TCP/IP-(18MCA45E)

UNIT-I

‘ARP & RARP’

FACULTY:

Dr. R. A. Roseline, M.Sc., M.Phil., Ph.D.,

Associate Professor and Head,

Post Graduate and Research Department of Computer Applications,

Government Arts College (Autonomous), Coimbatore – 641 018.

ARP & RARP

ARP:

- Address Resolution Protocol(ARP)
- ARP is a protocol used by the Internet Protocol (IP) [RFC826], to map IP network addresses to the hardware addresses used by a data link protocol. ... The hardware address is also known as the Medium Access Control (MAC) address, in reference to the standards which define Ethernet.

RARP:

- RARP is abbreviation of Reverse Address Resolution Protocol which is a protocol based on computer networking which is employed by a client computer to request its IP address from a gateway server's Address Resolution Protocol table or cache.
- The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

Proxy ARP

- Proxy ARP is a technique by which a proxy device on a given network answers the ARP queries for an IP address that is not on that network. The proxy is aware of the location of the traffic's destination, and offers its own MAC address as the (ostensibly final) destination.

Advantages of Proxy ARP:

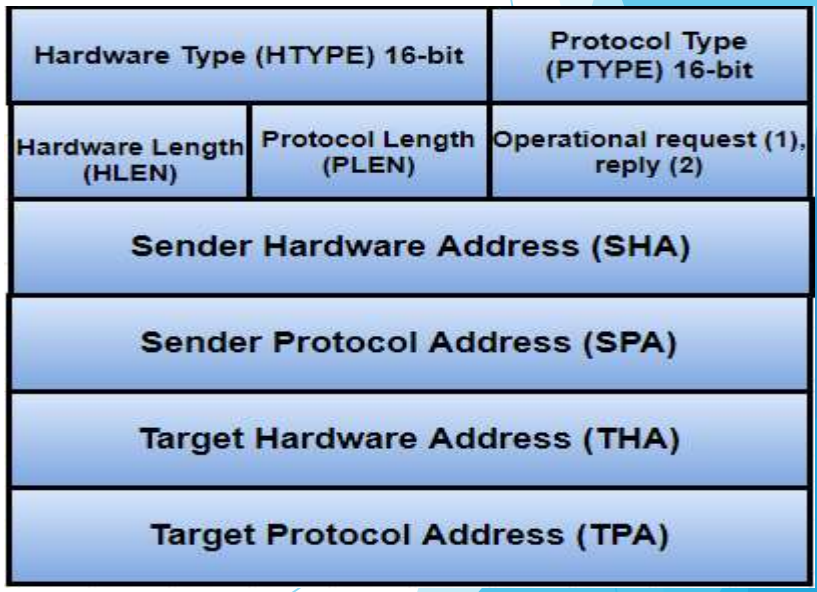
- The main advantage of proxy ARP is that it can be added to a single router on a network and does not disturb the routing tables of the other routers on the network.
- Proxy ARP must be used on the network where IP hosts are not configured with a default gateway or do not have any routing intelligence.

Disadvantages of Proxy ARP:

- It increases the amount of ARP traffic on your segment.
- Hosts need larger ARP tables in order to handle IP-to-MAC address mappings.
- Security can be undermined. A machine can claim to be another in order to intercept packets, an act called "spoofing."
- It does not work for networks that do not use ARP for address resolution.

