



Università  
degli Studi  
della Campania  
*Luigi Vanvitelli*

## Reti di Calcolatori e Cybersecurity

# ARP - DHCP - ICMP

Ing. Vincenzo Abate

• Come connetto livello 3 con livello 2?



# Trasmissione di un pacchetto IP

Quando un host deve trasmettere un pacchetto IP, lo strato di livello inferiore incapsula il pacchetto in una frame di livello 2

Le tecnologie di livello 2 sono molteplici

Nel seguito consideriamo due casi

- Interfacce di rete LAN basate su tecnologia Ethernet
- Interfacce di rete WAN basate su tecnologie che realizzano collegamenti seriali punto-punto

MAC consente di mettere in comunicazione host sullo stesso reticolato.

# Trasmissione di un pacchetto IP

L'incapsulamento di un pacchetto IP in una frame Ethernet richiede la conoscenza degli indirizzi di livello 2 (MAC address) dell'interfaccia mittente e destinataria su ogni hop che il pacchetto attraversa

Due scenari possibili:

Mittente e destinatario IP del pacchetto sono nella stessa subnet IP

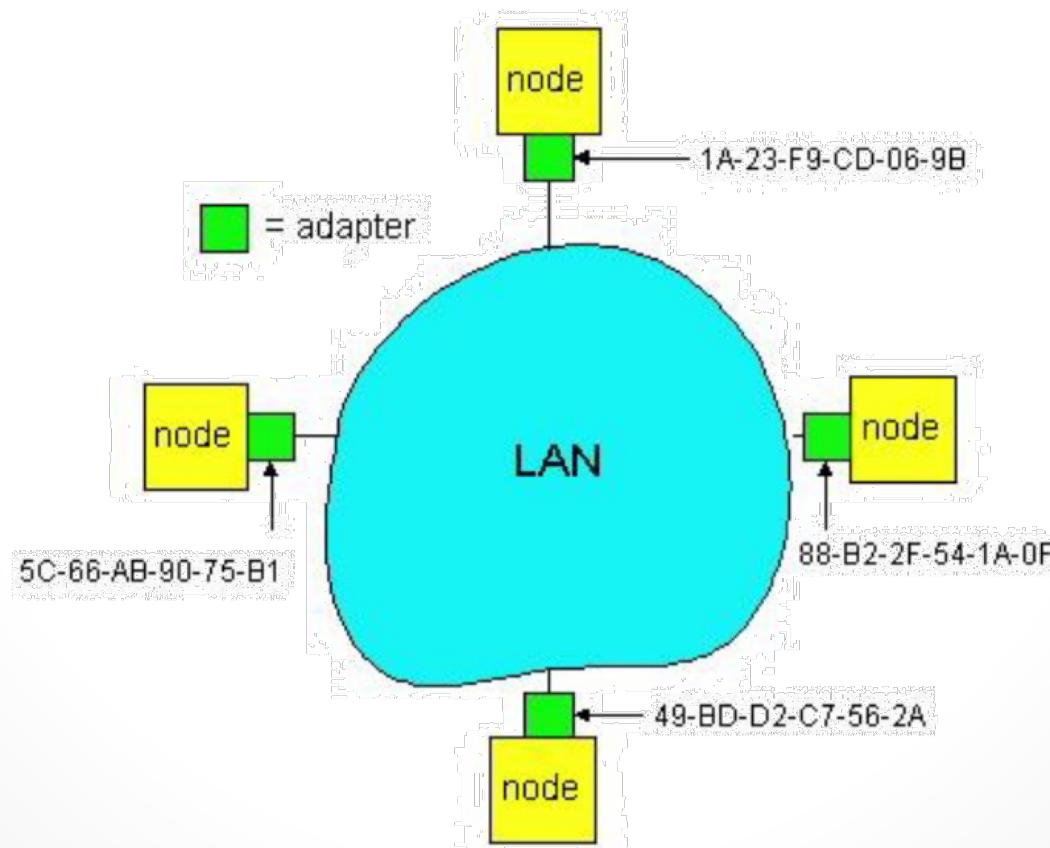
- Un solo hop

Mittente e destinatario IP del pacchetto sono in subnet IP diverse, collegate mediante uno o più router

- Molteplici hop: mittente-router, [router-router, ...], router-destinatario

# MAC address

Ogni scheda di rete in una LAN ha un indirizzo MAC (di 48 bit) univoco cablato nell'hardware della scheda dal costruttore



# Frame Ethernet



Una PDU di livello 2 (frame) Ethernet presenta nell'header:

- SA: indirizzo MAC di 48 bit che identifica la scheda che ha trasmesso la frame
- DA: indirizzo MAC di 48 bit che identifica la destinazione della frame

La destinazione può essere:

- Unicast – una specifica scheda collegata nella rete locale
- Broadcast – tutte le schede collegate alla rete locale
- Multicast – un sottoinsieme di schede collegate alla rete locale

# Frame Ethernet



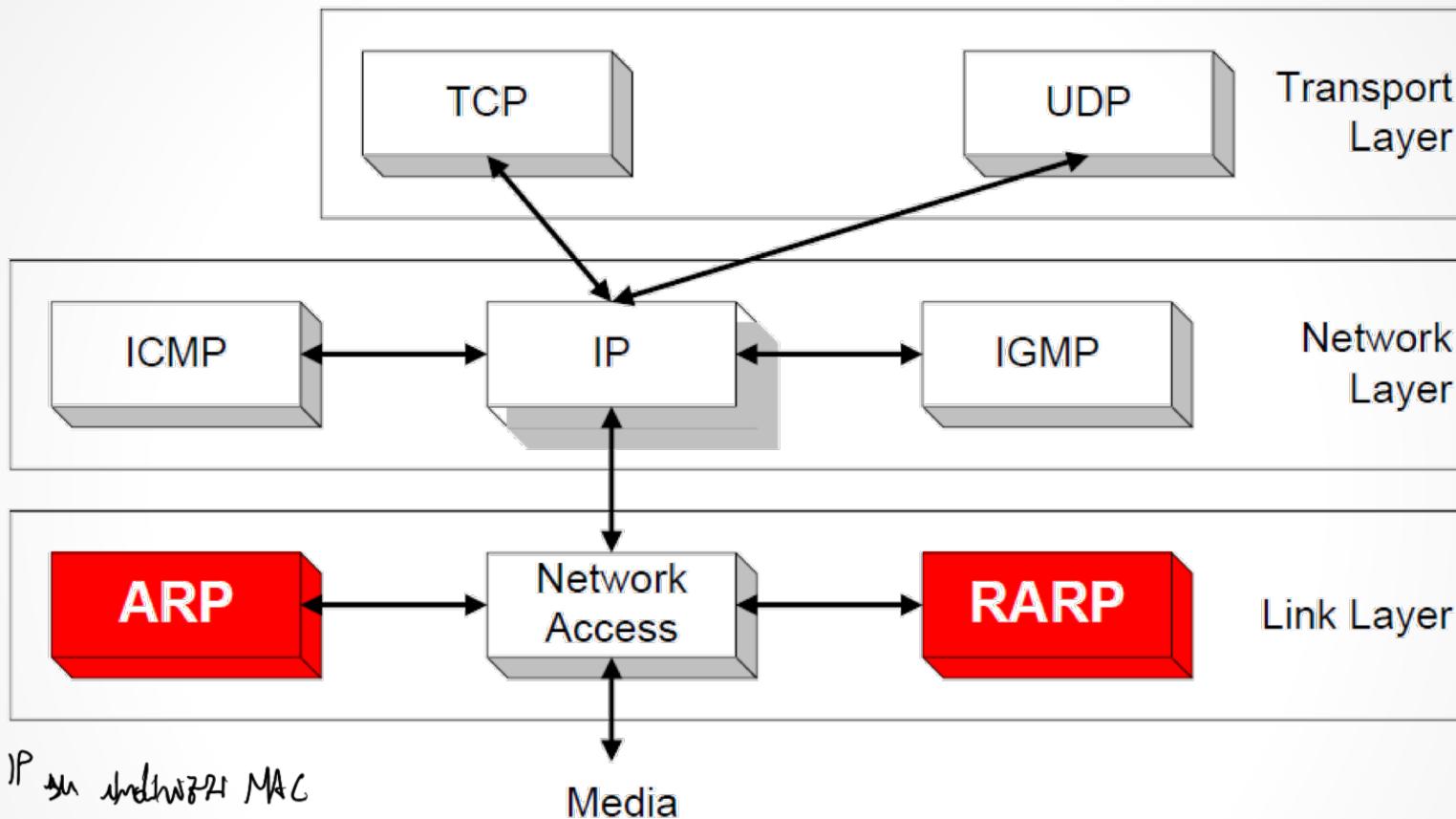
Gli indirizzi MAC sono rappresentati comunemente in notazione esadecimale  
↳ Col mac vado a livello fisico sulla scheda video per livello di astrazione

