È un protocollo di livello 3 di supporto a IP:

 i router o gateway della rete inviano dei messaggi ICMP per segnalare malfunzionamenti nella rete

Un pacchetto ICMP utilizza un header IP standard, come se fosse un livello superiore, ma è parte del protocollo IP stesso e quindi supportato da tutti i dispositivi di livello 3:

 Ciò nonostante non rende IP affidabile, ma cerca di fornire delle informazioni sullo stato della rete

Oltre a fornire feedback sullo stato delle connessioni, ICMP viene utilizzato per controllare lo stato della rete:

- alcune applicazioni di rete utilizzano attivamente ICMP per verificare la connettività della rete
- altre applicazioni utilizzano i messaggi ICMP per ottenere informazioni sulla reta in maniera indiretta (traceroute)

Schema di un pacchetto ICMP

Utilizza un header IP standard, in cui il campo protocollo è messo a 1:

- indirizzi IP sorgente e destinazione identificano la comunicazione
- campo TTL per evitare che il pacchetto circoli all'infinito nella rete

Può includere informazioni riguardanti altri livelli dello stack TCP/IP (es. port-unreachable).

La prima informazione fornita nel payload del pacchetto ICMP è il campo type:

 identifica il tipo di informazione fornita dal pacchetto e la struttura e logica del resto del pacchetto, infatti il pacchetto stesso cambia in base a questo campo

Alcuni esempi di messaggi possono essere:

- Echo Reply
- Destination Unreachable
- Redirect
- Echo
- Time exceeded

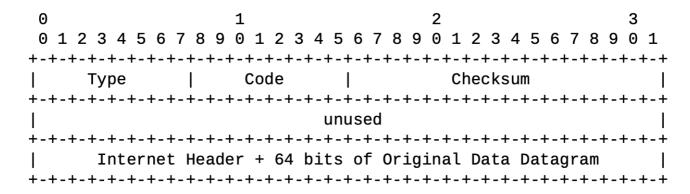
Echo e echo replay (type = 0)

Se un host riceve un echo (request) deve rispondere con una echo replay. Pensato appositamente per testate attivamente la connettività di rete (usato da ping)

Θ			2									3					
0 1 2	2 3 4 5	6 7 8	9 0 1	2 3	4 5	5 6	7 8	9	0 1	2	3	4	5	6	7 8	9 (1
+-																	
	Туре	Checksum															
+-																	
	Identifier							r									
+-															+-+		
	Inter	net Hea	der +	64 l	oits	s of	0r	igi	nal	Da	ata	l D	at	ag	ram	l	
+-													+-+				

Destination Unreachable (type = 3)

Pacchetto utilizzato per informare che è impossibile raggiungere una certa destinazione (non solo IP). L'indirizzo IP di destinatzione utilizzato sarà l'indirzzo IP sorgente del pacchetto intereassato all'errore



ICMP Packet too big

Un tipo particolare della famiglia unreachable, inviato dai router se il pacchetto IP non può essere inoltrato a causa di MTU troppo piccolo

Messaggio ICMP potenzialmente inviato in caso di impossibilità di inoltro per un pacchetto troppo grande:

- in caso di frammentazione non supportata dal router
- in caso di flag do not fragment settato dal mittente nell'header IP

Ha (anche) lo scopo di consentire l'individuazione del path MTU

Il tempo di vita del pacchetto è esaurito. Il code = 0 è utilizzato per segnalare che il pacchetto è stato scartato a causa del TTL esaurito:

 prima di inviare il pacchetto il router decrementa il TTL, se questo va a 0 il pacchetto non viene inviato. Il router manda il pacchetto ICMP con type=1 e code=0 per segnalare questa informazione

Redirect Message (type = 5)

Esiste un percorso migliore per inviare il pacchetto a destinazione. In base alle proprie regole di routing, un gateway può informare il mittente del pacchetto IP che esiste un percorso migliore per inviare pacchetti alla destinazione desiderata