Telefonica

WIRESHARK

Protocolo IP

Arquitectura TCP/IP

Protocolo Internet

Protocolo Internet

Modelo de operación

El protocolo IP, implementa dos funciones básicas

- **Direccionamiento**, proceso utilizado para mover datagramas, donde necesitamos
  - Nombre, indica qué buscamos
  - Dirección, indica dónde está
  - Ruta, indica cómo llegar hasta destino
- **Fragmentación**, necesaria cuando un datagrama tiene un tamaño mayor que la red por la que va a pasar
  - Identificación y posición (offset)
  - Mas fragmentos

Protocolo Internet

Modelo de operación

IP, trata cada datagrama como una entidad independiente y no proporciona

- Mecanismos para aumentar la fiabilidad
- Control de flujo
- Secuenciamiento

Protocolo Internet

Modelo de operación

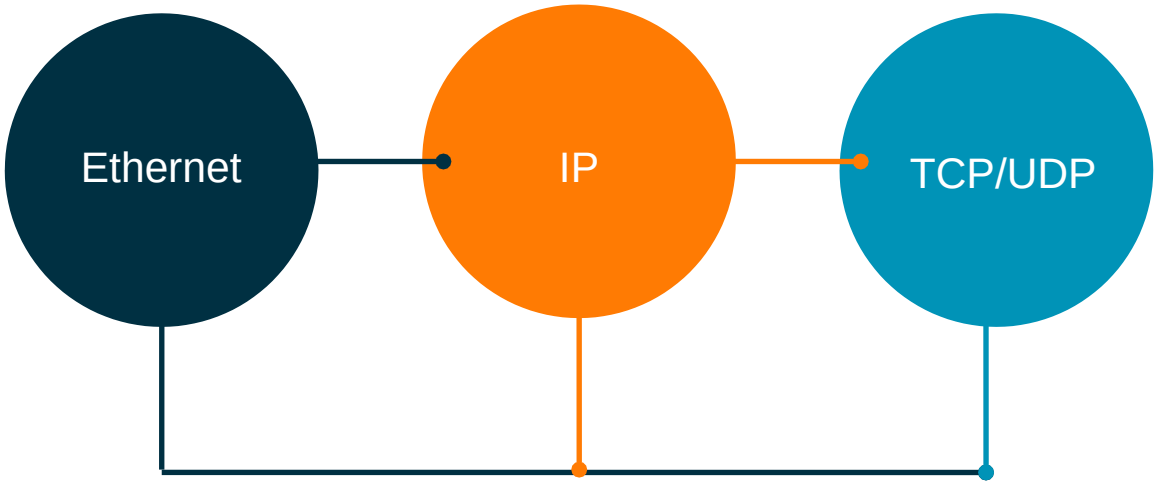
Utiliza cuatro mecanismos clave para prestar sus servicios

- **Tipo de servicio**, indica la calidad del servicio prestado
- **Tiempo de vida**, indica el tiempo que está un datagrama en circulación
- **Fragmentación**, se encarga, si fuera necesario, de la fragmentación y ensamblado de datagramas
- **Suma de control** para detectar errores

Protocolo Internet

Modelo de operación

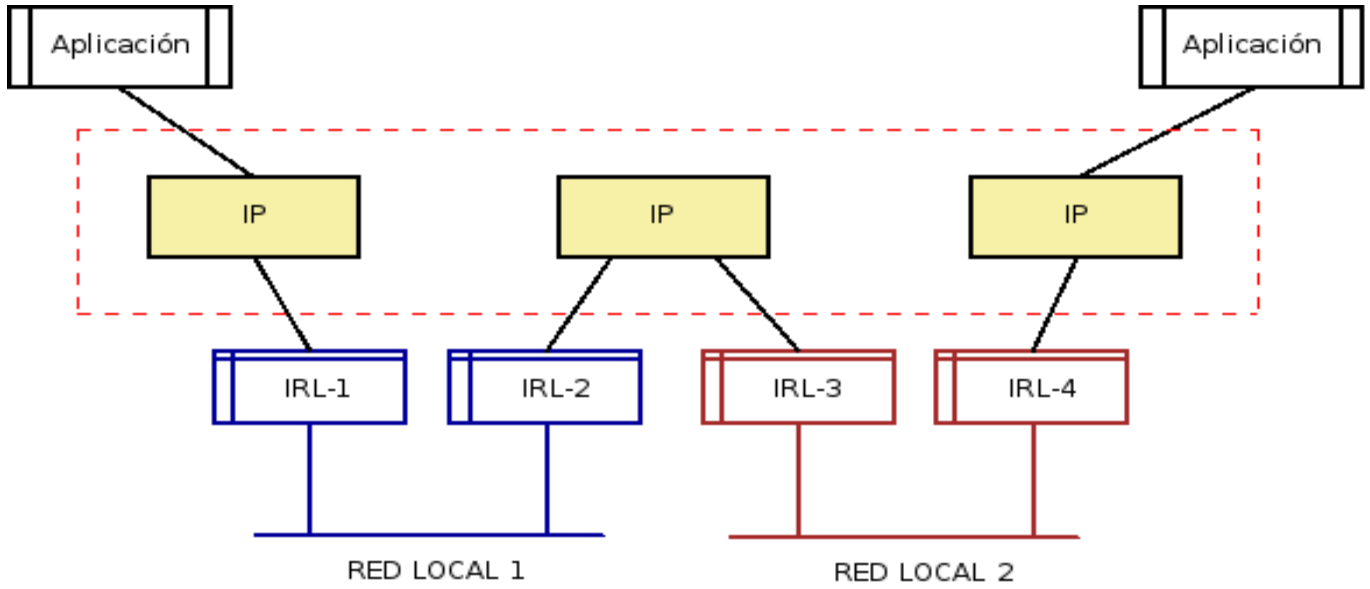
IP, interactúa con los protocolos de transporte y con la red local