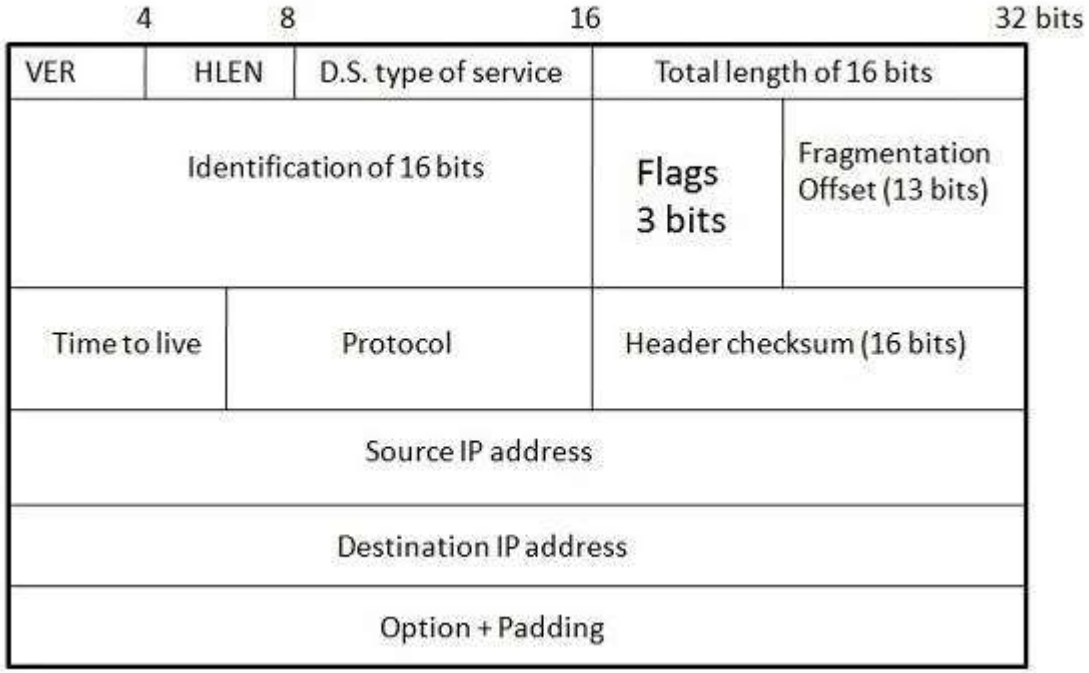
ARP PACKAGE

- The address resolution protocol (ARP) uses a basic message format that contains either address resolution request or address resolution response.
- The ARP message size depends on the address size of the link layer and the network layer.
- The message header describes the network type used at each layer and the address size of each layer.
- The message header is complete with the help of the operation code, which is 1 for request and 2 for the response.
- The payload of the packet has four addresses, these are:
  - Hardware address of the sender hosts
  - Hardware address of the receiver hosts
  - Protocol address of the sender hosts
  - Protocol address of the receiver hosts



Internet Protocol (IP)

- Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data.
- In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.
- Internet protocol transmits the data in form of a datagram as shown in the following diagram:



Datagrams

- Datagrams are also called "**IP datagrams**" since they are used by the Internet protocol (IP).
- A datagram header defines the source and destination of the data as well as other information, such as the total length (or size) of the datagram, time to live (TTL), and the specific protocol used to transfer the data.

Structure of a datagram:

- Each datagram has two components, a **header** and a **data payload**.
- The header contains all the information sufficient for routing from the originating equipment to the destination without relying on prior exchanges between the equipment and the network.
- Headers may include source and destination addresses as well as a type field.
- The payload is the data to be transported.
- This process of nesting data payloads in a tagged header is called encapsulation.

Datagram network:

- A datagram is a basic transfer unit associated with a packet-switched network. Datagrams are typically structured in header and payload sections. Datagrams provide a connectionless communication service across a packet-switched network.

Fragmentation

- IP fragmentation is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size.
- The fragments are reassembled by the receiving host.

