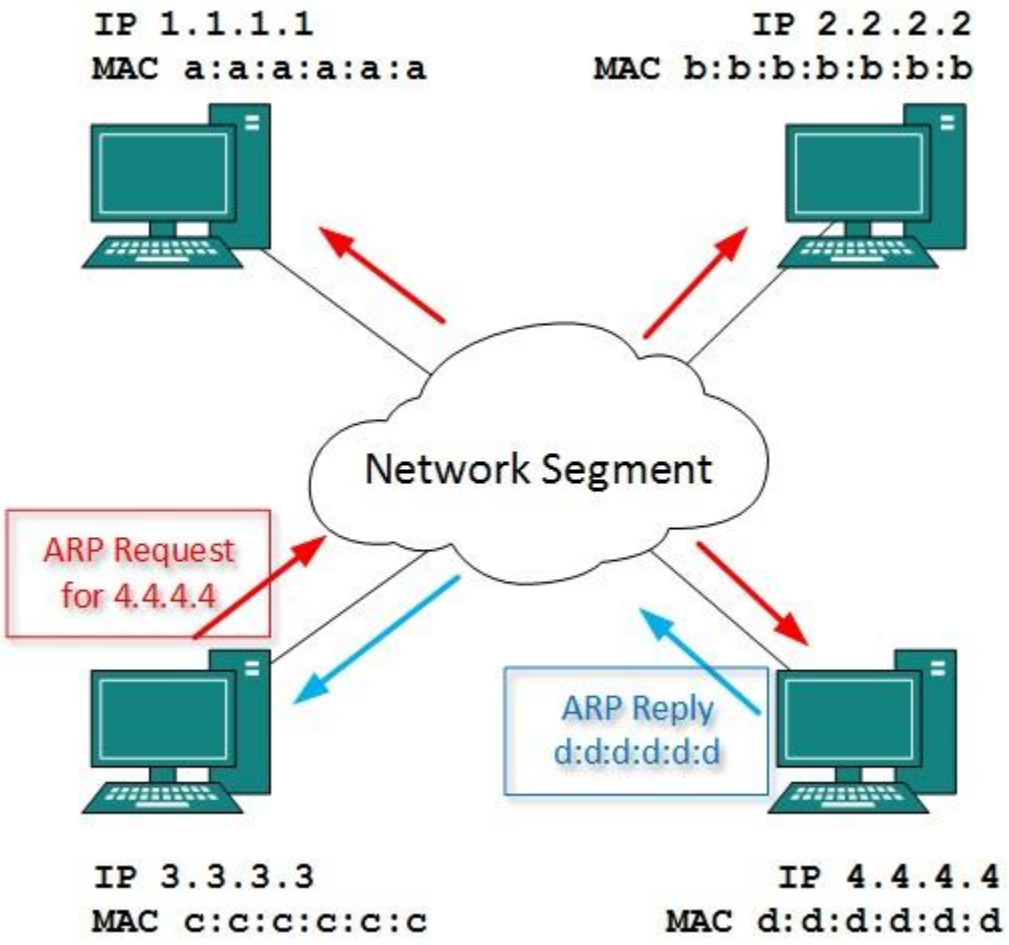
Network Layer Protocols

Address Resolution Protocol

In a network, every computer has an IP address by which a computer can be uniquely identified and addressed in whole broadcast domain. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belong to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card of a machine and it never changes.

On the other hand, IPs on the public domain are rarely changed but if their NIC is changed (in case of mechanical fault etc.) their MAC address also changes. This way, for Layer-2 communication to take place, a mapping between to is required.



[*Image: ARP Mechanism*]

To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking “who has this IP address?”. Because it is a broadcast, all hosts on the network segment (broadcast domain) receives this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, now it can communicates with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Internet Control Message Protocol

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet it is encapsulated in IP packet. Because IP is itself a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network the ICMP will report that problem.

Internet Protocol version 4

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A:** uses first octet for network addresses and last three octets for host addressing
- **Class B:** uses first two octets for network addresses and last two for host addressing
- **Class C:** uses first three octets for network addresses and last one for host addressing
- **Class D:** provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E:** experimental

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet) and public addresses (provided by ISPs and routable on internet).

Though IP is not reliable one but it provides ‘Best-Effort-Delivery’ mechanism.

Internet Protocol version 6

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but have removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of DHCP servers. This way even the DHCP server on that subnet is down, hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanism available for IPv6 enabled networks to easily speak and roam around different networks on IPv4. These are:

- Dual Stack implementation
- Tunneling
- NAT-PT

Source:

http://www.tutorialspoint.com/data_communication_computer_network/network_layer_protocols.htm