L'indirizzo MAC destinazione FF:FF:FF:FF:FF:FF indica una frame trasmessa in broadcast: tutti i sistemi collegati alla rete locale (inclusi i router) ricevono il pacchetto

Il campo Type (2 byte) indica il protocollo del pacchetto trasportato dalla frame nella parte Data (di lunghezza variabile)

- Type = 0x0800 indica il protocollo IPv4
- Type = 0x86DD indica il protocollo IPv6
- Type = 0x0806 indica il protocollo ARP (Address Resolution Protocol)
- Cfr.: <https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml>

# Protocolli ausiliari di livello 2



I protocolli **ARP** e **RARP** svolgono funzioni ausiliarie a supporto della trasmissione di datagrammi IP (ed in generale di un protocollo di livello rete) in reti locali con capacità di trasmissione broadcast (come, ad esempio, le LAN Ethernet)

# ARP e RARP

Il protocollo ARP serve ad associare un indirizzo di rete (es. IP) al corrispondente indirizzo MAC

- La sua funzione è necessaria quando un host vuole trasmettere un pacchetto IP ad una certa destinazione presente sulla rete locale e non ne conosce il corrispondente indirizzo MAC
- La conoscenza dell'indirizzo MAC è necessaria a costituire la frame secondo la struttura vista nella slide precedente
- ARP è definito in RFC 826

Il protocollo RARP serve ad associare un indirizzo MAC al corrispondente indirizzo di rete (es. IP) *fù nel confronto; es. workstation che non*

- Questa esigenza si presenta in circostanze particolari *hanno diritti, non puoi configurare IP,*

# ARP e RARP

## Primo caso

l'host destinazione è sulla stessa LAN (subnet IP)

## Secondo caso

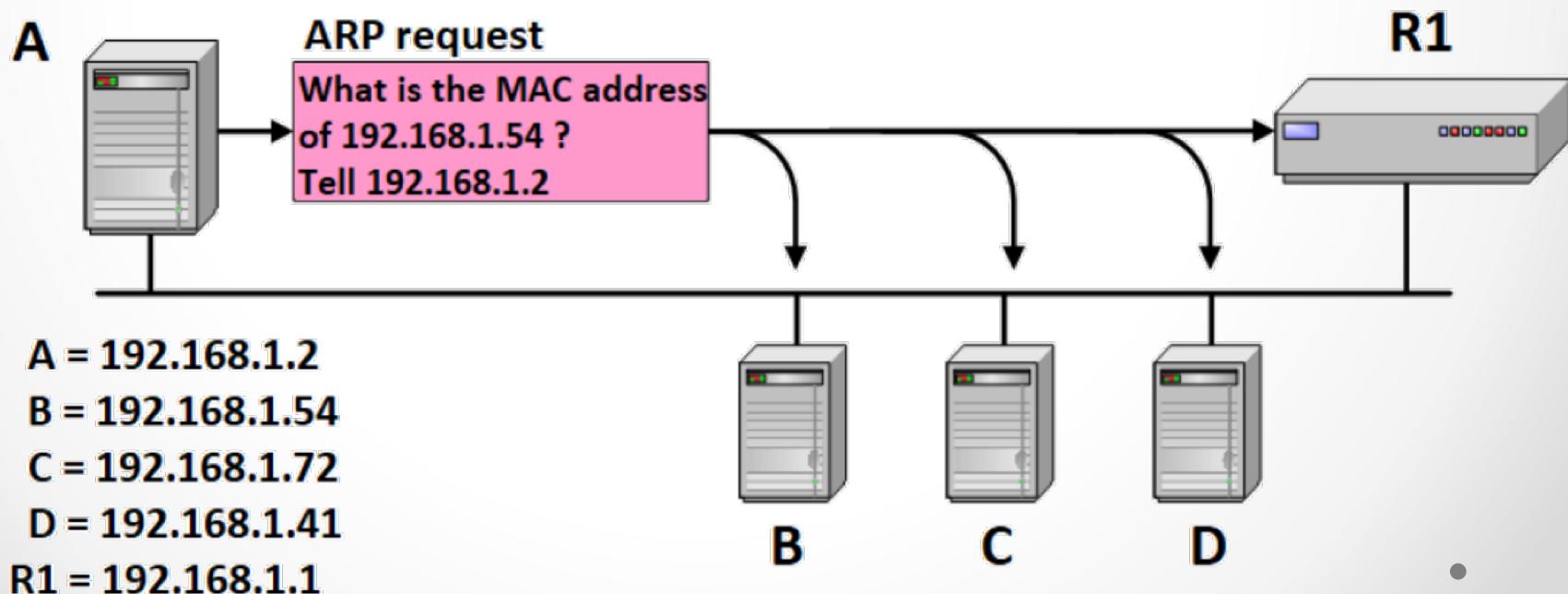
l'host destinazione non è sulla stessa LAN (subnet IP)

Indirizzo di rete è  
↑ lo stesso

# ARP e RARP

**Primo scenario:** A vuole trasmettere un pacchetto IP a B e la destinazione è nella stessa LAN (subnet IP) del mittente

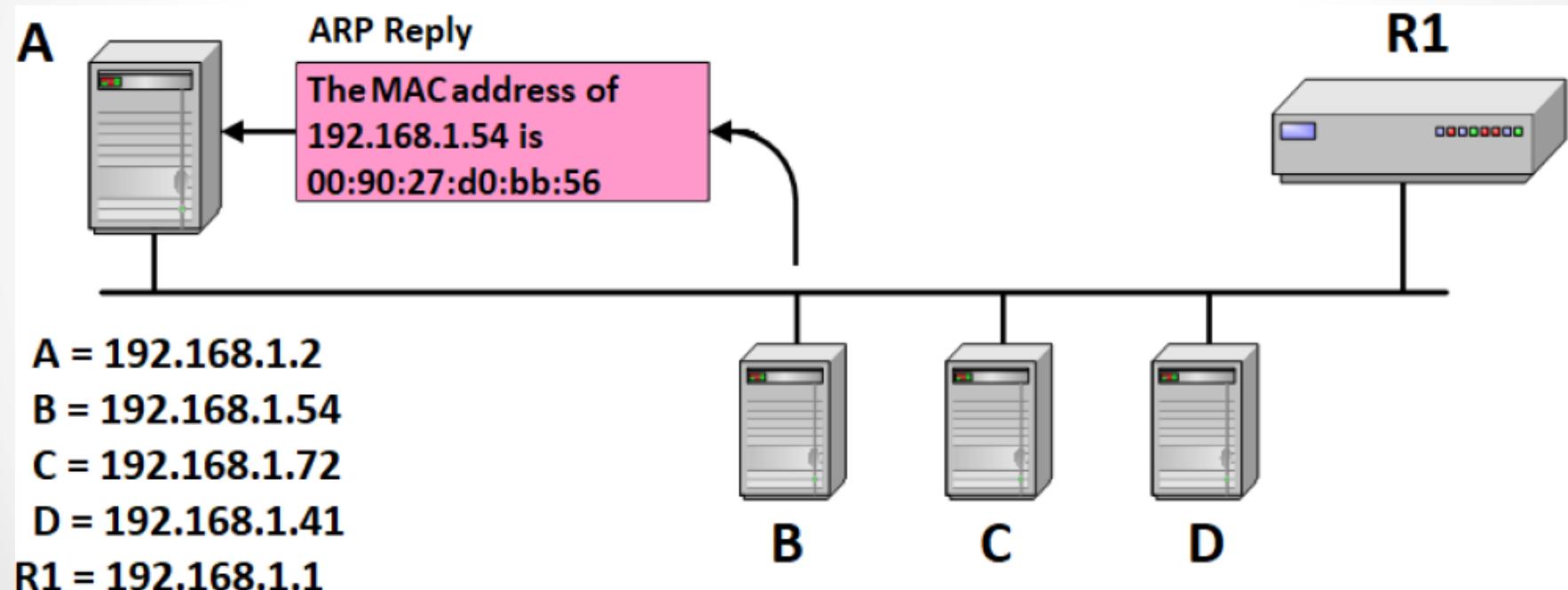
- A chiede mediante ARP di conoscere il MAC address associato alla destinazione B (target IP) direttamente raggiungibile
- La richiesta ARP è trasmessa in una frame con indirizzo MAC destinazione broadcast FF:FF:FF:FF:FF:FF



