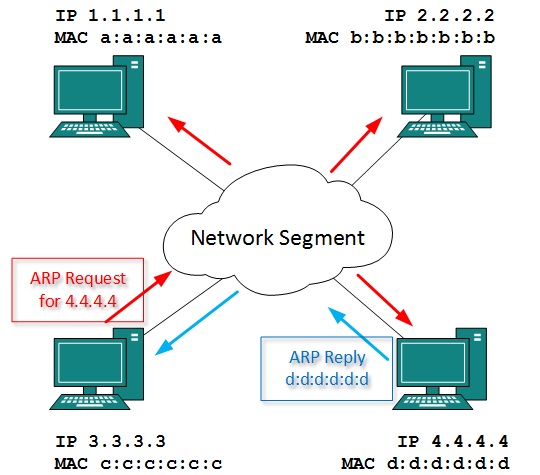
**Network Layer Protocols**

Every computer in a network has an IP address by which it can be uniquely identified and addressed. 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.

**Address Resolution Protocol(ARP)**

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

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.



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) receive 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, it can communicate 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 Protocol Version 4 (IPv4)

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**  - it uses first octet for network addresses and last three octets for host addressing
* **Class B**  - it uses first two octets for network addresses and last two for host addressing
* **Class C**  - it uses first three octets for network addresses and last one for host addressing
* **Class D**  - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
* **Class E**  - It is used as 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 are routable on internet).

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

## Internet Protocol Version 6 (IPv6)

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 has 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 Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the 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 mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

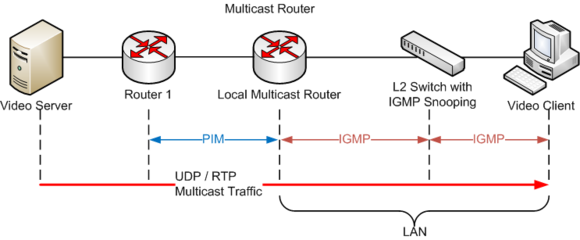
* Dual stack implementation
* Tunneling
* NAT-PT

**Internet Group Management Protocol (IGMP)**

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their host group memberships to any immediately neighboring multicast routers. IGMP is a integral part of IP. It must be implemented by all hosts conforming to level 2 of the IP multicasting specification. IGMP messages are encapsulated in IP datagrams, with an IP protocol number of 2.Version 3 of IGMP adds support for source filtering. This indicates the ability for a system to report interest in receiving packets;only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.  
  
The format of the IGMP packet is shown in the following illustration:

|  |  |  |
| --- | --- | --- |
| 8 | 16 | 32 bits |
| Type | Max response time | Checksum |
| Group address | | |
| *IGMP packet structure* | | |

A network designed to deliver a multicast service using IGMP might use this basic architecture:

[](http://en.wikipedia.org/wiki/File:IGMP_basic_architecture.png)

IGMP operates between the client computer and a local multicast router. Switches featuring IGMP snooping derive useful information by observing these IGMP

transactions. Protocol Independent Multicast (PIM) is then used between the local and remote multicast routers, to direct multicast traffic from the multicast server to many multicast clients.

IGMP operates on the network layer, just the same as other network management protocols like ICMP

The IGMP protocol is implemented on a particular host and within a router. A host requests membership to a group through its local router while a router listens for these requests and periodically sends out subscription queries.

IGMP is vulnerable to some attacks, and firewalls commonly allow the user to disable it if not needed.

**Internet Control Message Protocol (ICMP)**

The **Internet Control Message Protocol** (**ICMP**) is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.[1] It is assigned protocol number 1. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).

The Internet Control Message Protocol is part of the Internet Protocol Suite, as defined in RFC 792. ICMP messages are typically used for diagnostic or control purposes or generated in response to errors in IP operations (as specified in RFC 1122). ICMP errors are directed to the source IP address of the originating packet

### Header

The ICMP header starts after the IPv4 header and is identified by IP protocol number '1'. All ICMP packets have an 8-byte header and variable-sized data section. The first 4 bytes of the header have fixed format, while the last 4 bytes depend on the type/code of that ICMP packet.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ICMP Header Format** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ***Offsets*** | **Octet** | **0** | | | | | | | | **1** | | | | | | | | **2** | | | | | | | | **3** | | | | | | | |
| **Octet** | **Bit** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** |
| **0** | **0** | Type | | | | | | | | Code | | | | | | | | Checksum | | | | | | | | | | | | | | | |
| **4** | **32** | Rest of Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Type

ICMP type, see Control messages.

Code

ICMP subtype, see Control messages.

Checksum

Error checking data, calculated from the ICMP header and data, with value 0 substituted for this field. The Internet Checksum is used, specified in RFC 1071.

Rest of Header

Four-bytes field, contents vary based on the ICMP type and code.

### Data

ICMP error messages contain a data section that includes the entire IPv4 header, plus the first eight bytes of data from the IPv4 packet that caused the error message. The ICMP packet is then encapsulated in a new IPv4 packet.

## Reverse Address Resolution Protocol(RARP)

## Reverse Address Resolution Protocol(RARP) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache.

## C:\Users\TEXON\Desktop\rarptrans.png

 a special *RARP server* must be configured to listen for RARP requests and issue replies to them. Each physical network where RARP is in use must have RARP software running on at least one machine.RARP is not only very similar to ARP, it basically ***is*** ARP.It just describes a new method for using ARP to perform the opposite of its normal function. RARP uses ARP messages in exactly the same format as ARP, but uses different opcodes to accomplish its reverse function. Just as in ARP, a request and reply are used in an exchange. The meaning of the address fields is the same too: the sender is the device transmitting a message while the target is the one receiving it.

RARP packet:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **00** | **01** | **02** | **03** | **04** | **05** | **06** | **07** | **08** | **09** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** |
| Hardware type | | | | | | | | | | | | | | | | Protocol type | | | | | | | | | | | | | | | |
| Hardware address length | | | | | | | | Protocol address length | | | | | | | | Opcode | | | | | | | | | | | | | | | |
| Source hardware address ::: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Source protocol address ::: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Destination hardware address ::: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Destination protocol address ::: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Protocol type**.** 16 bits.

|  |  |
| --- | --- |
| **Protocol** | **Description** |
| **0x800** | IP. |

Hardware address length**.** 8 bits.  
Length of the hardware address in bytes.

Protocol address length**.** 8 bits.  
Length of the protocol address in bytes.

Opcode**.** 8 bits.

|  |  |  |
| --- | --- | --- |
| **Opcode** | **Description** | **References** |
| **3** | Request Reverse. | RFC 903 |
| **4** | Reply Reverse. | RFC 903 |

Source hardware address**.** Variable length.

Source protocol address**.** Variable length.

Destination hardware address**.** Variable length.

Destination protocol address**.** Variable length.