

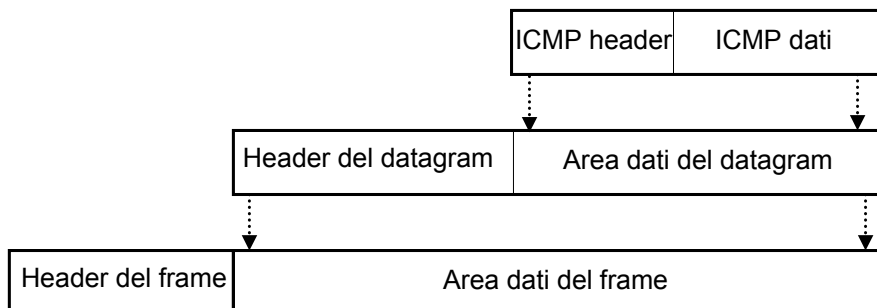
Protocollo ICMP

Internet Control Message Protocol

- **Internet Control Message Protocol (ICMP)**: usato dagli host, router e gateway per comunicare informazioni riguardanti il livello di rete, in particolari errori

- Es. Il messaggio "Destination host is unreachable" nel protocollo HTTP ha origine dall'ICMP

- Il messaggio ICMP è incapsulato in un datagram IP



Internet Control Message Protocol (2)

- ICMP usato per:
 - congestione e controllo di flusso dei datagram
 - comunicare periodicamente cambiamenti nelle tabelle di routing
 - determinare cammini circolari o eccessivamente lunghi
 - stimare il tempo di trasmissione da mittente a destinatario

Campo Time-To-Live del datagramma IP

- Poiché le tabelle di instradamento dei router non sono sempre “corrette”, è possibile che un pacchetto entri in cicli da cui non riesca ad uscire
- Per evitare congestioni dovute a situazioni di questo tipo, si fissa un limite al tempo entro cui un pacchetto può restare sulla rete. Nei pacchetti IP il campo **Time-To-Live** misura il tempo di vita rimanente al pacchetto.
- Ciascun router deve decrementare il TTL di almeno una unità (RFC 1812). Nella pratica, i pacchetti raramente rimangono in un router per più di un secondo ed i router semplicemente decrementano di uno il TTL prima di instradare un pacchetto

Campo Time-To-Live del datagramma IP (2)

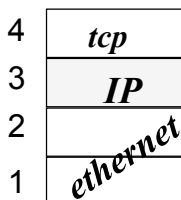
- Quindi, indipendentemente dal nome, **il TTL conta il numero di hop che il pacchetto può fare prima di giungere a destinazione o di essere scartato.**
- I router controllano se il TTL è uguale a zero dopo il decremento, subito prima dell'inoltro. Se il destinatario del pacchetto è il router stesso questo non viene mai scartato (RFC 1812).

Protocolli di supporto

protocolli che offrono servizi

portano “dati utente”
le loro pdu vengono imbustate in accordo alla pila iso-osi

esempi:

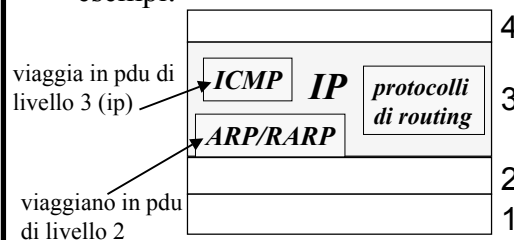


protocolli di supporto

portano dati “di controllo” e non offrono direttamente servizi

*la loro posizione nella pila è **indipendente** da come vengono imbustate le pdu*

esempi:



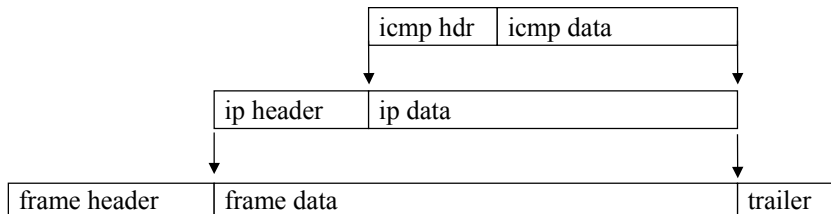
Internet Control Message Protocol (ICMP), RFC 792

- Scopi
 - Notifica situazioni di errore o anomalie
 - Supporta “debugging” interattivo della rete
- ICMP è funzionale ad IP e viaggia in pacchetti IP
- ICMP porta informazioni di controllo e di notifica di errori. Non porta dati. I pacchetti ICMP viaggiano all’interno dei pacchetti IP.
- Le funzionalità fornite da ICMP sono accessorie al livello 3, quindi ICMP è considerato un protocollo di livello 3. ICMP è sempre presente a fianco di IP.

