protocol; it does not check whether the payload carried by a datagram is corrupted during the transmission. IP puts the burden of error checking of the payload on the protocol that owns the payload, such as UDP or TCP. The datagram header, is added by IP, and its error-checking is the responsibility of IP.

Errors in the IP header can be a disaster. For example, if the destination IP address is corrupted, the packet can be delivered to the wrong host.

If the protocol field is corrupted, the payload may be delivered to the wrong protocol. If the fields related to the fragmentation are corrupted, the datagram cannot be reassembled correctly at the destination.

**Source and Destination Addresses.**

The 32-bit source and destination address fields define the IP address of the source and destination respectively.The source host should know its IP address. The destination IP address is either known by the protocol that uses the service of IP or is provided by the DNS.

Options.A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging.

Payload. Payload, or data, is the main reason for creating a datagram.

Payload is the packet coming from other protocols that use the service of IP.Comparing a datagram to a postal package, payload is the content of the package. In order to make the IP protocol independent of the physical network, the designers decided to make the maximum length of the IP datagram equal to 65,535 bytes. For physical networks, we must divide the datagram to make it possible for it to pass through these networks. This is called fragmentation.

When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed.A datagram can be fragmented by the source host or any router in the path. The Reassembly of the datagram, however, is done only by the destination host, because each fragment becomes an independent datagram.

The fragmented datagram can travel through different routes, and we can never control or guarantee which route a fragmented datagram may take, all of the fragments belonging to the same datagram should finally arrive at the destination host.

Three fields in an IP datagram are related to fragmentation: identification, flags, and fragmentation offset.

The 16-bit identification field identifies a datagram originating from the source host. The combination of the identification and source IP address must uniquely define a datagram as it leaves the source host.To guarantee uniqueness, the IP protocol uses a counter to label the datagrams. The counter is initialized to a positive number.

When the IP protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by one. As long as the counter is kept in the main memory, uniqueness is guaranteed.

When a datagram is fragmented,the value in the identification field is copied into all fragments. In other words, all fragments have the same identification number, which is also the same as the original datagram. The identification number helps the destination in reassembling the datagram.

Note: All fragments having the same identification value should be assembled into one datagram.

**The 3-bit flags field defines three flags.**

The leftmost bit is reserved (not used). The second bit (D bit) is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram.If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host .If its value is 0, the datagram can be fragmented if necessary. The third bit (M bit) is called the more fragment bit.If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment.

---

## MOBILE IP

Mobile IP is the extension of IP protocol that allows mobile computers to be connected to the internet at any location where the connection is possible.

**Stationary Hosts**

The original IP addressing was based on the assumption that a host is stationary, attached to one specific network. A router uses an IP address to route an IP datagram. For example, the IP address 10.3.4.24/8 defines a host attached to the network 10.0.0.0/8. This implies that a host in the Internet does not have an address that it can carry with itself from one place to another.

The address is valid only when the host is attached to the network. If the network changes, the address is no longer valid. Routers use this association to route a packet; they use the prefix to

deliver the packet to the network to which the host is attached. This scheme works perfectly with stationary hosts.

**Mobile Hosts**

When a host moves from one network to another, the IP addressing structure needs to be modified.

**Changing the Address**

One simple solution is to let the mobile host change its address as it goes to the new network. The host can use DHCP to obtain a new address to associate it with the new network. This approach has several drawbacks. First, the configuration files would need to be changed. Second, each time the computer moves from one network to another, it must be rebooted. Third, the DNS tables need to be revised so that every other host in the Internet is aware of the change. Fourth, if the host roams from one network to another during a transmission, the data exchange will be interrupted. This is because the ports and IP addresses of the client and the server must remain constant for the duration of the connection.

**Two Addresses**

The approach that is more feasible is the use of two addresses. The host has its original address, called the **home address,** and a temporary address, called the **care-of address.** The home address is permanent; it associates the host with its home network, the network that is the permanent home of the host. The care-of address is temporary. When a host moves from one network to another, the care-of address changes; it is associated with the foreign network, the network to which the host moves. Figure 2.7.3 shows the concept.