# ARP e RARP

**Primo scenario:** A vuole trasmettere un pacchetto IP a B e la destinazione è nella stessa LAN (subnet IP) del mittente

- La risposta ARP è inviata da B direttamente ad A



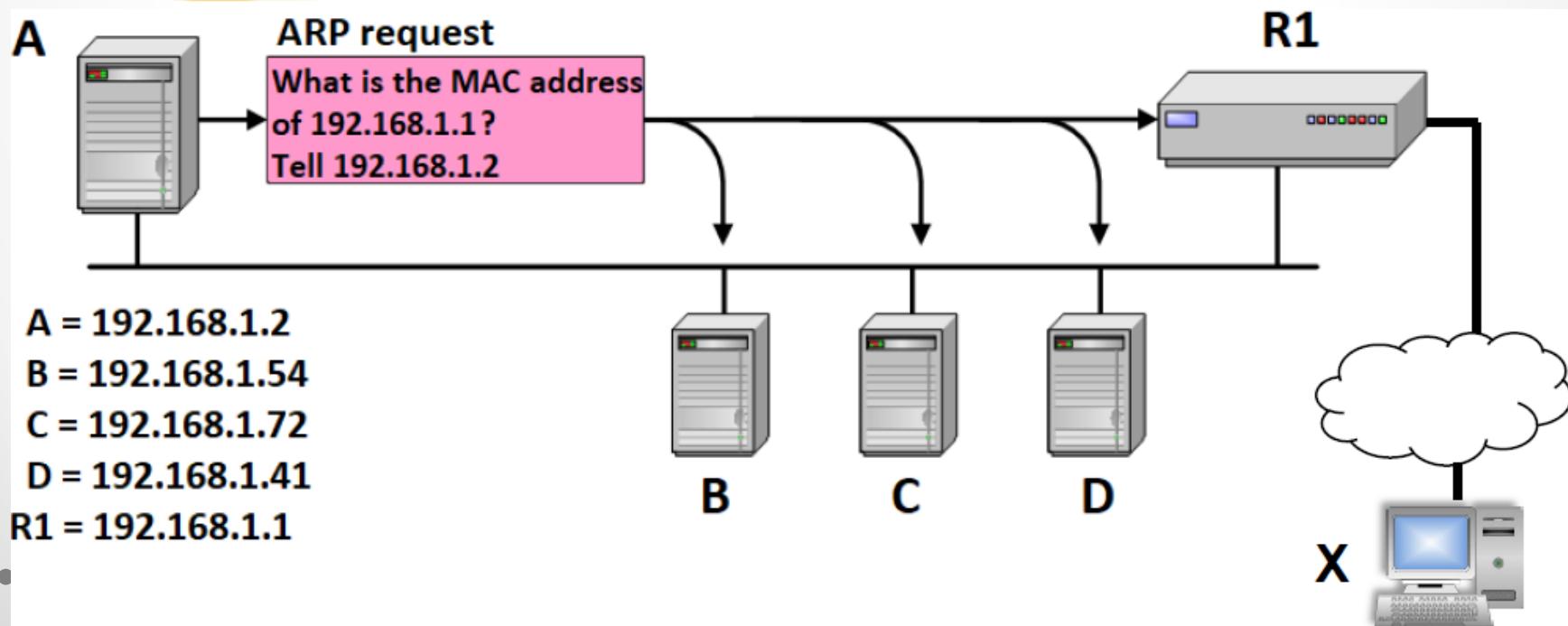
A sa che destinazione

↑ non è nella stessa subnet. Sa dalla tabella di routing chi chiamare

# ARP e RARP

**Secondo scenario:** A vuole trasmettere un pacchetto IP a X e : la destinazione è fuori dalla LAN (subnet IP) del mittente

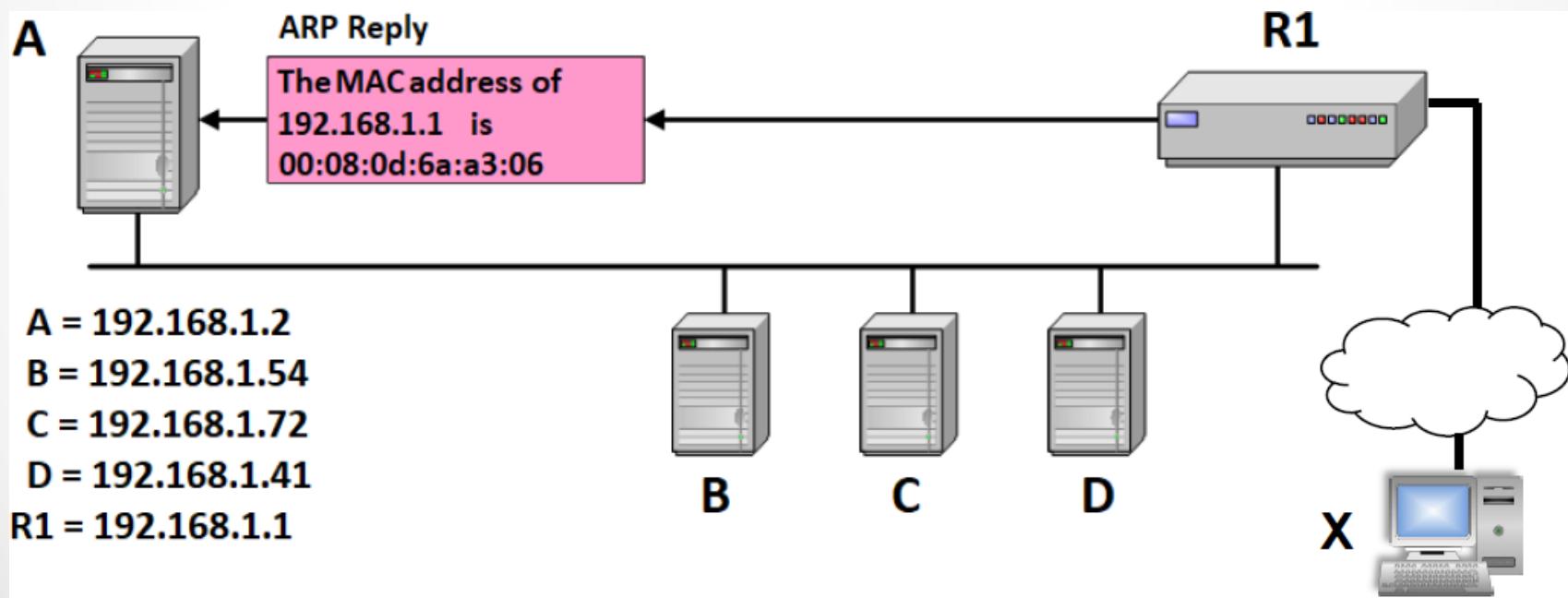
- In base alla sua tabella di routing, A determina l'indirizzo R1 del gateway associato alla destinazione X
- A chiede mediante ARP di conoscere il MAC address associato al gateway R1 (target IP) direttamente raggiungibile
- La richiesta ARP è trasmessa in una frame con indirizzo MAC destinazione broadcast FF:FF:FF:FF:FF:FF



