

...

6.2 ICMP (CONTROL PLANE)

È un protocollo usato per trasmettere messaggi di controllo tra router e host. Può essere considerato come parte dell'IP. I messaggi ICMP vengono trasportati da datagram IP. Esso è quindi anche un utilizzatore di IP. In IPv6, la maggior parte delle funzionalità di ICMP sono state spostate in IP.

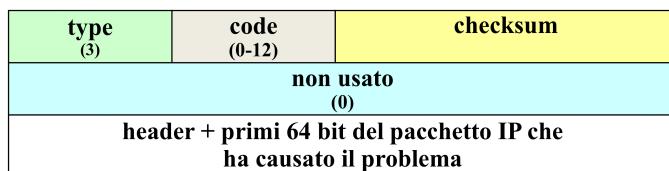


Type indica il tipo del messaggio:

- ERRORE: Destination Unreachable, Time Exceeded...
- QUERY: Address Mask Request...

Il ICMP non fixa errori, ma li segnala alla sorgente. I messaggi di errore contengono header + primi 8 byte del pacchetto problematico.

6.2.1 DESTINATION UNREACHABLE



Il router scatta un pacchetto per qualche motivo. Il campo code specifica il codice d'errore.

- 0 network unreachable
- 1 host unreachable
- 2 protocol unreachable
- 3 port unreachable
- 4 fragmentation needed and DF set
- 5 source route failed

6.2.2 TIME EXCEEDED

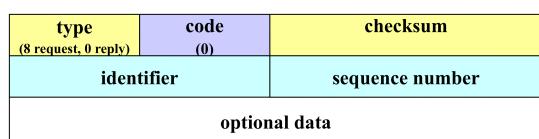


Mandato dal router sul corso TTL arrivi a 0. I.e.:

- code 0: un router ha scattato TTL a 0
- code 1: non tutti i frammenti sono arrivati all'host entro un tempo limite.

6.2.3 ECHO REQUEST

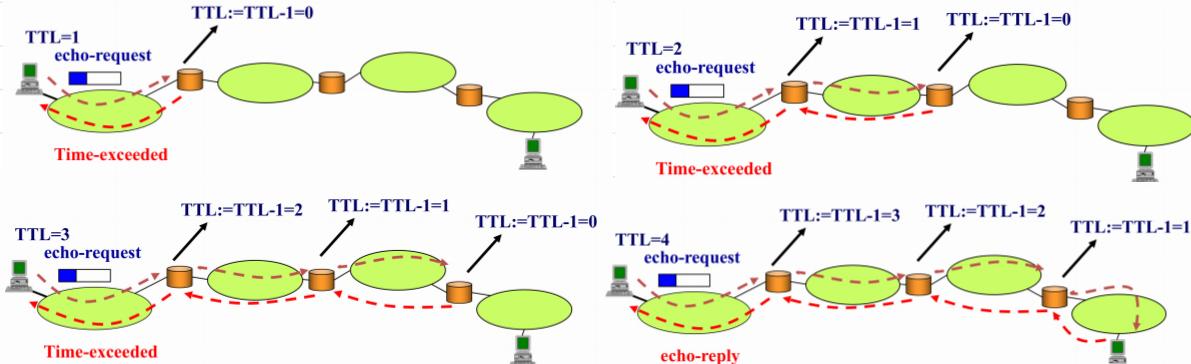
È un messaggio di diagnosi. Segue il paradigma Domanda/Risposta. Un host/router che riceve una Echo Request risponde con una Echo Reply.



Il campo identification viene scelto dal mittente. La risposta contiene lo stesso identificativo della domanda. Poi richiede comunque possono avere diverso ID ma sequence number diverso. Il mittente può aggiungere una sequenza di dati che verrà rimandata uguale per verificare errori.

I principali utenti delle Echo Requests sono "ping" e "traceroute".

Traceroute usa le Echo requests e TTL per tracciare il percorso dei pacchetti IP. Usa un incremento iterativo del TTL dei pacchetti IP con dentro uno Echo Request per sondare i vari router sul percorso.



Una alternativa è usare pacchetti UDP: la destinazione risponderà con un errore ICMP Port unreachable.

