

# Otros protocolos de capa Internet

## 1. Internet Control error Message Protocol (ICMP)

ICMP es una especie de sub capa IP, que trabaja en paralelo con este protocolo. Su propósito es proporcionar el control y la interpretación de errores. De hecho, IP está sin conexión y no detecta anomalías en la red.

Los equipos IP utilizan el protocolo ICMP para especificar cierto número de eventos importantes en TCP, como:

- Descubrimiento de los routers.
- Medida de los tiempos de tránsito (PING - *Packet Internet Groper*).
- Redirección de las tramas...

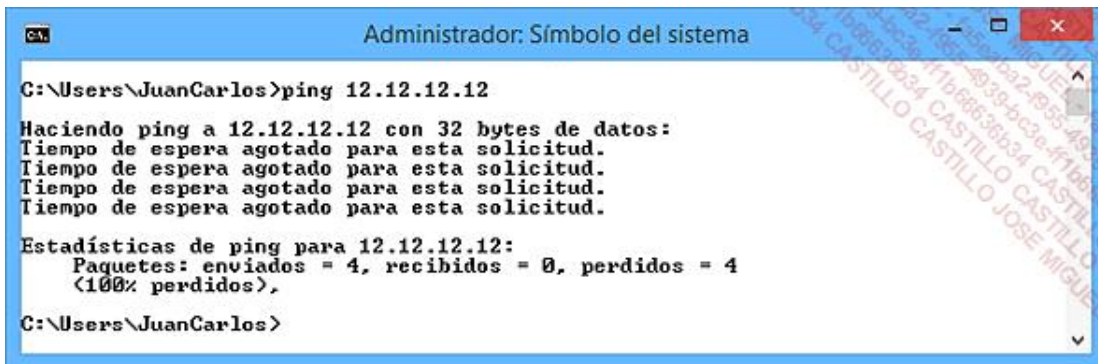
Los datos del paquete IP son la cabecera y los datos ICMP. En la cabecera IP, el número de servicio es 1.

El mensaje ICMP se identifica por su tipo y su código. Hay diferentes mensajes, entre los que podemos citar:

### Time Exceeded

Este mensaje indica que se ha sobrepasado el tiempo de espera para el destinatario. Se puede enviar si un paquete se pierde o si su TTL (en IPv4) es 0.

En este caso, el Tipo se informa a 11 y el código a 0 o 1.



```
Administrador: Símbolo del sistema
C:\Users\JuanCarlos>ping 12.12.12.12
Haciendo ping a 12.12.12.12 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Estadísticas de ping para 12.12.12.12:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
C:\Users\JuanCarlos>
```

*Ejemplo de mensaje «Time Exceeded» o «tiempo de espera agotado para esta solicitud»*

### Destination Unreachable

Este mensaje avisa que no se ha podido enrutar el paquete hacia su destino. Indica, por ejemplo, un problema en una ruta para llegar a una subred.

```
Administrador: Símbolo del sistema
C:\Users\JuanCarlos>ping 10.0.2.23

Haciendo ping a 10.0.2.23 con 32 bytes de datos:
Respuesta desde 10.0.2.15: Host de destino inaccesible.
Respuesta desde 10.0.2.15: Host de destino inaccesible.
Respuesta desde 10.0.2.15: Host de destino inaccesible.
Respuesta desde 10.0.2.15: Host de destino inaccesible.

Estadísticas de ping para 10.0.2.23:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (<0% perdidos),
C:\Users\JuanCarlos>
```

*Ejemplo de mensaje «Destination Unreachable» o «Host de destino inaccesible»*

### **Redirect**

Este mensaje indica al emisor que existe un camino mejor hacia el destino.

### **Echo request y Echo Reply**

Estos dos mensajes permiten probar si un nodo se puede comunicar con otro (petición de eco y respuesta al eco).