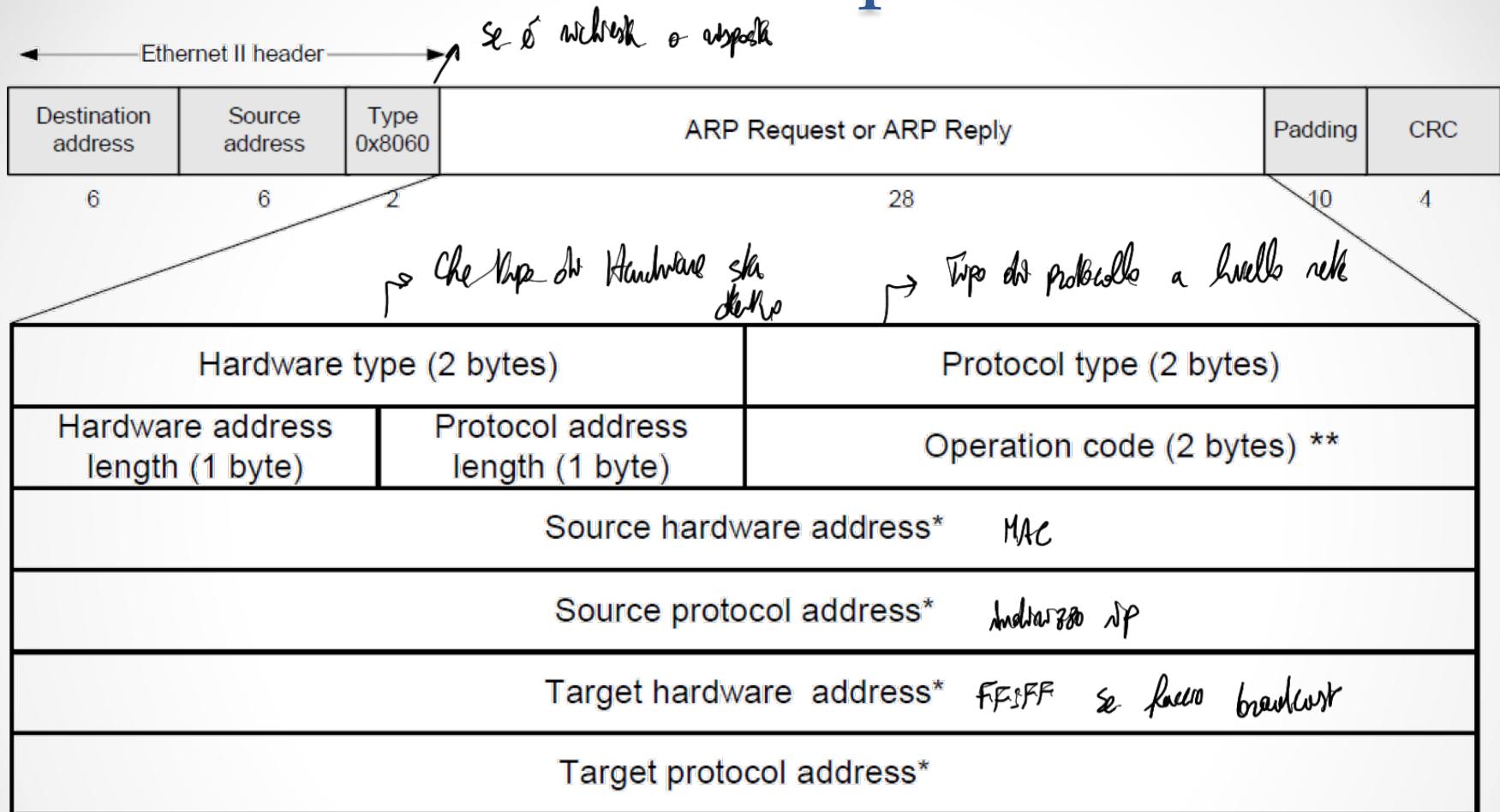
# ARP e RARP

Secondo scenario: A vuole trasmettere un pacchetto IP a X e : la destinazione è fuori dalla LAN (subnet IP) del mittente

- La risposta ARP è inviata dal gateway R1 direttamente ad A



# ARP struttura pacchetto



\*The length of the address fields is determined by the corresponding address length fields 12

- \*\* OpCode = 0x0001 → request
- OpCode = 0x0002 → reply

# ARP struttura pacchetto

La denominazione dei campi dei messaggi ARP usa i termini:

**Protocol** per riferirsi a indirizzi di rete (layer-3)

- tipicamente IPv4 a 32 bit (4 byte)

**Hardware** per riferirsi ad indirizzi fisici (layer-2)

- tipicamente MAC a 48 bit (6 byte)

**Source** per riferirsi al mittente del messaggio ARP

**Target** per riferirsi al destinatario del messaggio ARP

Complessivamente, un messaggio ARP contiene 4 indirizzi:

1. **Source hardware**
2. **Source protocol**
3. **Target hardware**
4. **Target protocol**



# ARP struttura pacchetto

Il campo **Operation Code** discrimina tra due tipi di messaggi:

ARP request con OpCode = 0x0001

ARP reply con OpCode = 0x0002

In un contesto nel quale ARP si usa per la risoluzione di indirizzi MAC rispetto ad indirizzi IP:

1. **source hardware address** specifica il MAC address dell'host mittente
2. **source protocol address** specifica l'indirizzo IP del mittente
3. **target hardware address** contiene:
  - FF:FF:FF:FF:FF:FF in una richiesta ARP "normale"
  - 00:00:00:00:00:00 nei messaggi **ARP Probe** ed **ARP Announcement**
  - l'indirizzo MAC del destinatario in una risposta
4. **target protocol address** contiene:
  - l'indirizzo IP di cui si desidera conoscere il MAC in una richiesta
  - l'indirizzo IP del destinatario in una risposta

# ARP caching

- Per ridurre il traffico sulla rete e ridurre il tempo necessario all'invio di nuovi pacchetti IP, ogni host mantiene in una cache le corrispondenze tra indirizzi logici e fisici precedentemente apprese
- Ciascuna corrispondenza viene mantenuta per un tempo limitato (alcuni minuti) e poi eliminata allo scadere di un timeout
- Per rinnovare le corrispondenze prossime alla scadenza, un host può inviare una richiesta ARP unicast al MAC address associato all'indirizzo IP
- Questo comportamento è definito "**Unicast Poll**" nella sezione 2.3.2.1 ARP Cache Validation di **RFC 1122**
- In questo modo si evita la trasmissione di una richiesta in broadcast

# ARP command

In quasi tutti i sistemi operativi, il comando arp consente di consultare le corrispondenze MAC-IP già presenti nella cache ARP dell'host

Il comando arp –f elimina tutte le corrispondenze presenti in cache (operazione di flush)

Esempio di output del comando arp su un sistema Windows

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	20-b0-01-1d-70-b0	dinamico
192.168.1.195	22-b0-01-1d-70-b9	dinamico
192.168.1.218	82-69-d7-6f-43-dd	dinamico
192.168.1.240	3c-52-82-08-ef-c2	dinamico
255.255.255.255	ff-ff-ff-ff-ff-ff	statico

Si osservi che l'indirizzo IP speciale 255.255.255.255 usato per inviare un pacchetto IP in broadcast nella propria rete è associato al MAC address broadcast FF:FF:FF:FF:FF:FF

Questa associazione è considerata statica in quanto non ottenuta tramite ARP

# Gratuitous ARP

Messaggio di risposta

Un "gratuitous ARP" (o GARP) è un messaggio ARP reply:

Trasmesso in una frame con MAC destinazione FF:FF:FF:FF:FF:FF  
con:

1. source hardware address dell'host mittente
2. source protocol address dell'host mittente
3. target hardware address FF:FF:FF:FF:FF:FF
4. target protocol address dell'host mittente

Risposta dove m<sup>ac</sup> 2 e 2 n<sup>l</sup>  
verso m<sup>ac</sup> 1, come destinazione a  
m<sup>ac</sup> 3 m<sup>ac</sup> verso e per broadcast

▼ Address Resolution Protocol (reply/gratuitous ARP)	
Hardware type:	Ethernet (1)
Protocol type:	IPv4 (0x0800)
Hardware size:	6
Protocol size:	4
Opcode:	reply (2)
[Is gratuitous:	True]
Sender MAC address:	00:53:ff:ff:bb:bb
Sender IP address:	10.0.0.22
Target MAC address:	ff:ff:ff:ff:ff:ff
Target IP address:	10.0.0.22

# Gratuitous ARP perché?

Un GARP è un messaggio di risposta ARP *unsolicited* cioè non generato per effetto di una precedente richiesta

Messaggi GARP possono essere generati se:

- L'host desidera popolare le ARP cache degli altri host della rete locale
  - Questo effetto potrebbe non essere raggiunto in quanto un host non è obbligato ad inserire le corrispondenze apprese mediante GARP *Non più fatta devono essere aggiornata*
- L'host ha modificato il proprio indirizzo IP oppure ha subito una disconnessione dalla rete e desidera aggiornare del cambiamento gli altri host (e switch) della rete locale
  - *Avviso tutto che la mia associazione è cambiata*

# ARP probe

Un "ARP Probe" è un messaggio ARP request:

Trasmesso in una frame con MAC destinazione FF:FF:FF:FF:FF:FF  
con:

1. source hardware address dell'host mittente
2. source protocol address 0.0.0.0
3. target hardware address 00:00:00:00:00:00
4. target protocol address indirizzo oggetto del "probe"

▼ Address Resolution Protocol (request)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: 00:50:56:c0:00:01
Sender IP address: 0.0.0.0
Target MAC address: 00:00:00:00:00:00
Target IP address: 192.168.174.111

# ARP probe perché?

Un ARP Probe può essere usato per verificare che nella rete locale non ci siano altri host con lo stesso indirizzo IP target

- L'eventuale ricezione di una risposta al probe è sintomo che un altro host nella rete locale è già configurato con l'indirizzo IP target
- Usando un ARP Probe, anziché un Gratuitous ARP, si evita di inserire una entry duplicata nelle cache degli altri host della rete locale, cioè si evita il verificarsi del problema della duplicazione di un indirizzo IP  
*Non so se duplicate esiste*

# ARP Announcement

Un "ARP Announcement" è un messaggio ARP request:

Trasmesso in una frame con MAC destinazione FF:FF:FF:FF:FF:FF

con:

1. source hardware address dell'host mittente
2. source protocol address dell'host mittente
3. target hardware address 00:00:00:00:00:00 oppure  
FF:FF:FF:FF:FF:FF
4. target protocol address dell'host mittente

Address Resolution Protocol (request/gratuitous ARP)	
Hardware type:	Ethernet (1)
Protocol type:	IPv4 (0x0800)
Hardware size:	6
Protocol size:	4
Opcode:	request (1)
[Is gratuitous:	True]
Sender MAC address:	00:50:56:c0:00:01
Sender IP address:	192.168.174.111
Target MAC address:	00:00:00:00:00:00
Target IP address:	192.168.174.111

# ARP Announcement Perché?

Con lui possono aggiornare ma non è detto. Ma è un messaggio di richiesta.

Un ARP Announcement è simile ad un gratuitous ARP perché:

**source protocol address == target protocol address**

con la differenza di essere un messaggio di richiesta

A differenza di un ARP Probe, un ARP Announcement trasmette una associazione completamente definita tra un indirizzo MAC sorgente ed un indirizzo IP sorgente

↓ Questo ip e questo mac sono associati

- Gli host della rete locale che ricevono l'announcement possono aggiornare le proprie ARP cache

I messaggi ARP announcement vengono usati con le stesse finalità dei messaggi gratuitous ARP

→ Se uno ha lo stesso ip risponde e mi invia un messaggio con lo stesso ip.

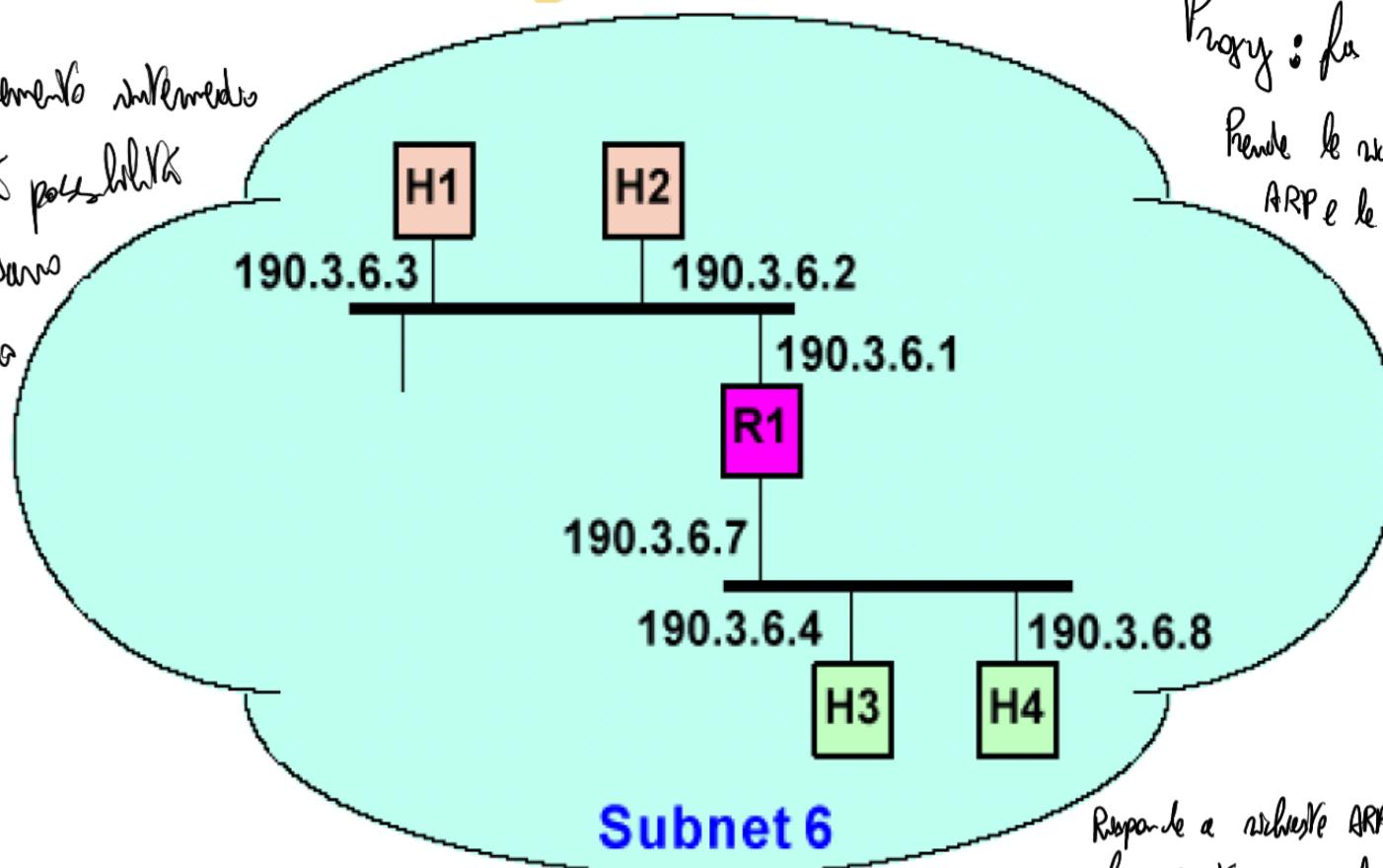
Anche un ARP Announcement può essere usato per verificare che nella rete locale non ci siano altri host con lo stesso indirizzo IP target

- L'eventuale ricezione di una risposta è sintomo che un altro host nella rete locale è già configurato con l'indirizzo IP target

# ARP Proxy

- Permette di usare la stessa subnet su due o più reti fisiche diverse

Molti elementi intermedio  
che dà possibilità  
a reti che usano  
stesso indirizzo  
della subnet



Proxy : fa da tramite  
Prende le richieste  
ARP e le risolve.

Risponde a richieste ARP di host  
che appartengono a rete che  
non possono raggiungere.  
⇒ A 1a2 le richieste passano a R2.

# RARP - Reverse ARP

Il protocollo RARP svolge il ruolo opposto ad ARP

Indirizzo fisico (MAC) → indirizzo logico (IP)

Usato per sistemi diskless:

- X terminal, diskless workstation
- Al boot non conoscono il loro indirizzo IP

Presuppone l'esistenza nella rete locale di un server RARP che risponde alla richiesta

Questo protocollo è oggi superato da DHCP che, oltre ad assegnare un indirizzo IP, consente di fornire all'host ulteriori parametri di configurazione (netmask, default gateway, server DNS locale, ecc.)

# Dinamic Host Configuration Protocol

A livello APPlicativo

Il DHCP (Dynamic Host Configuration Protocol) fornisce un meccanismo per assegnare dinamicamente gli indirizzi IP ed i parametri di configurazione ad un host tramite TCP/IP (RFC 1533, 1534, 1541 e 1542)

Estensione del protocollo BOOTP *bootstrapping*

# Dinamic Host Configuration Protocol

Tramite **DHCP** è possibile assegnare:

- **indirizzo IP e subnet mask,**
- **DNS,**
- **server WINS**
- **gateway** (default gateway della rete)

che il client dovrà utilizzare.

Può offrire altri parametri

# Dinamic Host Configuration Protocol

**DHCP Server** è una macchina che si fa carico di distribuire gli indirizzi e gli altri parametri di configurazione ai client che ne fanno richiesta.

