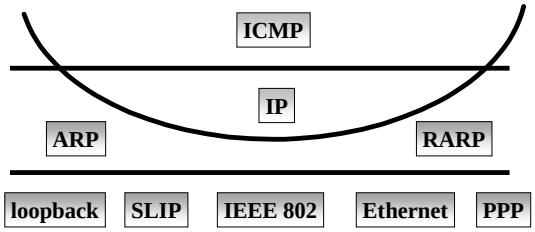
Address Resolution Protocol (ARP)

This protocol enables the IP layer to associate to hosts their physical addresses.

ARP/RARP interface IP to the underlying Data Link protocols



ARP tables

ARP maintains a dynamic table of <u>IP address / Hardware address</u> pairs.

This table is made available to the IP layer for address resolution purposes

ARP cache

A limited number of previous IP address / Hardware address pairs are kept in a cache for future use.

Then, IP may perform address resolution without real ARP queries over the network

ARP under DOS

```
C:\WINDOWS>arp -a
No ARP Entries Found
C:\WINDOWS>ping dora
Pinging dora.di.unito.it [130.192.239.28]
Reply from 130.192.239.28: bytes=32 time=1ms TTL=255
C:\WINDOWS>arp -a
Interface: 130.192.239.122
  Internet Address      Physical Address      Type
  130.192.239.1         08-00-20-21-66-26     dynamic
  130.192.239.28        08-00-20-20-e6-06     dynamic
```


ARP under Unix™

See *commands.txt* for sample output

Do *man arp* for the arp command, for viewing the arp table (*arp -a*), adding (*arp -s*) and deleting (*arp -d*) entries.

ARP format

2	2	1	1	2	6	4	6	4
ht	**pt**	**hs**	**ps**	**op**	**sh**	**sip**	**th**	**tip**

***ht**: hardware type (1 for Ethernet)*
***pt**: protocol type (0x800 for IP)*
***hs**: hardware address size (6 for Ethernet)*
***ps**: protocol address size (4 for IP)*
***op**: 1 for ARP request, 2 for reply*
***sh, th**: sender and target hardware address*
***sip, tip**: sender and target IP address*

28 bits ARP packet

Example: ARP request

```
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 2 arrived at 15:15:47.92
ETHER:  Packet size = 60 bytes
ETHER:  Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER:  Source      = 8:0:20:21:66:26, Sun
ETHER:  Ethertype = 0806 (ARP)
ETHER:
ARP:  ----- ARP/RARP Frame -----
ARP:  … next slide
```

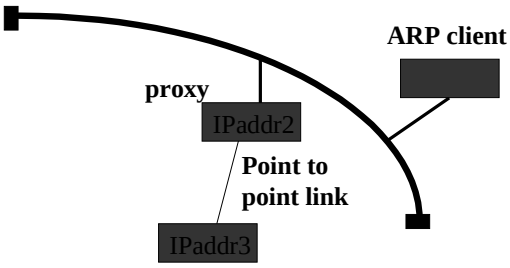

Example: ARP request

```
ETHER:  … previous slide
ARP:  ----- ARP/RARP Frame -----
ARP:  Hardware type = 1
ARP:  Protocol type = 0800 (IP)
ARP:  Length of hardware address = 6 bytes
ARP:  Length of protocol address = 4 bytes
ARP:  Opcode 1 (ARP Request)
ARP:  Sender's hardware address = 8:0:20:21:66:26
ARP:  Sender's protocol address = 130.192.239.1, pianeta
ARP:  Target hardware address = ?
ARP:  Target protocol address = 130.192.239.181, paros
```


Proxy ARP

A computer may advertise its hardware address not only for its own IP number, but also for the IP numbers of other hosts, thus acting as a proxy ARP agent.

Proxy ARP

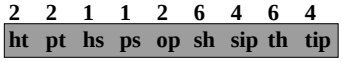


Reverse ARP (RARP)

Used for booting diskless workstations:

the hardware address can be read from the interface card, as is broadcast to the local network with an RARP request. An IP address for the local workstation is thus obtained from a server [RFC 903].