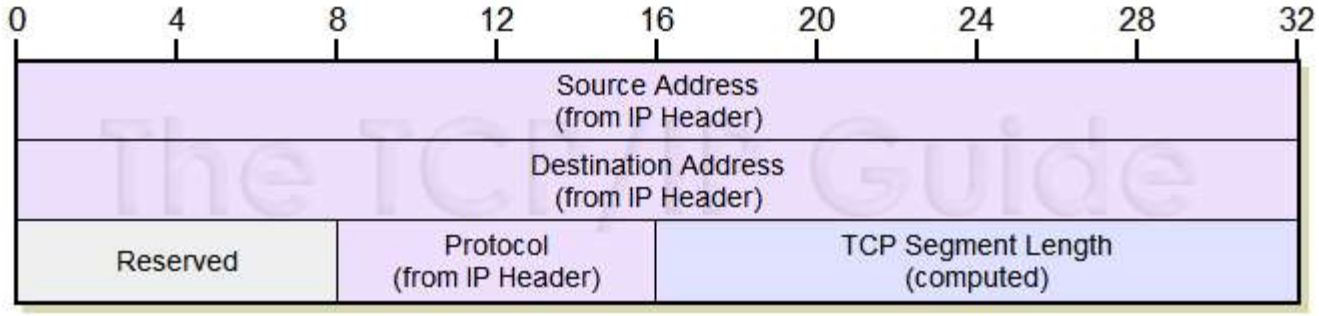
Options

The TCP Options (MSS, Window Scaling, Selective Acknowledgements, Timestamps, Nop) are located at the end of the TCP Header which is also why they are covered last.

- Maximum Segment Size (MSS)
- Window Scaling.
- Selective Acknowledgements (SACK)
- Timestamps.
- Nop.

Checksum

The TCP/IP checksum is used to detect corruption of data over a TCP or IPv4 connection. ... IPv4 uses the checksum to detect corruption of packet headers. i.e. the source, destination, and other meta-data. The TCP protocol includes an extra checksum that protects the packet "payload" as well as the header.



IP Package

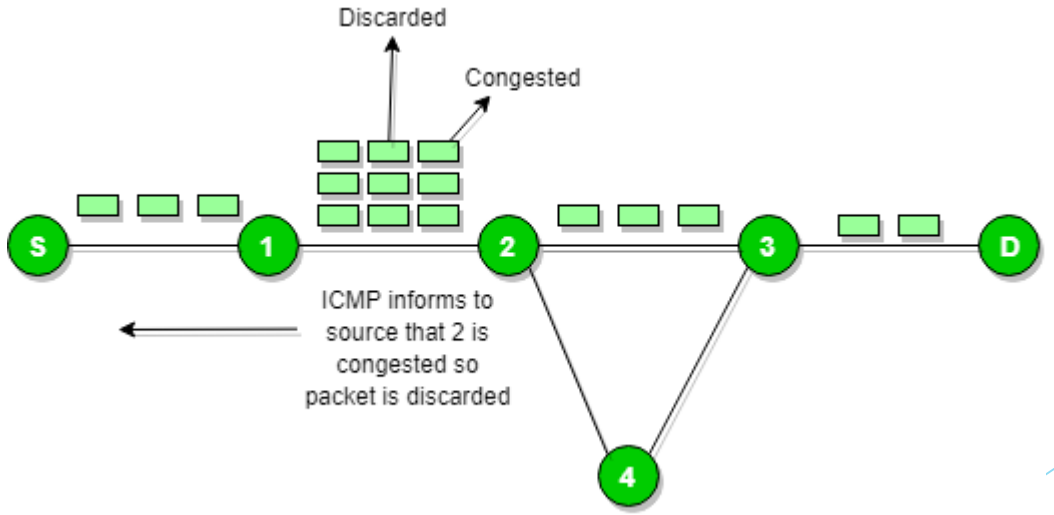
- IP packet encapsulates data unit received from above layer and add to its own header information. The encapsulated data is referred to as **IP Payload**.
- IP header contains all the necessary information to deliver the packet at the other end.

Internet Control Message Protocol (ICMP)

- Since IP does not have a inbuilt mechanism for sending error and control messages.
- It depends on Internet Control Message Protocol(ICMP) to provide an error control.
- It is used for reporting errors and management queries.
- It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.