**Scope** - range degli indirizzi distribuibili

**Lease** - periodo di validità di una configurazione, alla scadenza il client deve richiederla nuovamente.

Il client **affitta** il suo indirizzo di rete per un determinato periodo di tempo.



# Dinamic Host Configuration Protocol

Il processo di configurazione DHCP avviene in quattro fasi:

1. **dhcpdiscover** - richiesta di IP
2. **dhcpoffer** - offerta di IP
3. **dhcprequest** - selezione di IP
4. **dhcpack** - conferma di IP

Mi aggiendo al  
miglior  
caso

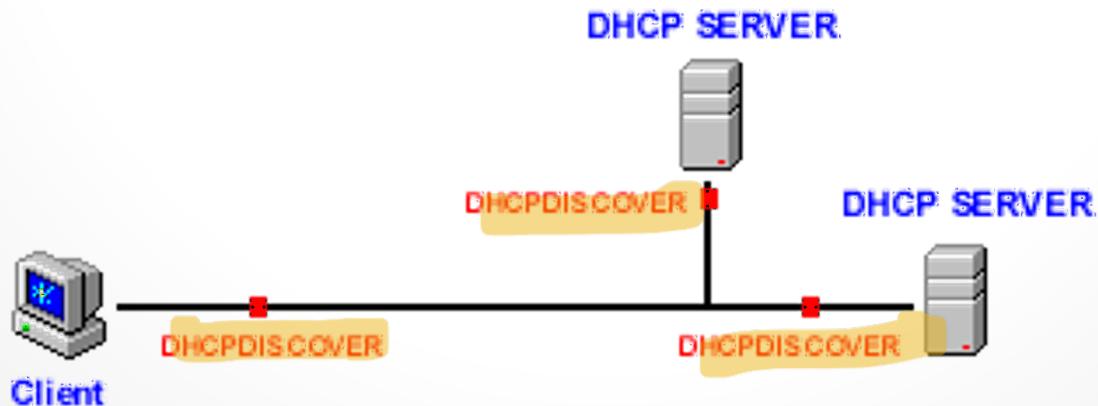
# Dinamic Host Configuration Protocol

## DHCPDISCOVER - Richiesta di IP

Il client manda una richiesta via TCP/IP all'indirizzo broadcast:

- mittente 0.0.0.0 Qualecosa che non so'
- destinazione 255.255.255.255

la richiesta contiene l'indirizzo MAC della scheda di rete e il nome del computer.

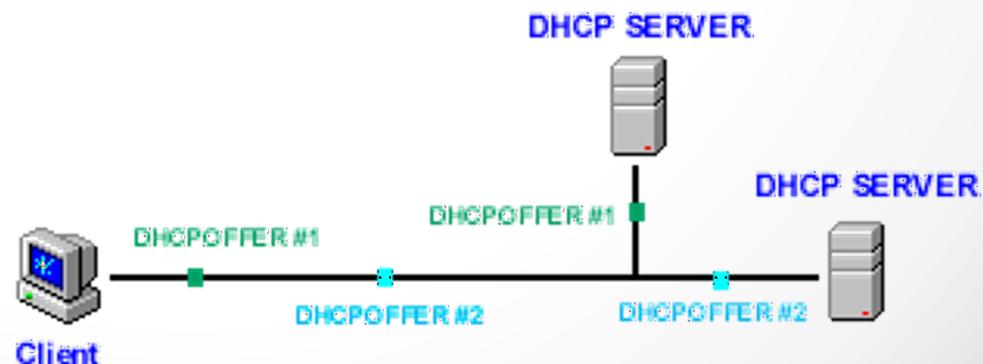


# Dinamic Host Configuration Protocol

## DHCPOFFER - Offerta di IP

Il server DHCP manda un messaggio broadcast contenente un'indirizzo IP selezionato dallo SCOPE e l'indirizzo MAC del client

Il client utilizzerà il primo IP che riceverà, nel caso che ci siano più server DHCP sulla rete, gli altri verranno ignorati.



# Dinamic Host Configuration Protocol

DHCP OFFER

Source IP Address = 198.189.20.1

Dest IP Address = 255.255.255.255

Offered IP Address = 198.189.20.78

Client MAC Address = 44-45-53-54-00-00

Subnet Mask = 255.255.255.255 gw c'c 0

Length of Lease = 72 Hours

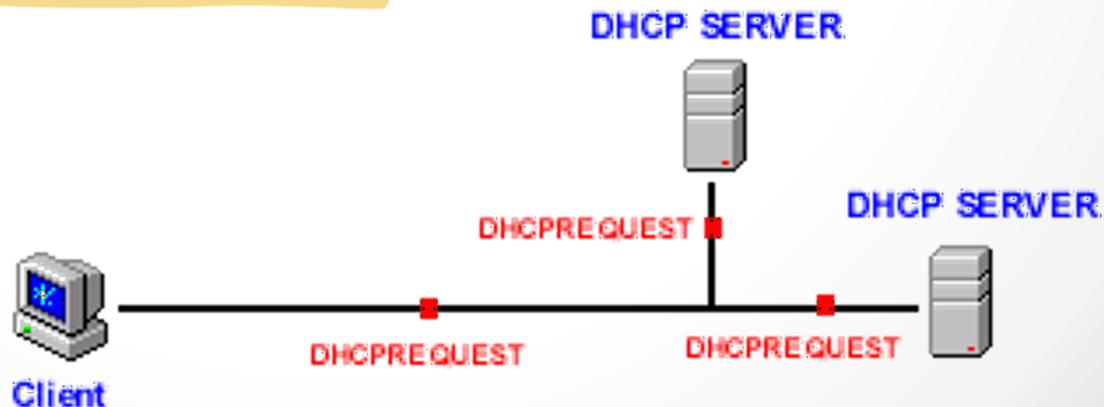
Server Identifier = 198.189.20.1 ch snelle nf dhcp

# Dinamic Host Configuration Protocol

## DHCPREQUEST - Selezione di IP

Dopo aver accettato un IP, il client manda un messaggio broadcast informando tutti i server DHCP che ha accettato un IP.

Il messaggio include l'indirizzo del server DHCP che ha mandato l'IP che è stato accettato → tutti gli altri server ritirano le loro offerte.

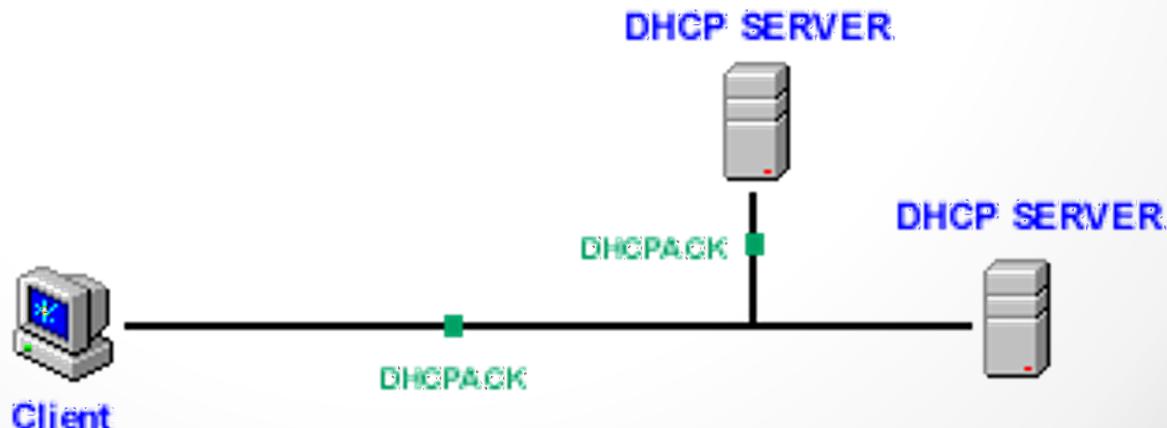


# Dinamic Host Configuration Protocol

## DHCPACK - Conferma di IP

Il server DHCP manda un messaggio di conferma al client, contenente il valore di Lease per l'IP.

Quando il client riceve il messaggio di ACK completa la configurazione del TCP/IP.



# Dinamic Host Configuration Protocol

## DHCPACK

**Source IP Address = 198.189.20.1**

**Dest. IP Address = 198.189.20.78**

**Offered IP Address = 198.189.20.78**

**MAC Address = 44-45-53-54-00-00**

**Subnet Mask = 255.255.255.0**

**Lenth of Lease = 72 Hours**

**Server Identifier = 198.189.20.1**



**DHCP SERVER\_1**

# Dinamic Host Configuration Protocol

## DHCPNACK - Negazione di IP

Il server DHCP manda un messaggio di rifiuto al client se non può assegnare la configurazione richiesta.