Protocolo Internet

Modelo de operación

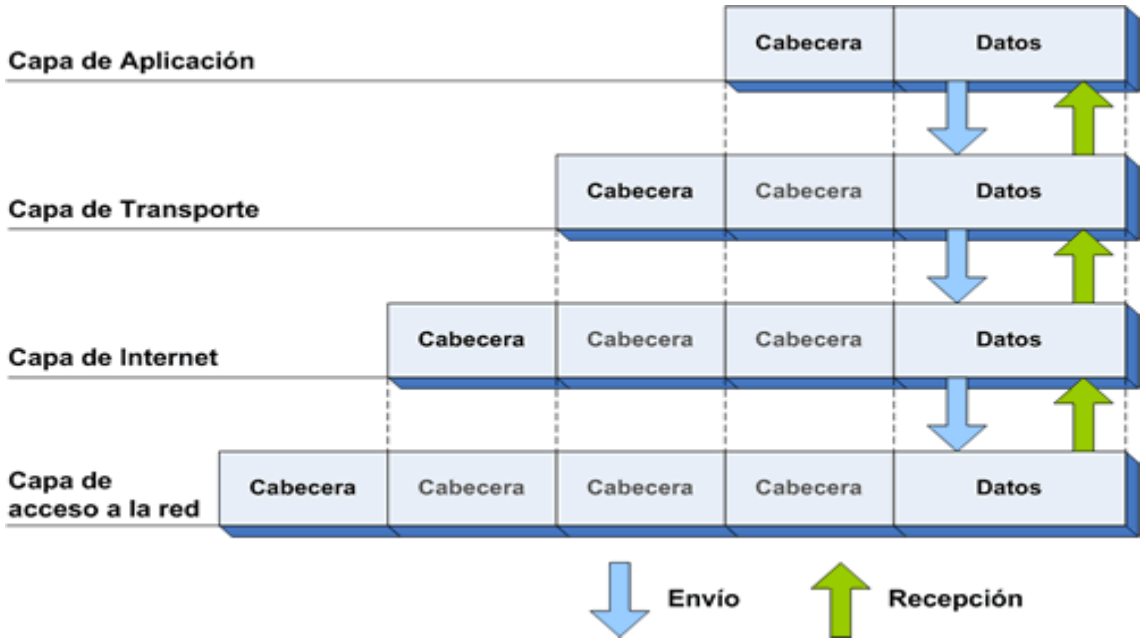
IP, interactúa con los protocolos de transporte y con la red local



Protocolo Internet

Modelo de operación

En el proceso, cada nivel, añade sus parámetros corespondientes, eliminandolos en destino



Protocolo Internet

Modelo de operación

La fragmentación, es necesaria cuando un datagrama debe atravesar una red que limita el tamaño del paquete a uno inferior