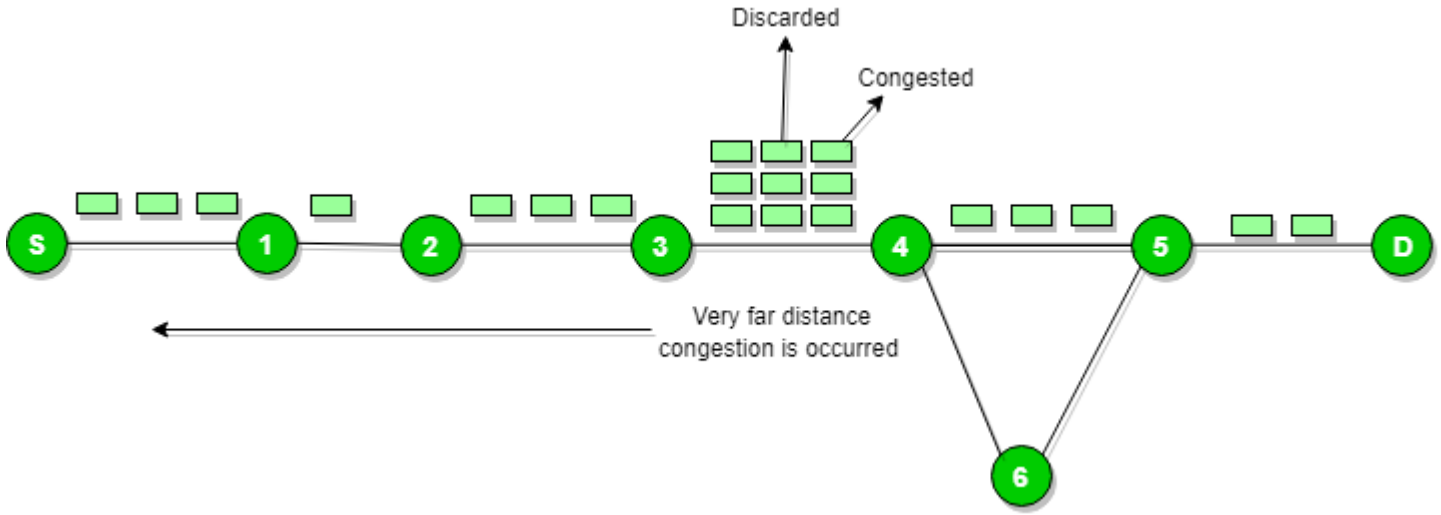
Source quench message :

- Source quench message is request to decrease traffic rate for messages sending to the host(destination).
- Or we can say, when receiving host detects that rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.



- ICMP will take source IP from the discarded packet and informs to source by sending source quench message.

- Then source will reduce the speed of transmission so that router will free for congestion.



- When the congestion router is far away from the source the ICMP will send hop by hop source quench message so that every router will reduce the speed of transmission.

Types of message

Echo Request, Echo Reply:

- Used to test destination accessibility and status. A host sends an Echo Request and listens for a corresponding Echo Reply.
- This is most commonly done using the ping command..

Destination Unreachable, Echo Reply:

- Sent by a router when it cannot deliver an IP datagram. A datagram is the unit of data, or packet, transmitted in a TCP/IP network.

Source Quench:

- Sent by a host or router if it is receiving data too quickly for it to handle. The message is a request that the source reduce its rate of datagram transmission.

Redirect Message:

- Sent by a router if it receives a datagram that should have been sent to a different router. The message contains the address to which the source should direct future datagrams.
- This is used to optimize the routing of network traffic.

Router Advertisement, Router Solicitation:

- Allow hosts to discover the existence of routers.
- Routers periodically broadcast their IP addresses via Router Advertisement messages.
- Hosts may also request a router address by broadcasting a Router Solicitation message to which a router replies with a Router Advertisement.

Time Exceeded:

- Sent by a router if the datagram has reached the maximum limit of routers through which it can travel.

Parameter Problem:

- Sent by a router if a problem occurs during the transmission of a datagram such that it cannot complete processing.
- One potential source of such a problem is invalid datagram header.

Timestamp Request, Timestamp Reply:

- Used to synchronize the clocks between hosts and to estimate transit time.

Information Request, Information Reply:

- Obsolete. These messages were used earlier by hosts to determine their inter-network addresses, but are now considered outdated and should not be used.

Address Mask Request, Address Mask Reply:

- Used to find the mask of the subnet (i.e. what address bits define the network).
- A host sends an Address Mask Request to a router and receives an Address Mask Reply in return.