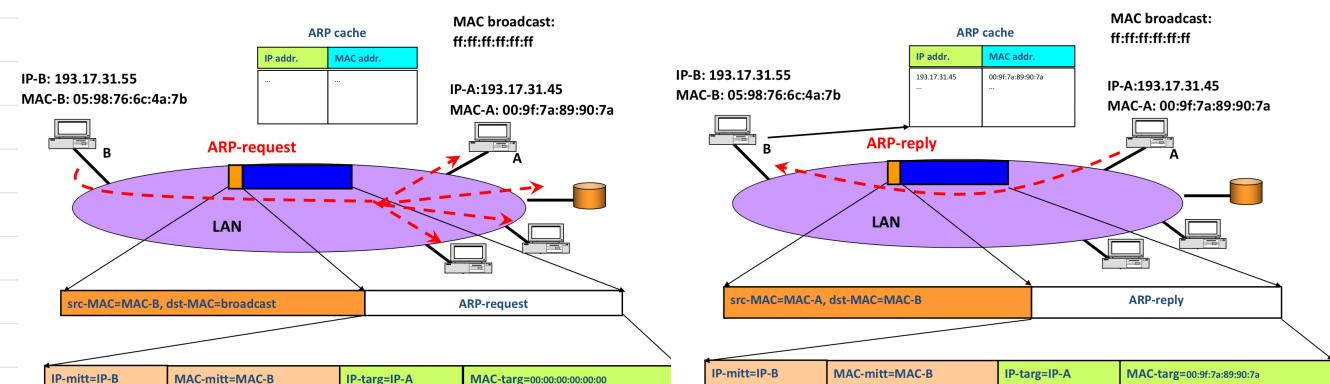
6.2.4 ADDRESS MASK REQUEST

Un host che invia al router locale per conoscere la propria netmask. È solitamente sostituito da DHCP e viene usato solo in fase di setup.

6.3 ARP e RARP

Nell'insieme direzionale abbiamo bisogno di sapere l'esistenza di una tabella di corrispondenza IP-MAC. Questa Tabella è generata da ARP. ARP si basa sul broadcast delle reti IP. Se nella ARP-cache (tabella IP-MAC) non è presente un MAC allora verrà broadcastata una ARP-request. Ogni host controlla se il MAC corrisponde al proprio e, se sì, risponde con una ARP-reply.

I messaggi ARP vengono incapsulati in frame di livello 2. Gli indirizzi MAC sono a 48 bit in notazione esadecimale. La ARP-request viene mandata al MAC broadcast FF:FF:FF:FF:FF:FF.



Il RARP esegue l'operazione inversa: arriva un IP e un MAC. Oggi è sostituito da DHCP. Il RARP viene usato per il booting in rete di macchine diskless.

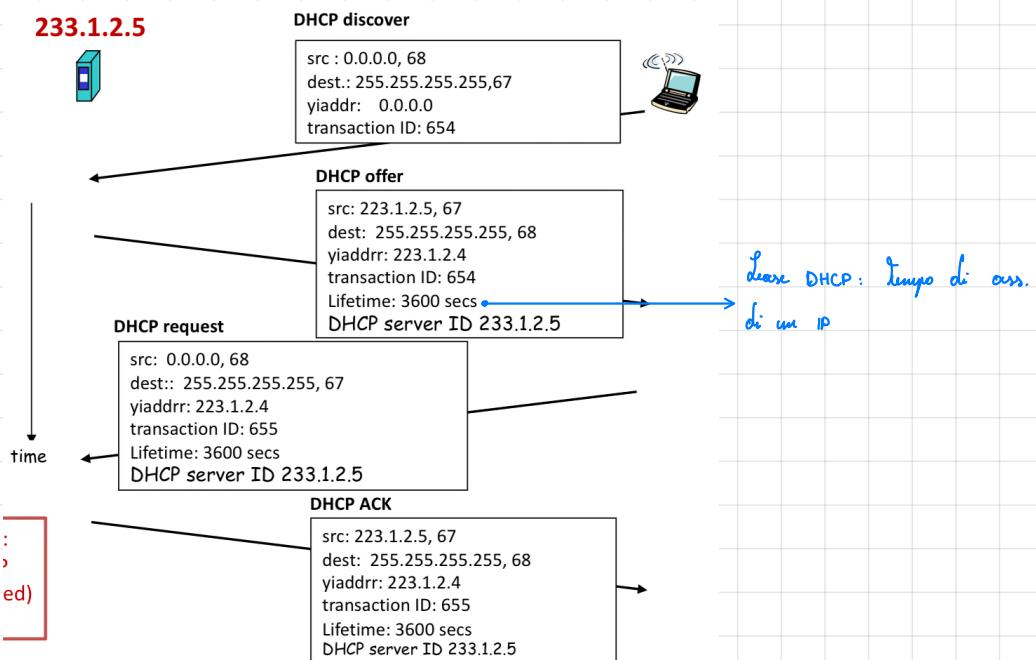
6.4 DHCP

Assegnare IP fissi ai vari host è scomodo e poco flessibile. È meglio usare un server che gestisce molti indirizzi e li allochi in modo dinamico. Ci sono 3 tipi di associazioni:

- **dinamica**: gli IP sono nuovi degli host, quindi si riutilizzano IP quando possibile.
- **statica**: il server ha una tabella IP-MAC che viene consultata ad ogni query.
- **autonoma**: il server automatizza la procedura di corrispondenza sulla tabella

Il **DHCP** risolve questo problema. È un protocollo client/server. Quando un host necessita IP manda in broadcast un messaggio di **DHCP DISCOVER**. Il server risponde con una offerta **DHCP OFFER**. Se il client accetta l'offerta manda una **DHCP REQUEST**. Il server conferma con **DHCP ACK**, mandando i parametri di configurazione. Oppure il client ha finito manda una **DHCP RELEASE**.

Il **DHCP** usa delle porte nede (67 server, 68 client) e tutti i messaggi sono mandati in broadcast.



È possibile che in una rete ci siano più server. È possibile anche avere un **DHCP relay**, una specie di proxy DHCP, permettendo al vero server di stare su un'altra rete IP da quella del client.

DHCP è un protocollo di livello 5; è trasportato da UDP e lavora con:

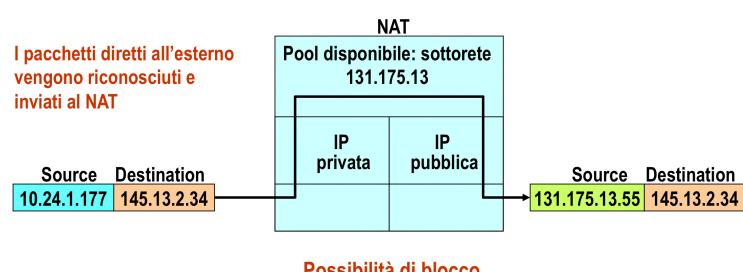
- SORGENTE: 0.0.0.0
- DESTINAZIONE: 255.255.255.255
- P. SORGENTE: 68
- P. DESTINAZIONE: 67

I parametri di configurazione sono principalmente:

- IP
- Netmask
- Gateway (router di default)
- DNS server

6.5 NAT

Il NAT traduce indirizzi privati in pubblici. È un servizio offerto a livello router.



Venne assegnato a ogni indirizzo privato un indirizzo pubblico da un pool. Le associazioni vengono tenute in una tabella.

Le associazioni hanno un tempo limitato pari alla durata della connessione. Nel caso del TCP è facile, ma nel caso di UDP è più difficile. Poiché alcune applicazioni trasportano IP (ASCII/BIN) nei loro messaggi, è necessaria la

(fornita dal firewall/Other)

funzionalità di Application Level Gateway (ALG) che traduce anche indirizzi indirizzi leggendo dentro i vari pacchetti. Gli ALG sono, precisamente, come dei proxy con la sola differenza dell'essere trasparenti. Gli ALG sono necessari per il corretto funzionamento del NAT.

Il NAT tradizionale (detto anche allorno NAT) permette l'inizio di sessioni solo dall'interno. Le informazioni di routing possono essere distribuite solo dall'interno all'interno. Ci sono due tipi di NAT Tradizionali: **BASIC** e **NAPT**:

- **BASIC NAT:** viene tradotto solo l'IP e c'è una corrispondenza diretta tra IP pubblici e privati. Possono esserci blocchi a causa della scarsa presenza di IP pubblici.
- **NAPT:** viene tradotta la coppia indirizzo-porta, in modo da permettere allo stesso IP pubblico di corrispondere a più IP privati.

Il NAT bidirezionale permette di usare un server pubblico con indirizzo privato. Per ottenere ciò, si usa il DNS che usa un unico spazio e collabora con il NAT. Questo tipo di DNS si chiama **dynamic-DNS**. Per far corrispondere IP:PORTA ai corrispondenti pubblici si usa il cosiddetto **port-forwarding**.