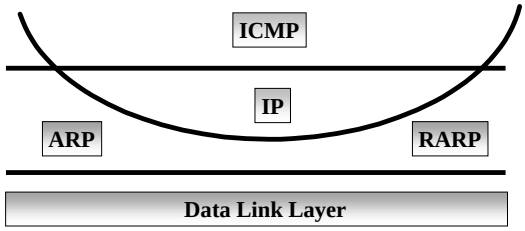
RARP format



***ht**: hardware type (1 for Ethernet)*
***pt**: protocol type (0x800 for IP)*
***hs**: hardware address size (6 for Ethernet)*
***ps**: protocol address size (4 for IP)*
***op**: 3 for RARP request, 4 for reply*
***sh, th**: sender and target hardware address*
***sip, tip**: sender and target IP address*

28 bits RARP packet

Internet Control Message Protocol (ICMP)

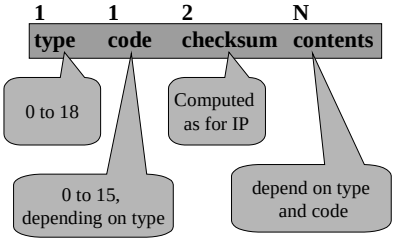


Internet Control Message Protocol (ICMP)

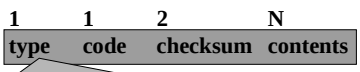
Used for handling Network layer error conditions of different kinds. An ICMP message is returned to the sender of the IP datagram that caused the delivery problems.

The ICMP message is sent within an IP datagram, after the IP header.

ICMP format

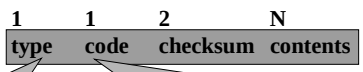


ICMP type



0 echo reply (ping)	11 time exceeded
3 destination unreachable	12 parameter problem
4 source quench	13 timestamp request
8 echo request	14 timestamp reply
9 router advertisement	17 address mask request
10 router solicitation	18 address mask reply

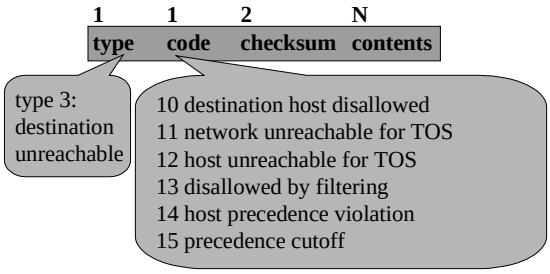
15 ICMP codes for type 3



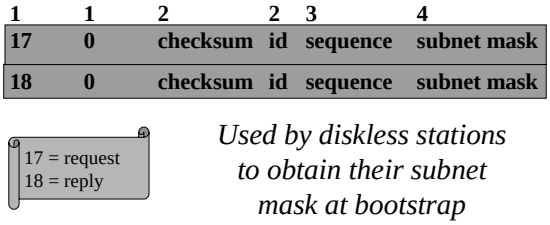
type 3: destination unreachable

0 network	5 source route failed
1 host	6 destination net unknown
2 protocol	7 destination host unknown
3 port	9 destination net disallowed
4 fragmentation needed, but disallowed	

15 ICMP codes for type 3



ICMP address mask request/reply



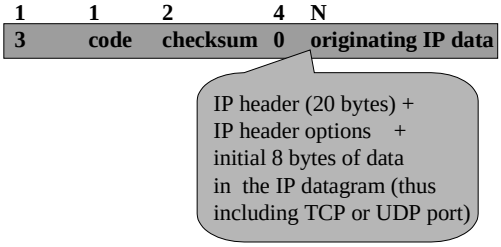
Used by diskless stations to obtain their subnet mask at bootstrap

Exercise

Run TCPdump;

Start an Xterminal and obtain the ICMP address mask request and reply over the Ethernet

ICMP destination unreachable

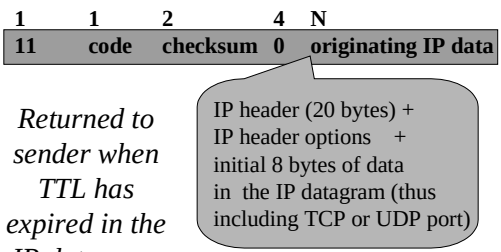


Exercise

Run TCPdump;

Telnet to a non-existing host, obtain an ICMP unreachable error message.

ICMP time exceeded



Returned to sender when TTL has expired in the IP datagram

Exercise

Using TCPdump and TTCP, implement a Traceroute program.

Hint: set TTL to 1 in TTCP with UDP datagrams to obtain an ICMP time exceeded error from the first route; set TTL to 2 for the second router, etc., until the desired host is reached. Use UDP port 50,000, so that "port unreachable" is returned when the final host is reached.