Il procedimento va ripetuto.

# Dinamic Host Configuration Protocol

controlla se non questo si rinnova



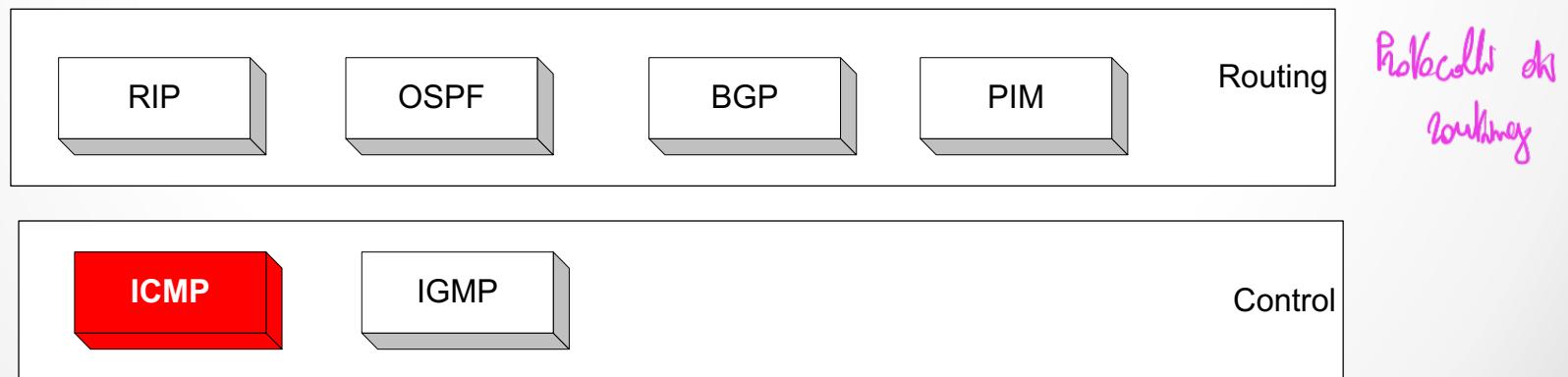
## Rinnovo DHCP

tempo di cessione

- Il client DHCP viene riavviato e il tempo di lease non è scaduto (DHCPREQUEST e DHCPACK).
- 50% del tempo di lease: il client invia messaggio al server DHCP per rinnovare il lease.  
→ Se prima non ho avuto risposta
- 85% del tempo di lease: il client invia in broadcast una richiesta DHCP per rinnovare la configurazione. Se il DHCP server che aveva precedentemente concesso la licenza riceve il messaggio, la rinnova, altrimenti viene inviato un DHCPNACK e quindi il client dovrà ripetere le quattro fasi iniziali.

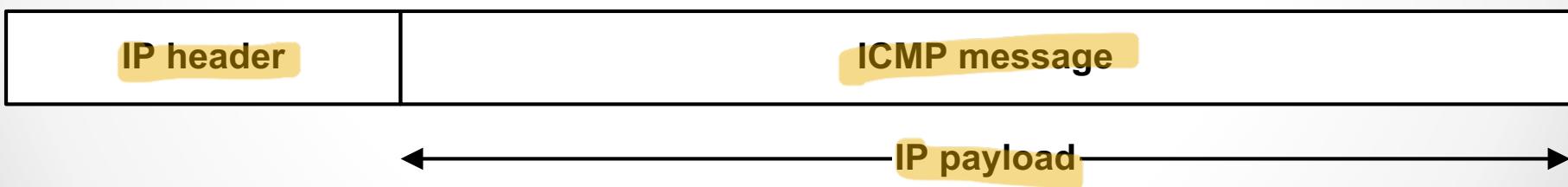
# Internet Control Message Protocol (ICMP)

- The IP (Internet Protocol) relies on several other protocols to perform necessary control and routing functions:
  - Control functions (ICMP)
  - Multicast signaling (IGMP)
  - Setting up routing tables (RIP, OSPF, BGP)

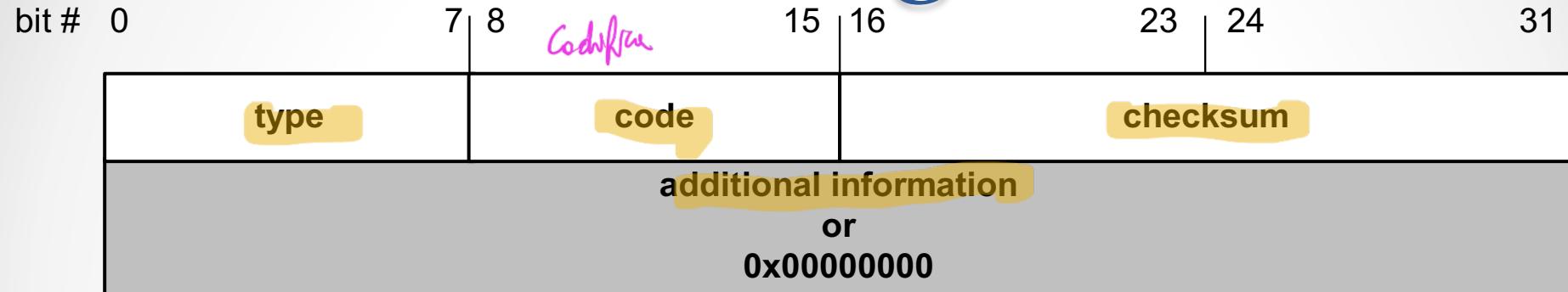


# Overview

- The **Internet Control Message Protocol (ICMP)** is a helper protocol that supports IP with facility for
  - Error reporting
  - Simple queries *Request*
- ICMP messages are encapsulated as IP datagrams:



# ICMP message format

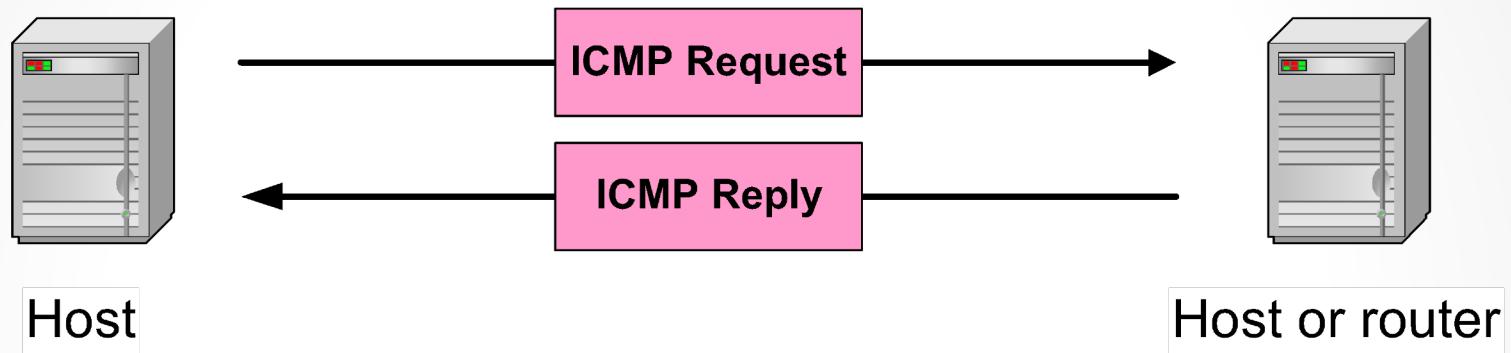


## 4 byte header:

- Type (1 byte): type of ICMP message
- Code (1 byte): subtype of ICMP message
- Checksum (2 bytes): similar to IP header checksum.  
Checksum is calculated over entire ICMP message

If there is no additional data, there are 4 bytes set to zero.  
→ each ICMP messages is at least 8 bytes long

