Module 7

Internet And Internet Protocol Suite

Lesson

22

IP addressing. ICMP

LESSON OBJECTIVE

General

The lesson will continue the discussion on IPv4 along with the idea of ICMP.

Specific

The focus areas of this lesson are:

1. Addressing scheme in IPv4.
2. Importance of ICMP
3. Message types in ICMP
4. ICMP header.
5. ARP & RARP

7.2.1. IP ADDRESSING

Every host and router on the internet has an IP address, which encodes its network number and host number. The combination is unique: no two machines have the same IP address. All IP addresses are 32 bits long and are used in the source and destination address fields of the IP packets. This machines connected to multiple networks have a different IP address on each network. The class A, B, C and D formats allow for up to 126 networks with 16 million hosts each, 16,382 networks with up to 60k hosts, 2 million networks with up to 254 hosts each and multicast in which the datagram is directed to multiple hosts. Class E addresses beginning with 11110 are reserved for future use. Tens of thousands of networks are connected to the internet, and these networks are assigned a number by the Network Information Center (NIC), to avoid conflicts. 32 bit network addresses are usually written in dotted decimal notation. In this format each of the four bytes is written in decimal from 0 to 255. The lowest address is 0.0.0.0 and the highest address is 255.255.255.255.The values 0 and -1 have special meanings. The value 0 means this network or this host. The value -1 is used as a broadcast address to mean all hosts on the indicated network.

Fig 5.47 page number 416 Tannenbaum

7.2.2 INTERNET CONTROL MESSAGE PROTOCOL

IP provides unreliable connectionless datagram service, original aim being efficient use of network resources. IP being a best effort delivery service lacks error control and assistance mechanisms.

What happens if something goes wrong? What happens if a router must discard a datagram because it cannot find a router to the final destination or because the time-to-live field has a zero value? These are examples where IP has no built-in mechanism to notify the original host. There are may other situation where IP is found lacking.

The internet control message protocol (ICMP) has been designed to take care of the above deficiencies. It is a companion to IP. ICMP in spite of being a network layer protocol does not pass messages directly to the datalink layer. Instead the messages are first encapsulated inside IP datagrams whose protocol field is set to 1.

Types of messages

ICMP messages are divided into two broad categories:

1. Error reporting Messages.
2. Query Messages.

1. Error reporting:

ICMP was designed to compensate the shortcoming of unreliability in IP. However ICMP does not correct errors, but only reports them. Error reporting messages are always sent to the original source. Five types of errors are handled:

Destination unreachable—In situations where a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or host sends a *destination unreachable* message back to the source.

Source Quench—IP being a connectionless protocol, there is no communication between the source host, the router and the destination host. The resulting lack of flow control is a major hazard in the operation of source-destination delivery. And the lack of congestion control causes major problems n the routers. The *source quench* message in ICMP adds some flow control and congestion control to IP by notifying the source of a datagram being discarded and forcing it to slow down its transmission.

Time Exceeded—It is generated in two cases

a. A router receives a datagram with a zero value in the TTL field
b. All fragments that make up a message do not arrive at the destination host within a certain time limit

Parameter Problem—If a router or a destination host discovers an ambiguous or missing value in a any field of the datagram, it discards the datagram and sends a *parameter problem* message back to the source.

Redirection—When a host comes up, its routing table has a limited number of entries. It usually knows the IP address of a single default router. For this reason the host may send a datagram to the wrong router. The router that receives the datagram will forward it to the correct router and will send a redirection message back to the host for routing table updating.

2. **Query Messages:**

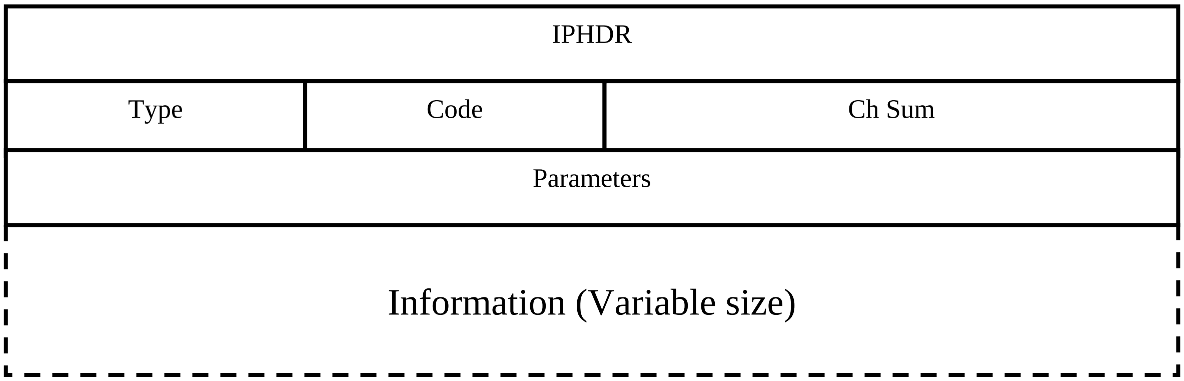
Query messages are used to diagnose some network problems. There are four different pairs of messages.

Echo Request/Reply messages—are designed for diagnostic purposes. Their combination determines whether two systems can communicate with each other.

Time stamp Request/Reply messages—can be used to determine the round trip time for an IP datagram to travel between two machines and also to synchronize the clocks in them.

Address mask Request/Reply message—are used between the host and the router to indicate which part of the address defines the network and the sub-network address and which part corresponds to the host identifier.

Router Solicitation and Advertisement—are useful to inform a host that wants to send data to a host on another network, the address of routers connected to its own network and also their status and functioning.



Type	Specifies the types of errors, generally 256 types of errors may occur
: Code	Parameters that can be coded in a few bits.
Checksum	Checksum of entire IP message
Parameters	Specifies more lengthy parameters.

Address resolution protocol

Although every machine on the Internet has its IP address, these cannot be actually used for sending packets because the data link layer hardware does not understand IP addresses. Thus it is very important to understand the mapping of IP addresses onto datalink layer addresses, such as Ethernet.

Assuming the sender knows the name of the intended receiver, the first step is to find the IP address for it, which is done by the Domain Name System. The upper layer software in the sender now builds a packet with the receiver’s address in the destination field and gives it to IP software to transmit. The IP software needs a way to find the destination’s Ethernet address even if the destination is on its own network. To do this, it can have a configuration file somewhere in the system that maps IP addresses onto Ethernet addresses. Otherwise, the sender outputs a broadcast packet onto the Ethernet asking about the owner of that particular IP address. On receiving that packet, each machine will check its IP address and only the correct user will respond. The protocol for asking the question and getting the reply is called ARP (Address Resolution Protocol). Almost every machine on the Internet runs it. Its advantage over the configuration files is simplicity. The system manager does not do much except assign each machine an IP address and decide subnet masks. ARP does the rest.

Reverse Address resolution protocol

RARP does the reverse of ARP, i.e. it helps to find a corresponding IP address given an Ethernet address. This protocol allows a newly-booted workstation to broadcast its Ethernet address enquiring about its IP address. The RARP server sees this request, looks up the Ethernet address in its configuration files, and sends back the corresponding IP address. It is better than embedding an IP address in the memory image because it allows the same image to be used an all machines. And its disadvantage is that it uses a destination address of all 1s (limited broadcasting) to reach the RARP server.

Objective Questions

22.01 All IP addresses are ____ bits long.

22.02 ___________________ assigns a number to networks connected to Internet to avoid conflict.

22.03 Error reporting messages are always sent to the source. (*True/False*)

22.04 There are ______ types of error reporting messages and ____ different pairs of query messages.

22.05 The protocol for asking the question and getting the reply is called ____________.

Subjective Questions

22.11 Discuss the addressing scheme in IP.

22.12 Why was ICMP needed?

22.13 Enlist the error reporting messages.

22.14 Describe the query messages.

22.15 Discuss ARP and RARP protocols.

Level 2 Questions

22.21