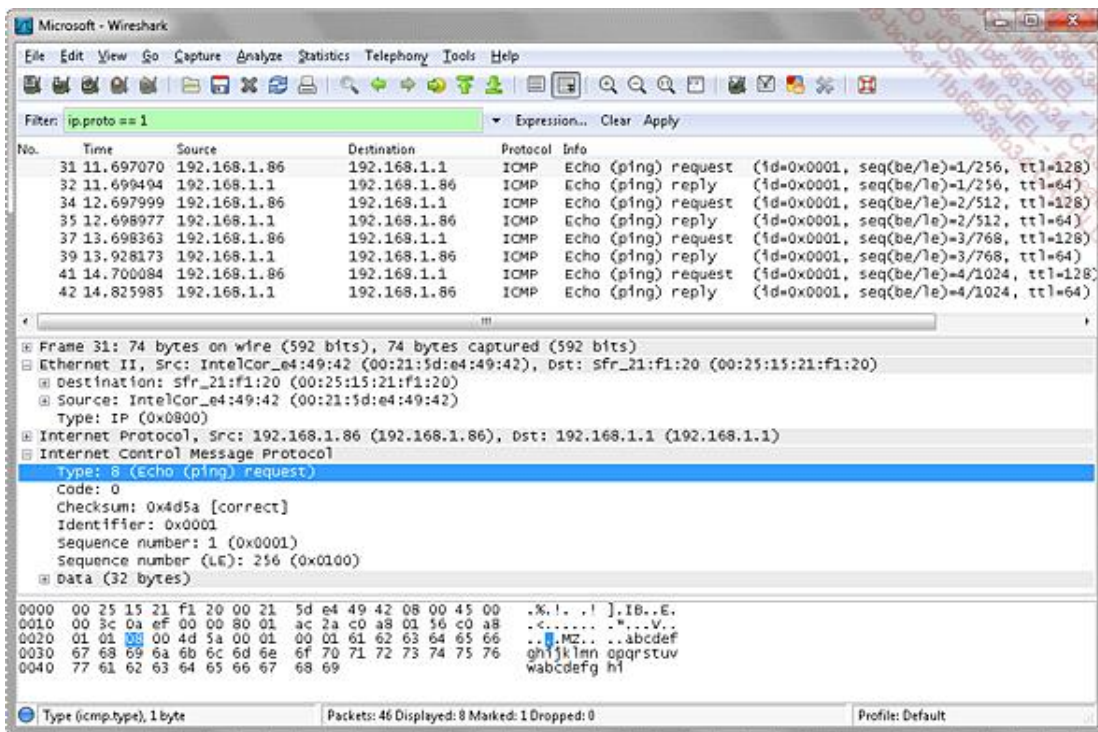
El comando Ping las utiliza.

```
Administrador: Símbolo del sistema
C:\Users\JuanCarlos>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (<0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\Users\JuanCarlos>
```

El tipo y el código de Echo Request se informan a 0. La respuesta positiva se indica con un mensaje de tipo 8 y el código se queda a 0.



➤ Esta trama se ha generado a partir de un comando ping 192.168.1.1 repetido cuatro veces desde un ordenador cuya dirección IP es 192.168.1.86.

## 2. Internet Group Management Protocol (IGMP)

Este protocolo de la capa de Red permite a un equipo añadirse o salir de un grupo multidifusión (*multicast*).

La cabecera IGMP se encapsula dentro de un paquete IP y tiene poca información, como, por ejemplo, un tipo que determina las diferentes acciones de identificación sobre un grupo, la información de pertenencia y de salida del grupo. También contiene la dirección del grupo al que se dirige la información.

## 3. Address Resolution Protocol (ARP) y Reverse Address Resolution Protocol (RARP)

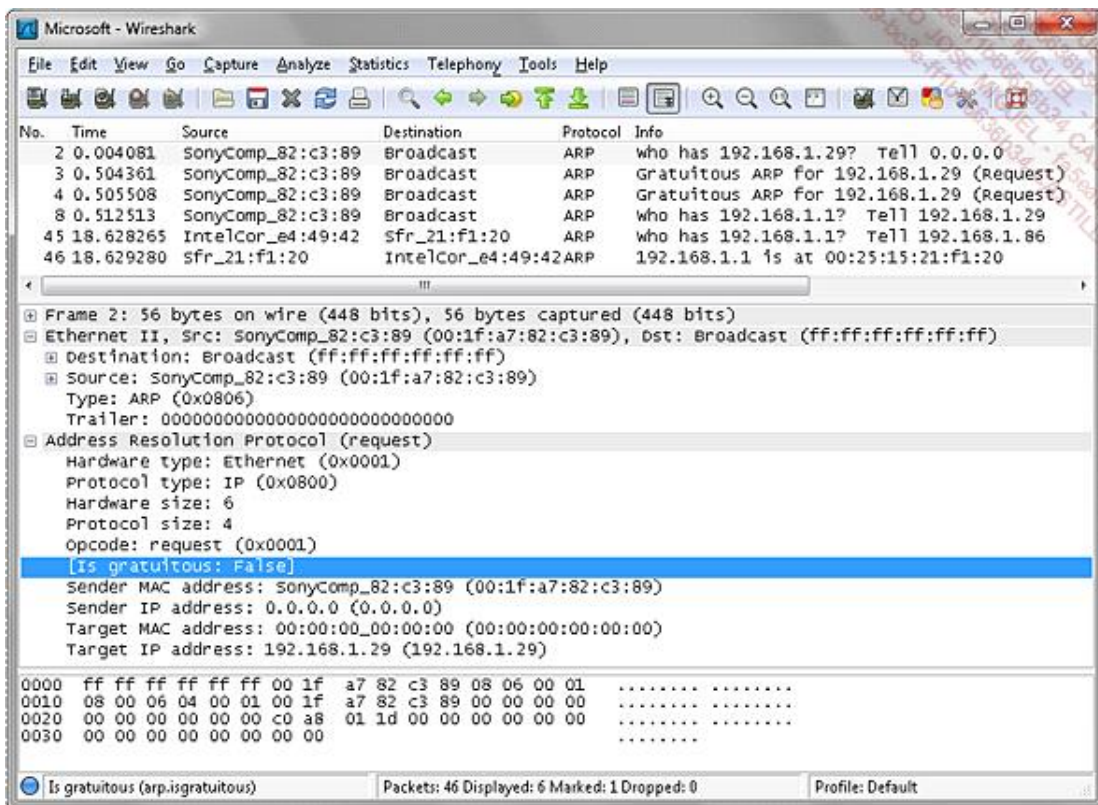
El objetivo del protocolo ARP es determinar la dirección MAC (dirección física) de un nodo a partir de su dirección IP (dirección lógica), en IPv4.