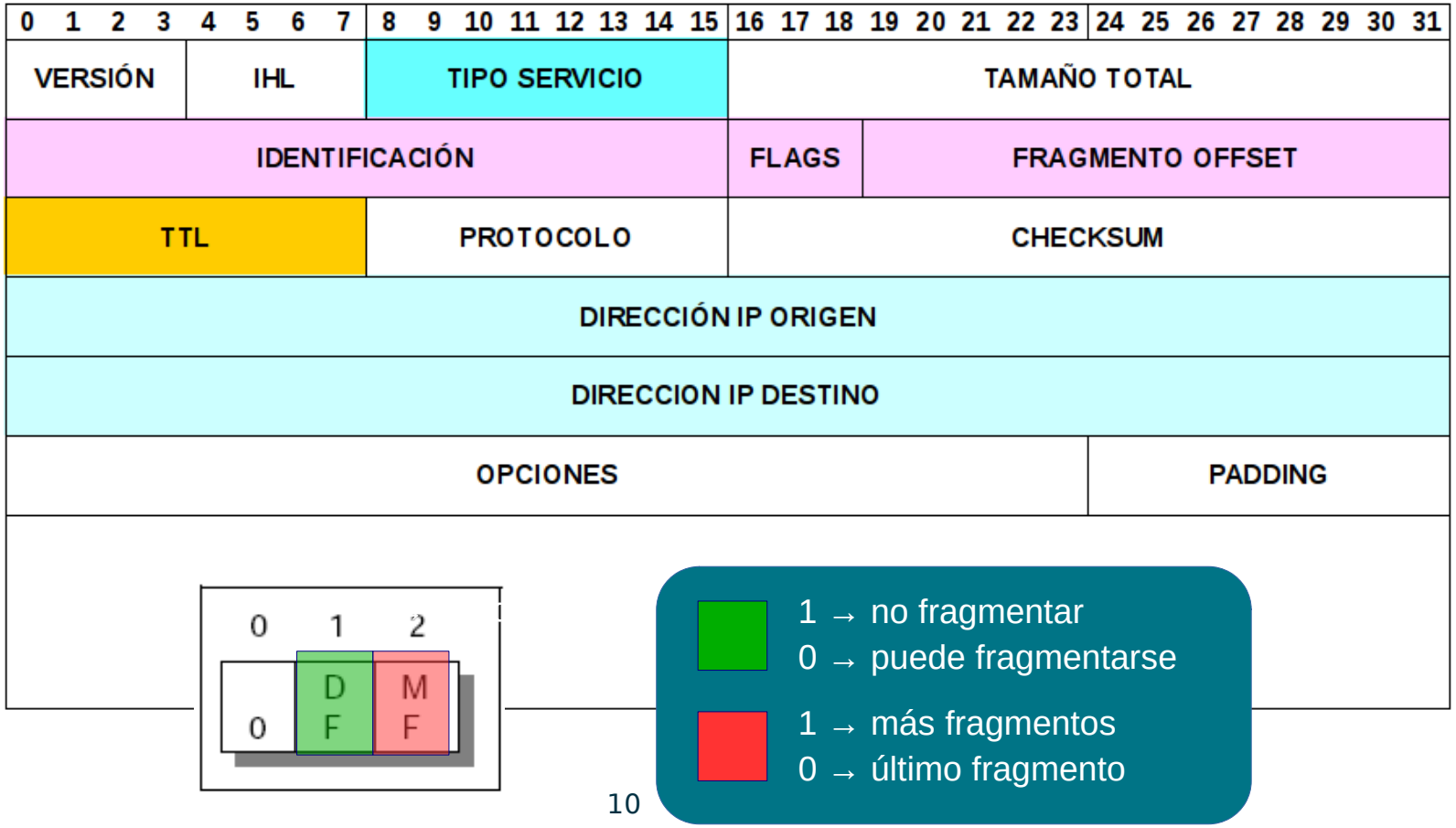
- El receptor, utiliza el campo de identificación, además de los campos origen, destino y protocolo, para ensamblar los fragmentos en el orden correcto
- Existirá un indicador **más fragmentos**, que marcará si hay o no más fragmentos

	Identificación	Offset	Flags
Fragmento 1	0x2d00	0	NF=0, MF=1
Fragmento 2	0x2d00	1480	NF=0, MF=0

