

Methods of Delivery

- A datagram can be delivered in one of four ways (since it is connectionless)
 - Unicast - directed to a single destination
 - Broadcast
 - Limited-broadcast 255.255.255.255: all hosts on local subnet
 - Network-directed broadcast: valid network address, all 1 in host part
 - Subnet-directed broadcast: valid network and subnet address, all 1 in host part
 - All-subnets-directed broadcast: valid network and all 1s in subnet and host part
 - Multicasting – Hosts are grouped using the same Class D IP address
 - Anycasting – Hosts are given same address and the first host to receive it will form a connection

Public and Private IP addresses

- Public IP addresses are unique throughout all the networks.
 - This will allow successful routing of datagrams from one to the other
- Private IP addresses are given to networks that do not need to crosstalk
 - Private IP addresses are not unique
- A range of IP addresses are reserved by RFC 1918 thus stopping routers from routing datagrams using such addresses
 - 10.0.0.0 to 10.255.255.255 (Class A)
 - 172.16.0.0 to 172.31.255.255 (Class B)
 - 192.168.0.0 to 192.168.255.255 (Class C)

[IP exhaustion problem]

- By May 1996
 - All Class A, 62% of Class B and 37% of Class C addresses were allocated or assigned
- Efforts have been made to limit allocation of Class A and Class B addresses, while allocating Class C addresses according to region
- The use of private IP addresses limits the exhaustion problem, allowing networks to communicate with other networks using one single public IP address
- Large use of Class C networks also meant that routing tables became very large
 - Thus the introduction of CIDR

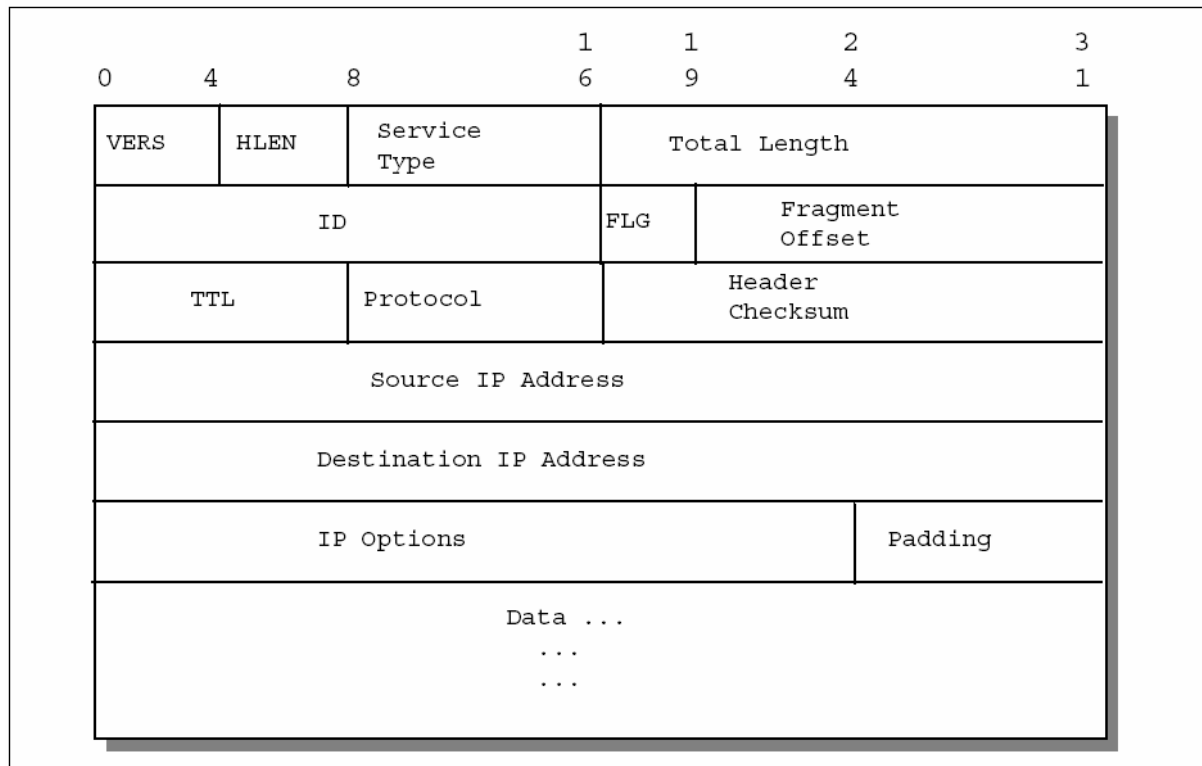
Classless Inter-Domain Routing (CIDR)

- CIDR does not route according to the class, but according to the IP prefix
 - IP Prefix is the high order bits of an IP address
- Each routing entry in the routing table will contain an IP address and a network mask to determine the IP prefix
 - To refer to 8 Class C networks in one go one would have
 - IP: 192.32.136.0
 - Mask: 255.255.248.0
- Combining multiple network addresses in one entry is known as *supernetting*.
- Nowadays address ranges are allocated in terms of CIDR ranges.
- Routing can now form a hierarchical structure