# ICMP Query message



## ICMP query:

- Request sent by host to a router or host
- Reply sent back to querying host

# Example of ICMP Queries

Type/Code: Description

8/0 Echo Request

0/0 Echo Reply

The ping command uses Echo Request/Echo Reply

13/0 Timestamp Request

14/0 Timestamp Reply

10/0 Router Solicitation

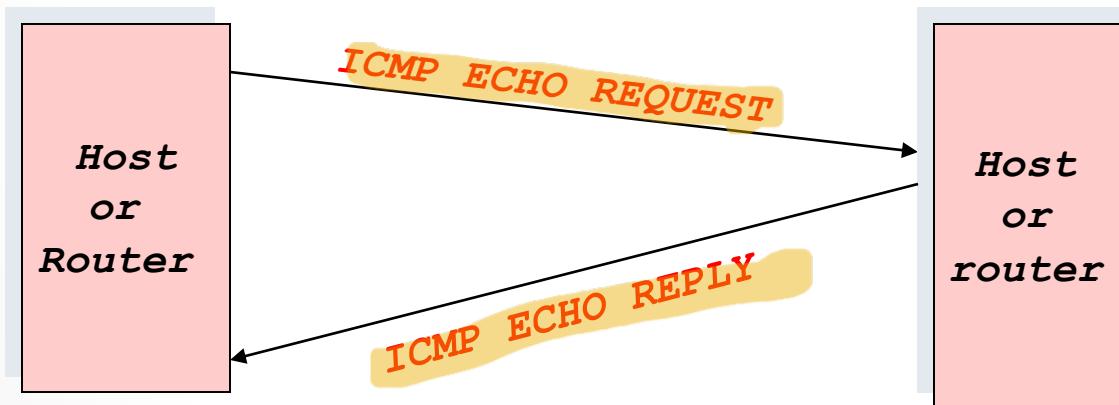
9/0 Router Advertisement

Dnsname routing

# Example of a Query:

## Echo Request and Reply

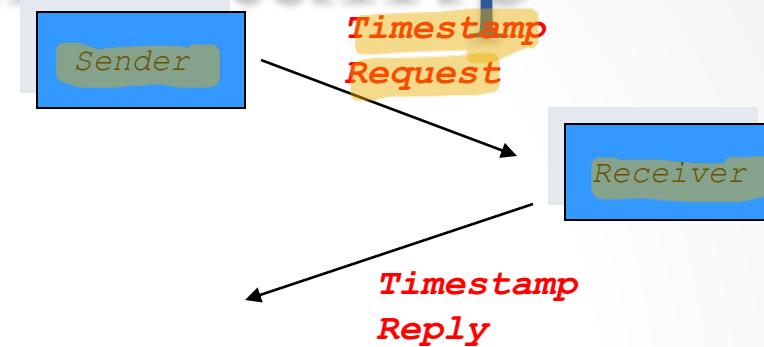
- Ping's are handled directly by the kernel
- Each Ping is translated into an ICMP Echo Request
- The Ping'ed host responds with an ICMP Echo Reply



Ping: comando che manda  
sequenza di messaggi  
e misura tempo e info

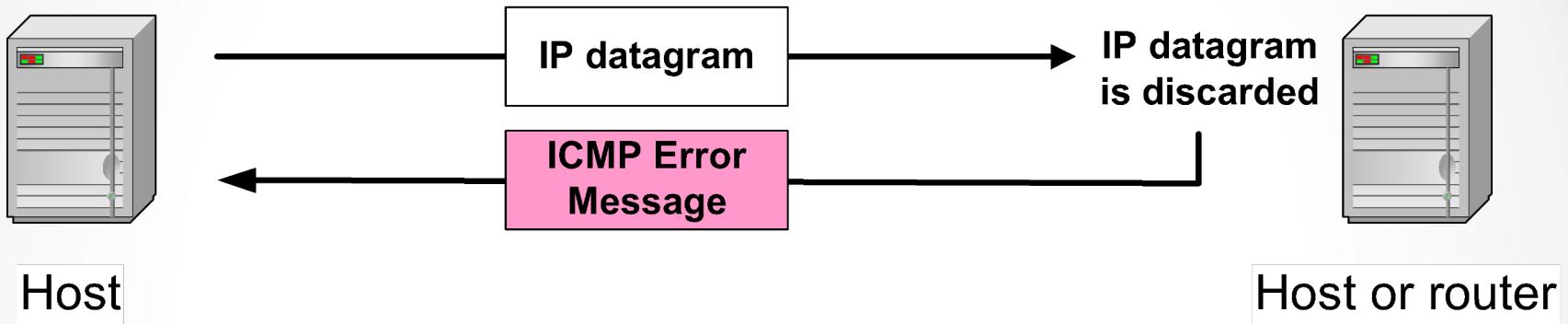
# Example of a Query: ICMP Timestamp

- A system (host or router) asks another system for the current time.
- Time is measured in milliseconds after midnight UTC (Universal Coordinated Time) of the current day
- Sender sends a request, receiver responds with reply



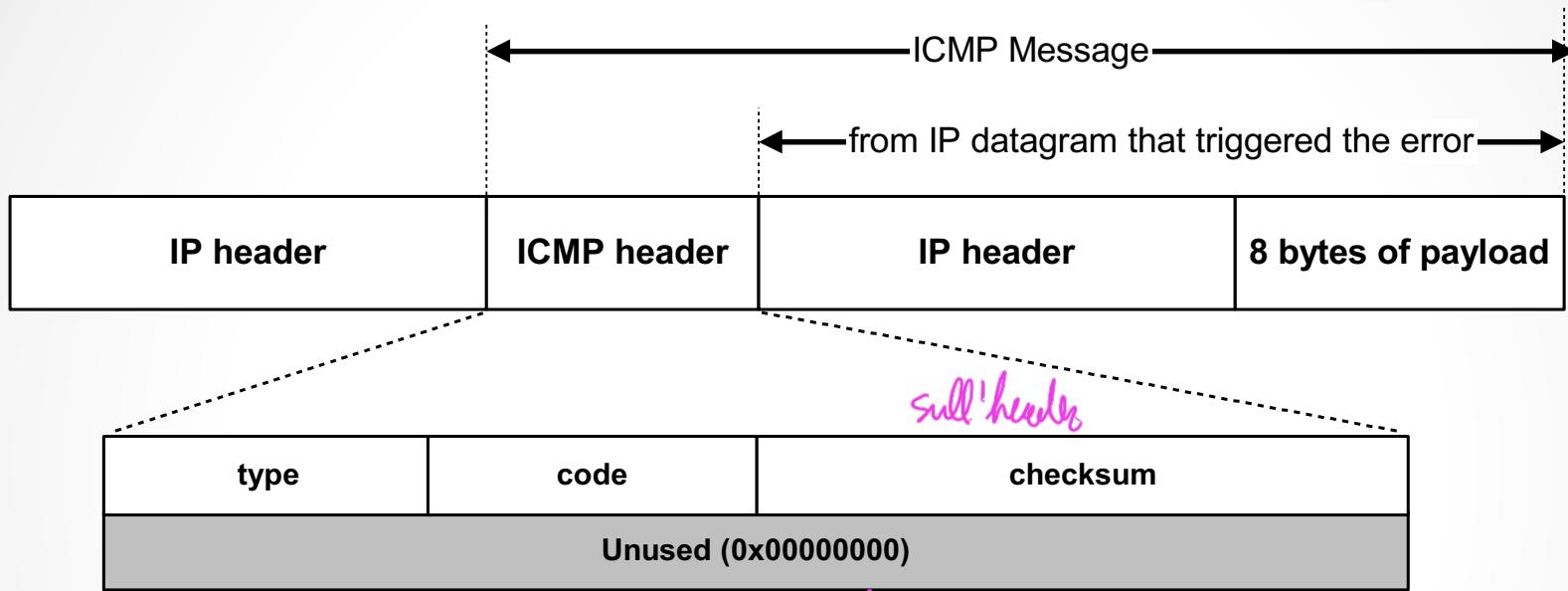
Type (=13 OR 14)	Code (=0)	Checksum
identifier		sequence number
	32-bit sender timestamp	
	32-bit receive timestamp	
	32-bit transmit timestamp	

# ICMP Error message



- **ICMP error messages report error conditions**
- **Typically sent when a datagram is discarded**
- **Error message is often passed from ICMP to the application program** : fragmentation needed

# ICMP Error message



- ICMP error messages include the complete IP header and the first 8 bytes of the payload (typically: UDP, TCP)

# Frequent ICMP Error message

Type	Code	Description	
3	0–15	Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

# Some subtypes of the “Destination Unreachable”

Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

“Twórczy qualche typ? dl. erroro?”

# Example: ICMP Port Unreachable

- RFC 792: If, in the destination host, the IP module cannot deliver the datagram because the indicated protocol module or process port is not active, the destination host may send a destination unreachable message to the source host.
- Scenario:

