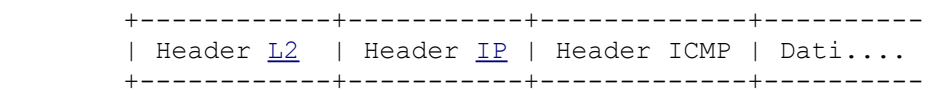
Protocollo ICMP

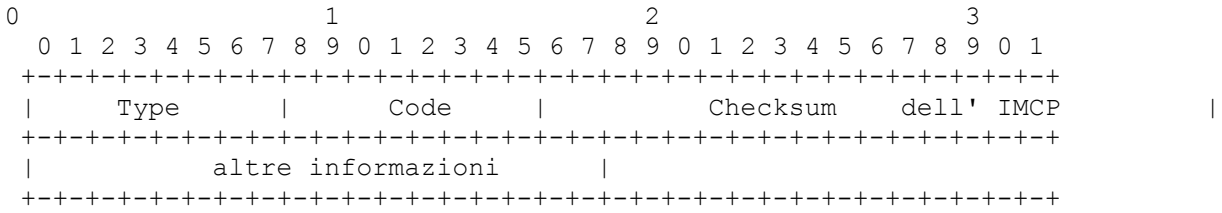
ICMP (Internet Control Message Protocol) è un protocollo di controllo per reti a pacchetto che trasmette informazioni su eventuali anomalie o malfunzionamenti nella trasmissione dei messaggi tra i vari componenti di una rete di calcolatori. ICMP è descritto dall'RFC 792, è usato da tutti i router, che se ne servono per **segnalare un errore** (Delivery Problem).

Questo meccanismo consente un error-reporting, offerto appunto dall'ICMP, ma non svolge azioni di correzione. Il protocollo ICMP viene ritenuto generalmente parte integrante del protocollo IP, viene incapsulato direttamente nel datagram IP e pertanto si colloca al terzo livello di ISO/OSI.

Un messaggio ICMP viene incapsulato in IP:



La struttura del pacchetto ICMP (RFC 792) è la seguente



In particolare sono rilevanti:

Type (8 bit) individua uno dei possibili tipi di messaggio ICMP

Code: (8 bit)fornisce ulteriori informazioni sul messaggio ICMP

Checksum (16 bit) meccanismo di controllo (tramite il calcolo del complemento) di eventuali errori nel messaggio ICMP

Type fondamentali sono

Tipo	Nome	
0	echo-reply	replica a a un ping
3	destination-unreachable	traffico TCP e UDP
5	redirect	instradamento dei pacchetti
8	echo-request	ping
11	time-exceeded (ttl-exceeded)	traceroute

In particolare i messaggi di tipo 3 sono fondamentali per garantire il funzionamento dei router dinamici e i relativi meccanismi di instradamento.

Significato dei messaggi ICMP

Tipo	Codice	Messaggio	Significato del messaggio
8	0	Richiesta di ECO	Questo messaggio è utilizzato quando si usa il comando *PING*. Questo comando, che permette di testare la rete, invia un datagramma ad un destinatario e gli chiede di restituirlo
3	0	Destinatario inaccessibile	La rete non è accessibile
3	1	Destinatario inaccessibile	Il terminale non è accessibile
3	2	Destinatario inaccessibile	Il protocollo non è accessibile
3	3	Destinatario inaccessibile	La porte non è accessibile
3	4	Destinatario inaccessibile	Frammentazione necessaria ma impossibile a causa del flag DF
3	5	Destinatario inaccessibile	Il router è fallito
3	6	Destinatario inaccessibile	Rete sconosciuta
3	7	Destinatario inaccessibile	Terminale sconosciuto
3	8	Destinatario inaccessibile	Terminale non connesso alla rete (inutilizzato)
3	9	Destinatario inaccessibile	Comunicazione con la rete vietata
3	10	Destinatario inaccessibile	Comunicazione con il terminale vietata
3	11	Destinatario inaccessibile	Rete inaccessibile per questo servizio
3	12	Destinatario inaccessibile	Terminale inaccessibile per questo servizio
3	11	Destinatario inaccessibile	Comunicazione vietata (filtraggio)
4	0	Source Quench	Quando il volume dei dati inviati è troppo importante, il router invia questo messaggio per prevenirne la saturazione richiedendo di ridurre la velocità di trasmissione
5	0	Reindirizzamento per un host	Il router osserva che il percorso di un computer non è ottimale e invia l'indirizzo del router da aggiungere nella tabella di router del computer
5	1	Reindirizzamento per un host e un servizio dato	Il router osserva che il percorso di un computer non è ottimale per un dato servizio e invia l'indirizzo del router da aggiungere nella tabella di router del computer
5	2	Reindirizzamento per una rete	Il router osserva che il percorso di un'intera rete non è ottimale e invia l'indirizzo del router da aggiungere nella tabella del router dei computer della rete
5	3	Reindirizzamento per una rete e un servizio dato	Il router osserva che il percorso di un'intera rete non è ottimale per un servizio dato e invia l'indirizzo del router da aggiungere nella tabella del router dei computer della rete
11	0	Tempo scaduto	Questo messaggio è inviato quando il tempo di vita di un datagramma è scaduto. L'intestazione del datagramma è rinviato affinché l'utente sappia quale datagramme è stato distrutto
11	1	Tempo di riassemblaggio di frammentazione scaduto	Questo messaggio è inviato quando il tempo di riassemblaggio dei frammenti di un datagramma è scaduto.