Se emite una difusión para encontrar una información concreta. Como se ha visto anteriormente, ARP administra una tabla de correspondencia (caché) para almacenar las relaciones. Esta resolución es necesaria para poder dirigir la trama al dispositivo adecuado en la red IP local.

ARP se adapta a los protocolos de capas bajas utilizados, incorporando los mensajes en estas tramas.

RARP (*Reverse ARP*) es una resolución inversa.

A continuación se observa el resumen de capturas de tramas ARP. El ordenador con dirección MAC 00:1F:A7:82:C3:89 busca al ordenador cuya dirección IP es 192.168.1.29. Observe que los tres primeros bytes de la dirección MAC (OUI) se sustituyen por el nombre del fabricante SONYCOMPUTERS:



➤ Tenga en cuenta que, al contrario que en otros protocolos, ARP no es un protocolo basado en IP. Por el contrario, lo sustituye y se encapsula directamente en la capa física (por ejemplo, Ethernet).

## 4. Internet Protocol Security (IPsec)

IPsec está diseñado para asegurar diferentes tipos de seguridad:

- Confidencialidad y protección contra el análisis del tráfico, a través del cifrado.
- Autenticidad de los datos y control de acceso a través de la autenticación mutua de los dos extremos de la comunicación, la firma, así como cálculos de integridad.
- Protección contra la inyección de paquetes.

➤ La repetición (*replay*) es una técnica que puede utilizar un intruso y que consiste en reenviar paquetes capturados durante una comunicación de red. El servidor recibe así la misma información repetida y sistemáticamente tiene que volver a procesarla y puede malinterpretar estos paquetes idénticos. Para evitar esta relectura, esta función antirrepetición añade un número de secuencia a la información. Así, el servidor es capaz de distinguir los paquetes que ya ha recibido y no volverá a tratarlos.

IPsec distingue dos niveles de protección a través de dos protocolos:

- *Authentication Header* (AH), que solo se ocupa de la autenticación, el control de integridad y el antirrepetición.
- *Encapsulating Security Payload* (ESP), que agrega la función de confidencialidad.

AH y ESP se pueden utilizar de manera conjunta o por separado, en función del nivel de protección deseado.

El primer nivel, o modo de transporte, protege una comunicación específica entre dos entidades. Así, por ejemplo,

los paquetes de comunicación de una aplicación, correspondiente a un puerto TCP dado, pueden ser seguras, sin que influya en el conjunto del tráfico.

El modo túnel se utiliza para proteger todas las comunicaciones entre dos entidades.

## 5. Lista de los números de protocolos de la capa Internet

Estos números de protocolo se pueden visualizar en parte en el archivo «Protocolo» que está en la misma carpeta que el archivo «Servicios» en Windows y «protocols» y «services» en Linux.

A continuación puede ver los principales números:

<b>N.º protocolo IP</b>	<b>Nombre del protocolo</b>
0	<i>Internet Protocol (IP)</i>
1	<i>Internet Control error Message Protocol (ICMP), utilizado principalmente por ping</i>
6	<i>Transmission Control Protocol (TCP)</i>
17	<i>User Datagram Protocol (UDP)</i>
47	<i>Generic Routing Encapsulation (GRE), utilizado por PPTP</i>
50	<i>Encapsulating Security Payload (ESP), utilizado por IPsec</i>
51	<i>Authentication Header (AH), utilizado por IPsec</i>