Network Layer and Protocols

Network Layer is responsible for the transmission of data or communication from one host to another host connected in a network. Rather than describing how data is transferred, it implements the technique for efficient transmission. In order to provide efficient communication protocols are used at the network layer. The data is being grouped into packets or in the case of extremely large data it is divided into smaller sub packets. Each protocol used has specific features and advantages.

Functions of Network Layer

The network layer is responsible for providing the below-given tasks:

- **Logical Addressing:** Each device on the network needs to be identified uniquely. Therefore network layer provides an addressing scheme to identify the device. It places the IP address of every sender and the receiver in the header. This header consists of the network ID and host ID of the network.
- **Host-to-host Delivery of Data:** The network layer ensures that the packet is being delivered successfully from the sender to the receiver. This layer makes sure that the packet reaches the intended recipient only.
- **Fragmentation:** In order to transmit the larger data from sender to receiver, the network layer fragments it into smaller packets. Fragmentation is required because every node has its own fixed capacity for receiving data.
- **Congestion Control:** Congestion is defined as a situation where the router is not able to route the packets property which results in aggregation of packets in the network. Congestion occurs when a large amount of packets are flooded in the network. Therefore network layer controls the congestion of data packets in the network.
- **Routing and Forwarding:** Routing is the process that decides the route for transmission of packets from sender to receiver. It mostly chooses the shortest path between the sender and the receiver. Routing protocols that are mostly used are path vector, distance vector routing, link state routing, etc.

Network Layer Protocols:

1. IP
2. ARP
3. RARP
4. ICMP
5. IGMP

IP (Internet Protocol)

IP stands for Internet Protocol. Internet Protocol helps to uniquely identify each device on the network. Internet protocol is responsible for transferring the data from one node to another node in the network. Internet protocol is a connectionless protocol therefore it does not guarantee the delivery of data. For the successful delivery higher level protocols such as TCP are used to guarantee the data transmission. The Internet Protocol is divided in two types. They are:

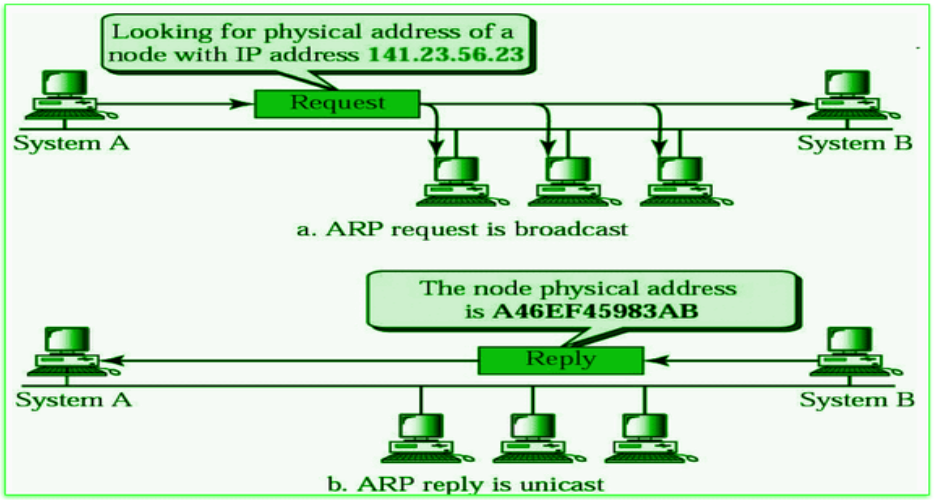
- **Pv4:** IPv4 provides with the 32 bit address scheme. IPv4 addressing has four numeric fields and are separated by dot. IPv4 can be configured either using DHCP or manually. IPv4 does not provide with more security features as it does not support authentication or encryption techniques. IPv4 is further divided into five classes as Class A, Class B, Class C, Class D and Class E.
- **IPv6:** IPv6 is the most recent version of IP. If provided with a 128 but addressing scheme. IP adress has eight fields that are separated by colon, and these fields are alphanumeric. The IPv6 address is represented in hexadecimal. IPv6 provides with more security features such as authentication and encryption. IPv6 supports end-to-end connection integrity. IPv6 provides with more range of IP adress as compared to IPv4.