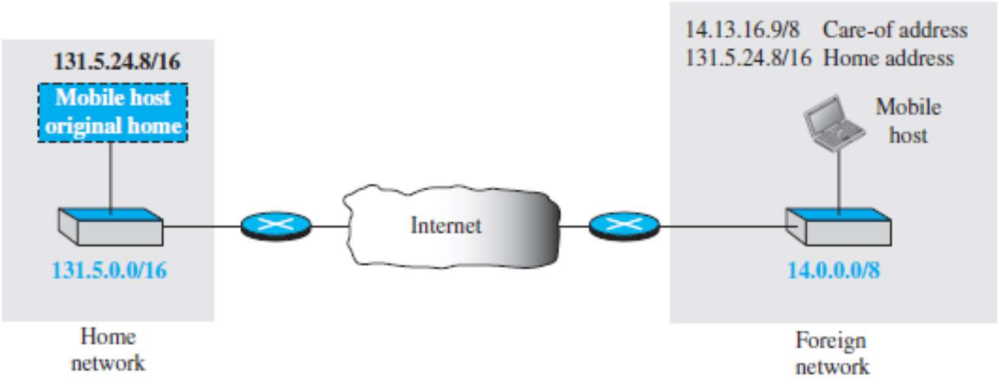


**Fig2.7.3: Home address and care-of address**

*[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-582]*

# ICMP

The Internet Control Message Protocol version 4 (ICMPv4) is a network-layer protocol.

When an IP datagram encapsulates an ICMP message, the value of the protocol field in the IP datagram is set to 1 to indicate that the IP payroll is an ICMP message.

ICMP messages are divided into two categories: error-reporting messages and query messages.

The error-reporting messages report problems that a router or a host(destination) may encounter when it processes an IP packet.

The query messages, help a host or a network manager get specific information from a router or another host.

For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages. An ICMP message has an 8-byte header and a variable-size data section. The first 4 bytes are common to all. The first field, ICMP type, defines the type of the message.The code field specifies the reason for the particular message type. The last common field is the checksum field.

**Error Reporting Messages**

One of the main responsibilities of ICMP is to report some errors that may occur during the processing of the IP datagram. ICMP does not correct errors, it simply reports them. Error correction is done by the higher-level protocols.The format is shown in figure 2.7.4.

Error messages are always sent to the original source because the only information available in the datagram about the route is the source and destination IP addresses. ICMP uses the source IP address to send the error message to the source (originator) of the datagram. To make the error-reporting process simple, ICMP follows some rules in reporting messages.

First, no error message will be generated for a datagram having a multicast address or special address (such as this host or loopback).Second, no ICMP error message will be generated in response to a datagram carrying an ICMP error message.Third, no ICMP error message will be generated for a fragmented datagram that is not the first fragment.