ICMP Message Types

- Echo Request
- Echo Response
- Destination Unreachable
- Time Exceeded
- Redirect (route change)
- altri ...

Relazione tra ICMP e IP



- regola 1: nessun messaggio ICMP viene generato a seguito ad eventuali errori rilevati su messaggi ICMP
- regola 2: se il pacchetto viene frammentato solo il primo frammento può generare messaggi di errore ICMP
- regola 3: i broadcast e multicast non generano ICMP

Messaggi di errore

Questi messaggi di errore seguono un pacchetto scartato:

- **TIME_EXCEEDED** (tempo scaduto)
 - il pacchetto ha TTL=0
- **DESTINATION_UNREACHABLE**
 - un gateway vede la rete destinazione a distanza infinita (net unreachable)
 - l'host non risponde ad una chiamata ARP (host unreachable)
 - l'host destinazione non conosce il protocollo nel pacchetto (protocol unreachable)
 - il pacchetto non può essere frammentato (fragmentation needed and DF set)

Far riferimento alla RFC 792 per ulteriori approfondimenti
in particolare alle sezioni "description" per ciascun messaggio.

Messaggi di errore (2)

- **PARAMETER_PROBLEM** (problema con i parametri).
 - Il gateway non riesce ad interpretare il pacchetto ricevuto a causa di un valore errato, possibile errore software
- **SOURCE_QUENCH** obsoleto (rallentamento, soffocamento della sorgente)
 - congestione di un gateway intermedio
 - host destinazione lento nell'acquisizione

Messaggi di informazione

- **ECHO_REQUEST** e **REPLY** (richiesta di echo e relativa risposta)
 - controllo di raggiungibilità di un host
- **TIMESTAMP** e **TIMESTAMP_REPLY**
come **ECHO** più informazioni su orario invio
 - misura di velocità del collegamento
 - sincronizzazione (approssimativa) dell'ora di sistema
- **REDIRECT** Un router intermedio si accorge che il percorso che il datagram sta seguendo non è ottimale: gli dice di cambiare percorso, ma nel frattempo inoltra il datagram originale verso la sua destinazione

ping

```
<patrigna@pascal ~> ping wilma.cs.brown.edu
PING wilma.cs.brown.edu: (128.148.19.15): 56 data bytes
64 bytes from 128.148.19.15: icmp_seq=1 ttl=239 time=1736 ms
64 bytes from 128.148.19.15: icmp_seq=2 ttl=239 time=1507 ms
64 bytes from 128.148.19.15: icmp_seq=6 ttl=239 time=1209 ms
64 bytes from 128.148.19.15: icmp_seq=8 ttl=239 time=762 ms
64 bytes from 128.148.19.15: icmp_seq=9 ttl=239 time=1235 ms
64 bytes from 128.148.19.15: icmp_seq=11 ttl=239 time=1566 ms
64 bytes from 128.148.19.15: icmp_seq=13 ttl=239 time=586 ms
64 bytes from 128.148.19.15: icmp_seq=14 ttl=239 time=352 ms
64 bytes from 128.148.19.15: icmp_seq=22 ttl=239 time=910 ms
^C
----wilma.cs.brown.edu PING Statistics----
29 packets transmitted, 9 packets received, 68% packet loss
round-trip min/avg/max = 352/1095/1736 ms
<patrigna@pascal ~>
```

ping

- Invia una successione di pacchetti ICMP **ECHO_REQUEST** e attende la relativa risposta **ECHO_REPLY**
- Misura il tempo che intercorre tra l'invio e la ricezione di ogni pacchetto e riporta semplici statistiche
- Il comando **ping** fa parte della dotazione standard di tutte le macchine sia Unix che Windows anche se con sintassi leggermente diverse.
- L'indirizzo wilma.cs.brown.edu viene risolto in un indirizzo IP normale che dall'output è 128.148.19.15
- In questo output alcuni pacchetti risultano persi, esattamente il 68%
- Ulteriori informazioni: manuale in linea di **ping** (sui sistemi Unix: **man ping**)

traceroute

```
<utente@pascal ~>traceroute wilma.cs.brown.edu
traceroute to wilma.cs.brown.edu (128.148.19.15), 30 hops max, 40 byte
packets
 1 gw1.fis.uniroma3.it (193.204.160.1) 3 ms 3 ms 2 ms
 2 141.108.132.1 (141.108.132.1) 832 ms 967 ms 402 ms
 3 mp4rm1.roma1.infn.it (141.108.127.6) 267 ms 106 ms 417 ms
 4 atm-garthen-rm.infn.it (192.135.31.5) 100 ms 939 ms 839 ms
 5 cnafint-ten34.infn.it (192.135.34.21) 1100 ms * 1056 ms
 6 mix-serial3-4.Washington.mci.net (204.189.152.161) 618 ms * *
 7 * core1-fddi-0.Washington.mci.net (204.70.2.1) 1249 ms *
 8 * * *
 9 wtn-bbn-nap.Washington.mci.net (206.157.77.218) 766 ms * *
```