12	0	Intestazione errata	Questo messaggio è inviato quando un campo di intestazione è errato. La posizione dell'errore viene rinviata
13	0	Time stamp request	Un terminale richiede ad un altro la sua ora e data sistema (universale 9
14	0	Timestamp reply	Il terminale ricevitore da la propria ora e data sistema affinché il terminale emettitore possa determinare il tempo di trasferimento dei dati
15	0	Richiesta di indirizzo di rete	Questo messaggio permette di richiedere alla rete un indirizzo IP
16	0	Risposta dell'indirizzo IP	Questo messaggio risponde al messaggio precedente
17	0	Richiesta di maschera di sub-rete	Questo messaggio permette di richiedere alla rete una maschera di bub-rete
18	0	Risposta di maschera di sub-rete	Questo messaggio risponde al messaggio precedente
17	0	Timestamp reply	Il terminale ricevitore da la propria ora e data sistema affinché il terminale emettitore possa determinare il tempo di trasferimento dei dati

Il protocollo ICMP è anche alla base di alcuni importanti servizi per la rete come il servizio **Ping** e il **traceroute.**

Ping

Il comando Ping consente di verificare la raggiungibilità di qualsiasi host, misura l'RTT(Round trip time) e si esegue affiancando al comando ping l'indirizzo IP o il nome del server richiesto. Attraverso l'invio di pacchetti di prova (di tipo echo-request)che vengono subito ritrasmessi al mittente (di tipo echo-reply) vengono fornite informazioni diagnostiche, per prima cosa se il nodo è raggiungibile e attivo, il tempo impiegato dai pacchetti, quanti ne sono andati persi e il tasso di errore. Il ping è risolutore dei nomi di dominio e degli indirizzi IP.

Traceroute

Il comando traceroute (o tracert per windows) consente di visualizzare l'elenco dei router attraversati da un pacchetto per giungere a destinazione. Esso sfrutta il protocollo ICMP

Protocollo ARP

Il protocollo ARP (Address Resolution Protocol),standardizzato in RFC 826, è un protocollo di rete fondamentale per il funzionamento di TCP/IP in IPv4 e permette di conoscere l'indirizzo fisico di una scheda di rete corrispondente all' indirizzo IP di un host di una rete locale.
ARP "mappa" la corrispondenza tra l'ndirizzo IP e l'indirizzo MAC (MAC address) dei terminali in una rete locale, consentendo così la risoluzione dell'indirizzo IP. Il protocollo inverso è detto RARP (Reverse Address Resolution Protocol)
Infatti anche se ogni scheda di rete (NIC) possiede un numero di identificazione di 48 bit, detto MAC, assegnato al momento della produzione della scheda in fabbrica, la comunicazione tra host in rete e legata all' indirizzo logico IP.
Il protocollo ARP interroga i terminali della rete per conoscere i loro indirizzi fisici, poi crea una tabella di corrispondenza tra gli indirizzi logici e quelli fisici in una memoria cache, detta **cache ARP**.
Quando un terminale deve comunicare con un altro, consulta la tabella di corrispondenza. Se l'indirizzo richiesto non è nella tabella, il protocollo ARP emette una richiesta in rete, invia in broadcast un pacchetto di **ARP Request**, con il proprio indirizzo MAC e l'indirizzo IP del destinatario di cui vuole conoscere il MAC Address. L'host di destinazione che riconoscerà il proprio indirizzo IP nel pacchetto di ARP-request, provvederà ad inviare una risposta **ARP Reply** .

Il comando per visualizzare la tabella arp immagazzinata nella cache locale è `arp -a,` per impostare manualmente degli indirizzi IP statici nella tabella ARP il comando è
`arp -s [IP address] [indirizzo fisico] .`