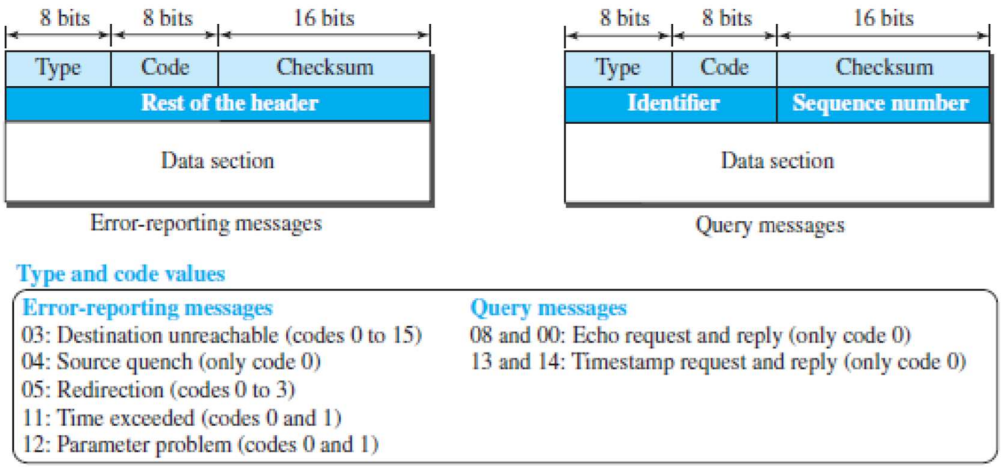


**Fig2.7.4: The format of ICMP messages.**

*[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-575]*

Note that all error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram.

The original datagram header is added to give the original source, which receives the error message,information about the datagram itself.

The 8 bytes of data are included because the first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP). This information is needed so the source can inform the protocols (TCPor UDP) about the error. Data field is shown in figure 2.7.5.

Destination Unreachable

The most widely used error message is the destination unreachable (type 3). This message uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination.

For example, code 0 tells the source that a host is unreachable.

This may happen, for example, when we use the HTTP protocol to access a web page, but the server is down. The message "destination host is not reachable" is created and sent back to the source.

Source Quench

Source quench (type 4) message informs the sender, that the network has encountered congestion and the datagram has been dropped; the source needs to slow down sending more datagrams.

Redirection Message

The redirection message (type 5) is used when the source uses a wrong router to send out its message.

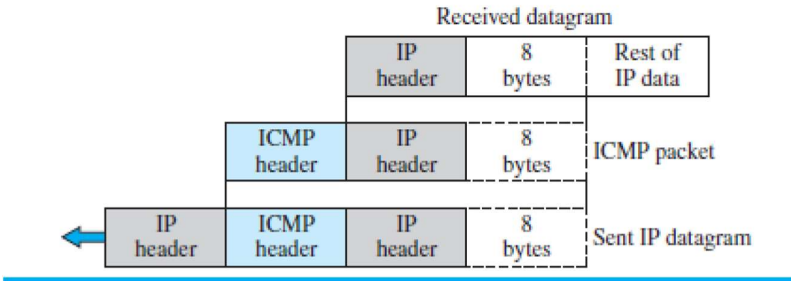


**Fig2.7.5: The Contents of data field.**

*[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-577]*

The router redirects the message to the appropriate router, but informs the source that it needs to change its default router in the future. The IP address of the default router is sent in the message.

**Parameter Problem**

A parameter problem message (type 12) can be sent when either there is a problem inthe header of a datagram (code 0) or some options are missing or cannot be interpreted(code 1).

Query Messages

Query messages in ICMP can be used independently without relation to an IP datagram. A query message needs to be encapsulated in a datagram, as a carrier.

Query messages are used to test the liveliness of hosts or routers inthe Internet, find the one-way or the round-trip time for an IP datagram between two devices, or even find out whether the clocks in two devices are synchronized.

**Query messages pairs: request and reply.**

The echo request (type 8) and the echo reply (type 0) pair of messages are used bya host or a router to test the liveliness of another host or router.

A host or router sends an echo request message to another host or router; if the latter is alive, it responds with an echo reply message.

The timestamp request (type 13) and the timestamp reply (type 14) pair of messages are used to find the round-trip time between two devices or to check whether the clocks in two devices are synchronized.The timestamp request message sends a 32-bitnumber, which defines the time the message is sent. The timestamp reply resends that number, and includes two new 32-bit numbers representing the time the request was received and the time the response was sent.

**Deprecated Messages**

Three pairs of messages are declared obsolete by IETF:

Information request and replay messages are not used today because their duties are done by the Address Resolution Protocol (ARP).

Address mask request and reply messages are not used today because their duties are done by the Dynamic Host Configuration Protocol (DHCP).

Router solicitation and advertisement messages are not used today because their duties are done by the Dynamic Host Configuration Protocol (DHCP).

---