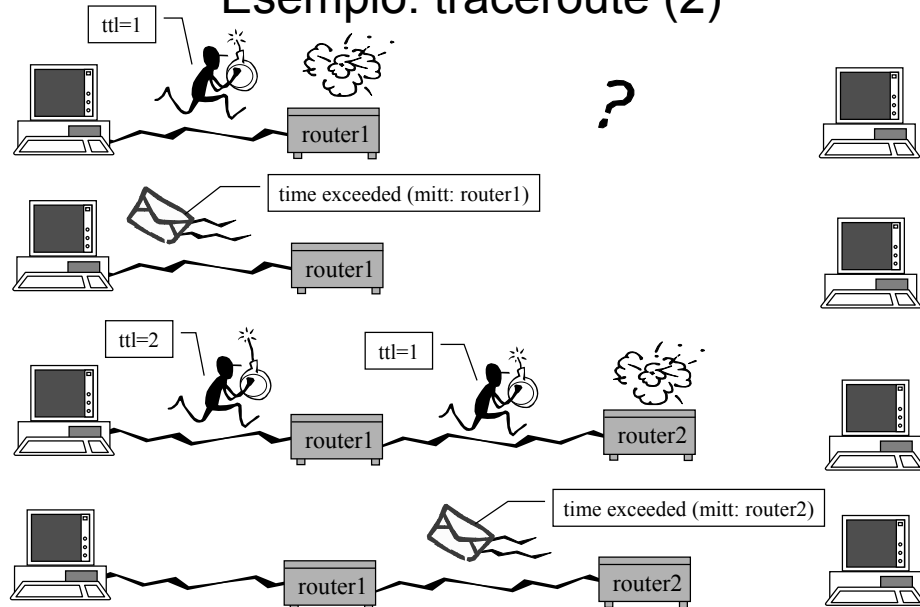
Traceroute (2)

```
10 * * chicago1-br1.bbnplanet.net (4.0.1.5) 857 ms
11 * * *
12 * boston1-br1.bbnplanet.net (4.0.2.245) 846 ms *
13 boston1-br2.bbnplanet.net (4.0.2.250) 680 ms * *
14 * * boston1-mr4.bbnplanet.net (4.0.44.19) 648 ms
15 providence-cr1.bbnplanet.net (4.0.45.106) 416 ms providence-
cr1.bbnplanet.net (4.0.45.102) 1298 ms *
16 brown.bbnplanet.net (131.192.32.2) 1444 ms 615 ms 802 ms
17 * * *
18 * ftp.cs.brown.edu (128.148.19.15) 834 ms 435 ms
<utente@pascal ~>
```


Esempio: traceroute

- Si ipotizzi di inviare un pacchetto, ad esempio un ECHO_REQUEST con $TTL=n$ "basso". Se il destinatario è troppo lontano l'ultimo router risponderà con un TIME_EXCEEDED, se il destinatario risponde con ECHO_REPLY allora è raggiungibile con n hop
- In realtà alcuni **traceroute** non utilizzano gli ECHO_REQUEST se non gli viene chiesto esplicitamente ma altri protocolli (UDP). Inoltre manda 3 pacchetti per ogni valore di n . Se non si osserva un TIME_EXCEEDED entro un tempo prestabilito **traceroute** visualizza un asterisco "**"
- Il manuale in linea di **traceroute** è estremamente interessante e mostra anche esempi di strani comportamenti da parte dei router

Esempio: traceroute (2)



traceroute

- Il comando **traceroute** permette di capire per quali router passano i pacchetti IP quando sono diretti ad una data destinazione.
- **traceroute** è compreso nella dotazione standard di tutti i sistemi Unix.
- Nei sistemi Windows il comando ha il nome **tracert** e sintassi leggermente differente.
- **traceroute** trova utilizzo anche nell'ambito dell'amministrazione della rete per isolare guasti o incoerenze nelle tabelle di routing.
- Dal punto di vista didattico la sua utilità è di mostrare il percorso dei pacchetti svelando un po' della topologia nascosta di Internet.