[IP Datagram]

- An IP datagram consists of
 - An IP header
 - Data (which is made up of a physical network header + data)
- Maximum length of an IP datagram is 64KB and a minimum of 576 bytes
- IP can allow for fragmentation
 - Necessary when crossing different networking technologies having differing MTUs
 - Each fragment has a header and is treated like a normal IP datagram
 - De-fragmentation is normally performed by the received host

[IP Header]



- Vers contains 4, until IPv6 starts being used
- Hlen is size of header in bytes
- Total Length is number of bytes in header+data

[IP Header (cont)]

- ID is a unique number for the IP datagram
 - Fragments of the same IP datagram have the same ID number
- Flag has 2 main bits (third is reserved)
 - DF: show if to allow fragmentation
 - MF: 0 means this is the last fragment, 1 means there are other fragments
- Fragment Offset: Number of 8 byte fragments contained in previous fragments
- TTL: Time to Live indicates number of hops, each router subtracts one from this
- Protocol: A number showing to which higher level protocol to pass the data. Ex.6 is TCP, 17 is UDP and 1 is ICMP
- Options give indications to intermediate routers

[IP Options]

- Loose Source Routing
 - Supply explicit routing information and each router records the route
- Strict Source Routing
 - Same as above yet routers have to obey the path given
- Record Router
 - Each router records the route yet host does not specify any route
- Internet Timestamp
 - Each router places a timestamp of when the datagram was processed

[ICMP]

- Internet Control Message Protocol (ICMP) is used to inform the host about errors in datagram processing
 - ICMP uses IP as if ICMP was a higher level protocol
 - ICMP reports errors and cannot be used to make IP reliable
 - ICMP does not report errors on ICMP messages
 - ICMP reports errors only for first fragment
- An ICMP packet contains
 - The TYPE of error
 - CODE referring to type of error
 - CHECKSUM for header+message
 - DATA contains ICMP message
- Original IP packet that causes an ICMP packet to be sent is discarded

[Popular ICMP messages]

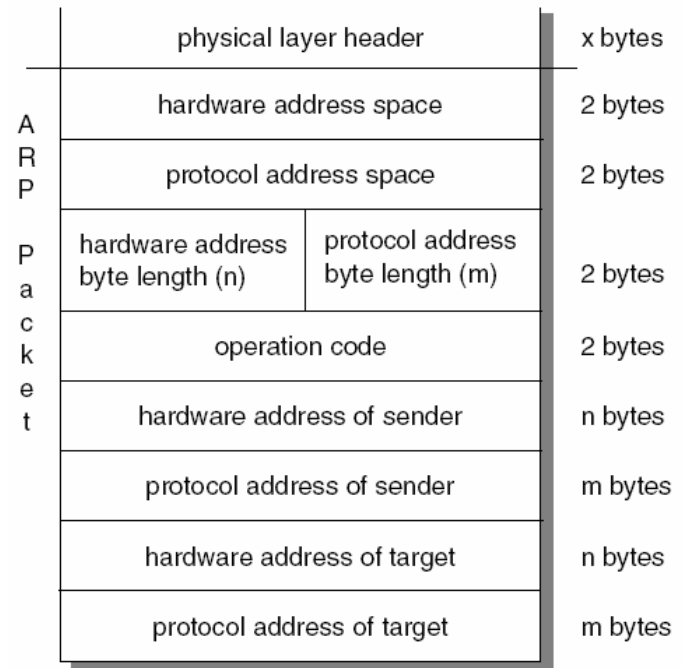
- Echo (8) and Echo Reply (0)
 - Used by ping
- Destination Unreachable (3)
 - Code shows what is unreachable
- Source Quench (4)
 - Buffer overflow forcing sender to slow down transmission rate
- Redirect (5)
 - Indicates alternate routers to routers
- Time Exceeded (11)
 - Used by trace routing

[IGMP]

- The Internet Group Management Protocol (IGMP) is used to allow hosts to participate in multi-casts
 - Supports host subscription to multicast addresses
 - Supports subnet subscription to multicast addresses
- IGMP is part of the IP protocol but makes use of the IP datagram as its carrier

[ARP]

- Whenever an IP datagram needs to be sent, the destination physical network address needs to be acquired.
- The Address Resolution Protocol (ARP) performs this task
- ARP lies both at layer 2 and layer 1 of the TCP/IP model.
- ARP builds the ARP table that allows it to translate an IP address to a physical network address.
- When an IP address is not found, the original IP datagram is discarded and an ARP request is sent out as a physical network broadcast
 - Routers will not forward physical network broadcast messages.
- Destination will recognise the IP address and will reply using an ARP reply
 - Destination will also learn ARP table entry for sender.
- Read about Proxy ARP that allows transparent subnetting to subnet-less hosts (default gateway is normally used).



[RARP]

- Reverse ARP is used by hosts that require an IP address when booted.
- An RARP request is sent to a known network address
- The RARP reply fills in the details of the sender's and receiver's IP address.
- A server must exist on the network that contains mappings between all MAC addresses and IP addresses.
- The use of DHCP or at least BOOTP is more common nowadays for such hosts.