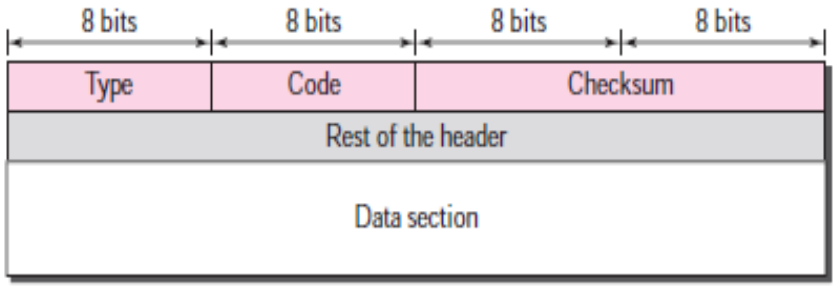
Message Format

Message Format:

- An ICMP message has an 8-byte header and a variable-size data section.

Although the general format of the header is different for each message type, the first 4 bytes are common to all.

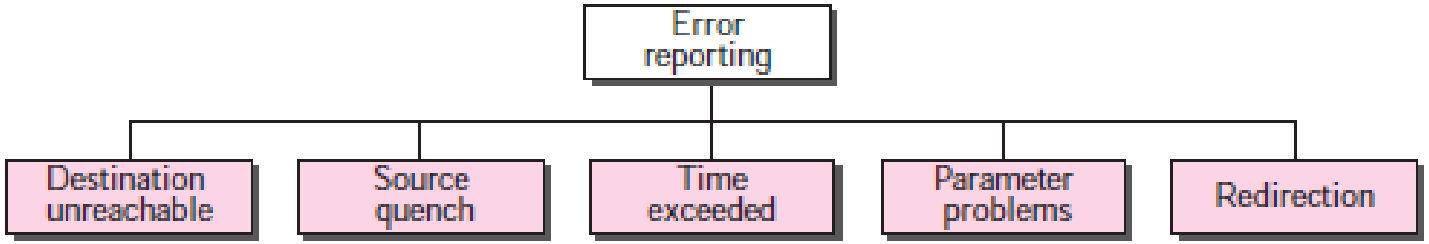
- The first field, ICMP type, defines the type of the message.
- The code field specifies the reason for the particular message type.
- The last common field is the checksum field (to be discussed later in the chapter).
- The rest of the header is specific for each message type.
- The data section in error messages carries information for finding the original packet that had the error.
- In query messages, the data section carries extra information based on the type of the query.



Error Reporting

Error Reporting Messages:

- One of the main responsibilities of ICMP is to report errors. Although technology has produced increasingly reliable transmission media, errors still exist and must be handled.
- This is an unreliable protocol.
- This means that error checking and error control are not a concern of IP



- No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- No ICMP error message will be generated for a datagram having a multicast address.
- No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Query

- A query is a request for data or information from a database table or combination of tables. This data may be generated as results returned by Structured Query Language (SQL) or as pictorials, graphs or complex results, e.g., trend analyses from data-mining tools.

Checksum

- In ICMP the checksum is calculated over the entire message (header and data).

Checksum Calculation:

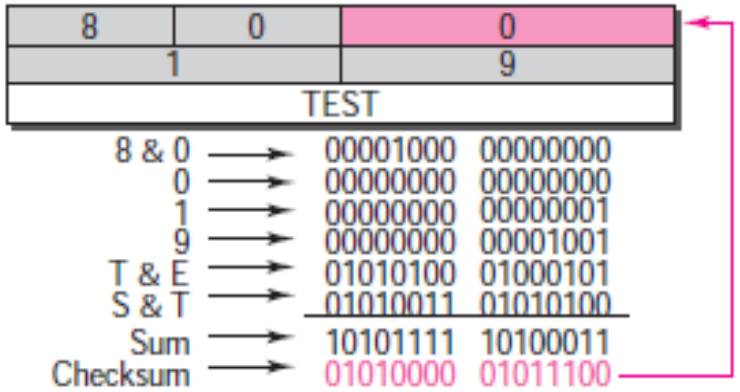
The sender follows these steps using one's complement arithmetic:

1. The checksum field is set to zero.
2. The sum of all the 16-bit words (header and data) is calculated.
3. The sum is complemented to get the checksum.
4. The checksum is stored in the checksum field.