ARP (Address Resolution Protocol)

ARP stands for Address Resolution Protocol. ARP is used to convert the logical address ie. IP address into physical address ie. MAC address. While communicating with other nodes, it is necessary to know the MAC address or physical address of the destination node. If any of the node in a network wants to know the physical address of another node in the same network, the host then sends an ARP query packet. This ARP query packet consists of IP address and MAC address of source host and only the IP address of destination host. This ARP packet is then received to every node present in the network. The mode with its own IP address recognises it and sends it MAC address to the requesting node. But sending and receiving such packets to know the MAC address of destination node it increases the traffic load. Therefore in order to reduce this traffic and improve the performance, the systems that makes use of ARP maintain a cache of recently acquired IP into MAC address bindings.

How Does ARP Work?

- The host broadcasts an ARP inquiry packet containing the IP address over the network in order to find out the physical address of another computer on its network.
- The ARP packet is received and processed by all hosts on the network; however, only the intended recipient can identify the IP address and reply with the physical address.
- After adding the physical address to the datagram header and cache memory, the host storing the datagram transmits it back to the sender.

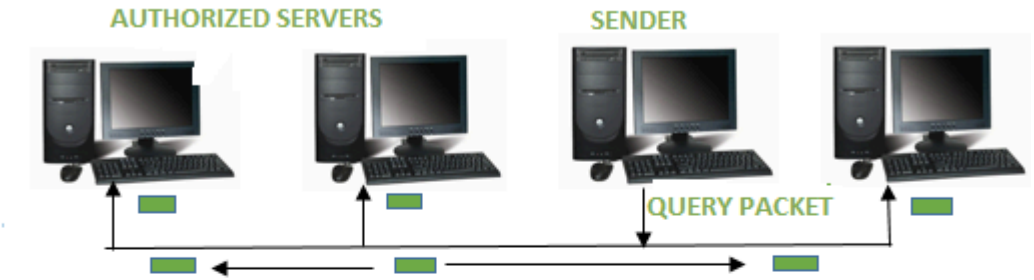


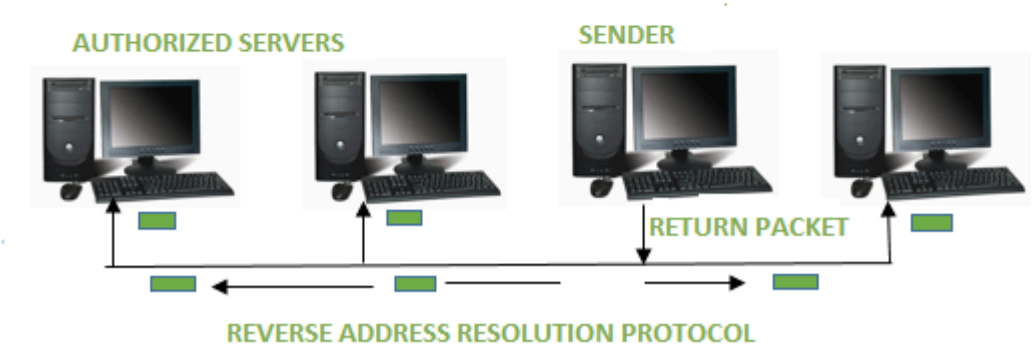
RARP

RARP stands for Reverse Address Resolution Protocol. RARP works opposite of ARP. Reverse Address Resolution Protocol is used to convert MAC address ie. physical address into IP address ie. logical address. RARP provides with a feature for the systems and applications to get their own IP address from a DNS(Domain Name System) or router. This type of resolution is required for various tasks such as executing reverse DNS lookup. As Reverse Address Resolution Protocol works at low level it requires direct network addresses. The reply from the server mostly carries a small information but the 32 bit internet address is used and it does not exploit the full potential of a network such as ethernet.

How Does RARP Work?

- Data is sent between two places in a network using the RARP, which is on the Network Access Layer.
- Every user on the network has two distinct addresses: their MAC (physical) address and their IP (logical) address.
- Software assigns the IP address, and the hardware then builds the MAC address into the device.
- Any regular computer connected to the network can function as the RARP server, answering to RARP queries. It must, however, store all of the MAC addresses' associated IP addresses. Only these RARP servers are able to respond to RARP requests that are received by the network. The information package must be transmitted over the network's lowest tiers.
- Using both its physical address and Ethernet broadcast address, the client transmits a RARP request. In response, the server gives the client its IP address.