Checksum Testing:

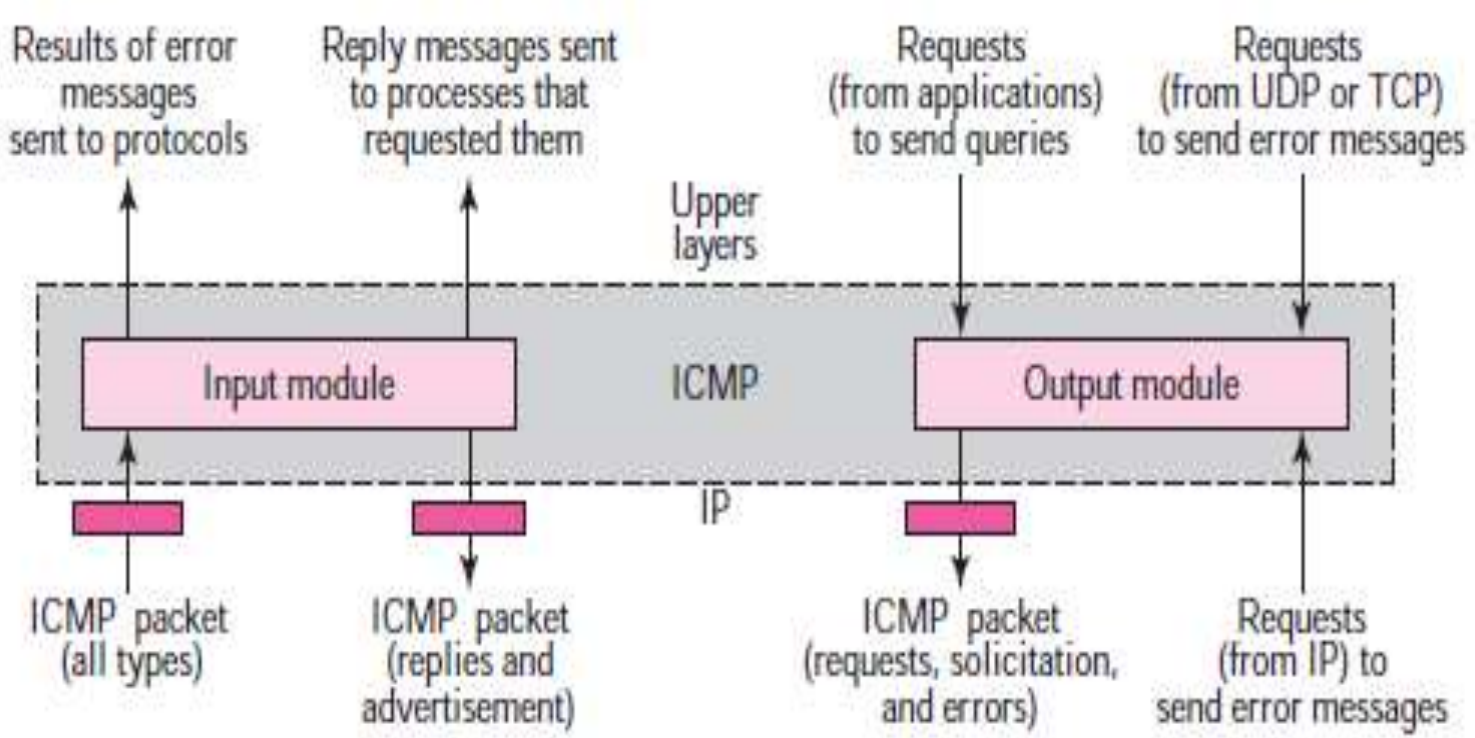
The receiver follows these steps using one's complement arithmetic:

1. The sum of all words (header and data) is calculated.
2. The sum is complemented.
3. If the result obtained in step 2 is 16 0s, the message is accepted; otherwise, it is rejected.



ICMP package

- To give an idea of how ICMP can handle the sending and receiving of ICMP messages.
- we present our version of an ICMP package made of two modules:
  - input module
  - output module.



Thank you