REVERSE ADDRESS RESOLUTION PROTOCOL

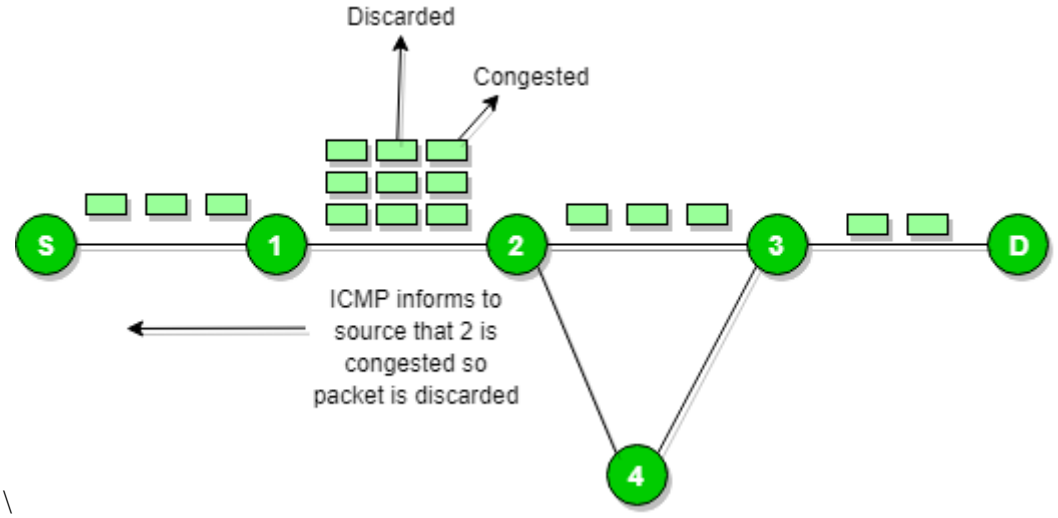
ICMP

ICMP stands for Internet Control Message Protocol. ICMP is a part of IP protocol suite. ICMP is an error reporting and network diagnostic protocol. Feedback in the network is reported to the designated host. Meanwhile, if any kind of error occur it is then reported to ICMP. ICMP protocol consists of many error reporting and diagnostic messages. ICMP protocol handles various kinds of errors such as time exceeded, redirection, source quench, destination unreachable, parameter problems etc. The messages in ICMP are divided into two types. They are given below:

- Error Message: Error message states about the issues or problems that are faced by the host or routers during processing of IP packet.
- Query Message: Query messages are used by the host in order to get information from a router or another host.

How Does ICMP Work?

- The main and most significant protocol in the IP suite is called ICMP. However, unlike TCP and UDP, ICMP is a connectionless protocol, meaning it doesn't require a connection to be established with the target device in order to transmit a message.
- TCP and ICMP operate differently from one another; TCP is a connection-oriented protocol, while ICMP operates without a connection. Every time a connection is made prior to a message being sent, a TCP Handshake is required of both devices.
- Datagrams including an IP header containing ICMP data are used to transmit ICMP packets. An independent data item like a packet is comparable to an ICMP datagram.



\

IGMP

IGMP stands for Internet Group Message Protocol. ICMP is a multicasting communication protocol. It utilizes the resources efficiently while broadcasting the messages and data packets. ICMP is also a protocol used by TCP/IP. Other hosts connected in the network and routers makes use of ICMP for multicasting communication that have IP networks. In many networks multicast routers are used in order to transmit the messages to all the nodes. Multicast routers therefore receives large number of packets that needs to be sent. But to broadcast this packets is difficult as it would increase the overall network load. Therefore ICMP helps the multicast routers by addressing them while broadcasting. As multicast communication consists of more than one senders and receivers the Internet Group Message Protocol is majorly used in various applications such as streaming media, web conference tools, games, etc.

How Does IGMP Work?

- Devices that can support dynamic multicasting and multicast groups can use IGMP.
- The host has the ability to join or exit the multicast group using these devices. It is also possible to add and remove customers from the group using these devices.
- The host and local multicast router use this communication protocol. Upon creation of a multicast group, the packet's destination IP address is changed to the multicast group address, which falls inside the class D IP address range.