Protocolo Internet

Especificación funcional

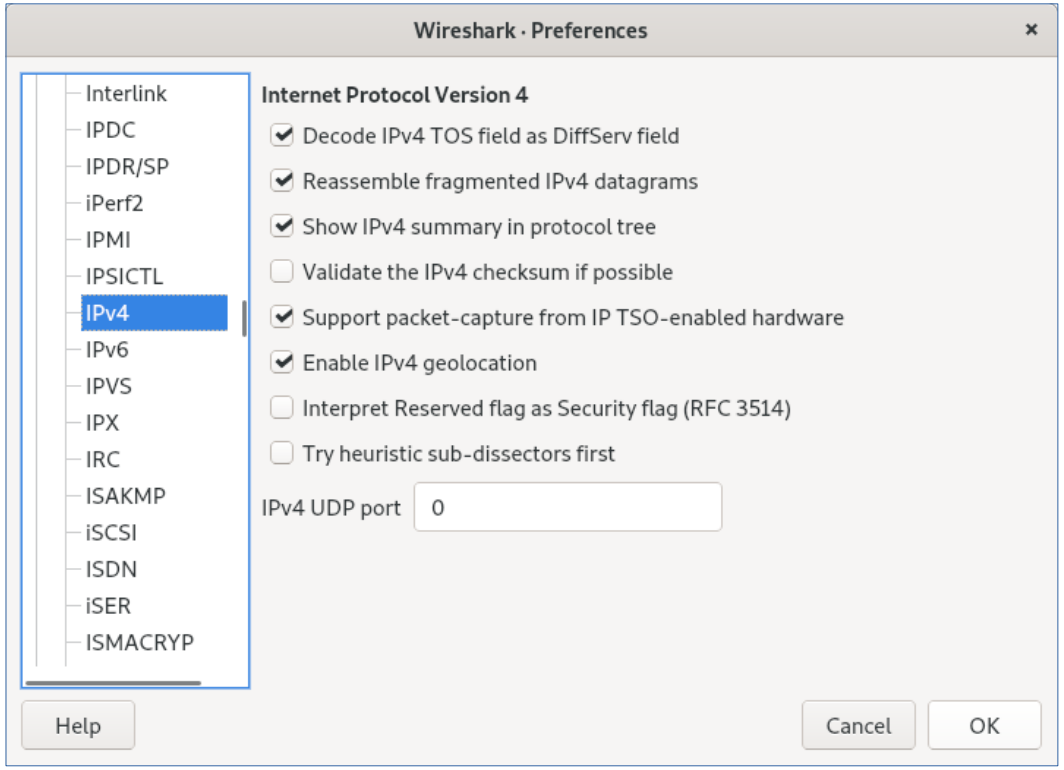
Cabecera IP



Protocolo Internet

Wireshark y protocolo IP

Ajustes del protocolo IP en Wireshark



Protocolo Internet

Ejemplos de filtrado

Sintaxis de filtros IP

```
# Dirección de origen o dirección de destino
ip.src == 192.168.10.1 || ip.dst == 192.168.10.1

# Dirección IP de origen o destino
ip.addr == 192.168.10.1

# Tamaño de la cabecera IP
ip.hdr_len > 20

# Flags utilizados en fragmentación IP
ip.flags.mf == 1
!(ip.frag_offset == 0)

# Tiempo de vida del paquete IP
ip.ttl > 20
```

Protocolo Internet

Debilidad IP

IP spoofing, se basa en suplantar la identidad de otro usuario

- Utiliza paquetes IP con una dirección de origen falsa, donde puede existir un equipo de filtrado o porque existe una relación de confianza entre dos sistemas
- En la mayoría de los casos, se utiliza para realizar ataques DoS o DDoS

Protocolo Internet

Debilidad IP

IP flooding, se basa en la inundación masiva de datagramas IP

El tráfico puede ser:

- Aleatorio, dirección de origen y destino es falsa
- Dirigido, cuando la dirección de origen, destino o ambas, es la máquina que recibe el ataque

Protocolo IP

Debilidad IP

Teardrop, intentará realizar una utilización fraudulenta de la fragmentación IP para confundir al sistema en el ensamblado y así, colapsar el sistema

	Fragmento 1	Fragmento 1
Fragmento 1	0	512
Fragmento 2	512	1024

Fragmentación correcta

	Fragmento 1	Fragmento 1
Fragmento 1	0	512
Fragmento 2	500	512
Fragmento 3	100	256

Fragmentación incorrecta

Protocolo Internet

Debilidad IP

Construcción errónea de la cabecera IP

- **IP bad headers field**, el objetivo es obtener de la máquina objetivo, un mensaje ICMP de error (parameters problem), para ello, debemos formar una cabecera IP con parámetros que no son correctos
  - Las comprobaciones varían en función de la máquina, por lo que es posible identificar el fabricante del mismo
- **IP non valid field values**, el objetivo es el mismo, pero el error generado es destination unreachable
  - Si no se recibe respuesta, podemos asumir, que existe un equipo de filtrado

Protocolo Internet

Laboratorio 1

Estudio de la fragmentación

- Comprobar el funcionamiento de la fragmentación, offset, flags
- ¿Qué tipo de tráfico es?
- En el segundo archivo, ¿qué diferencia significativa hay entre los dos archivos?

Arquitectura TCP/IP

Protocolo ARP

Protocolo ARP

Modelo de operación

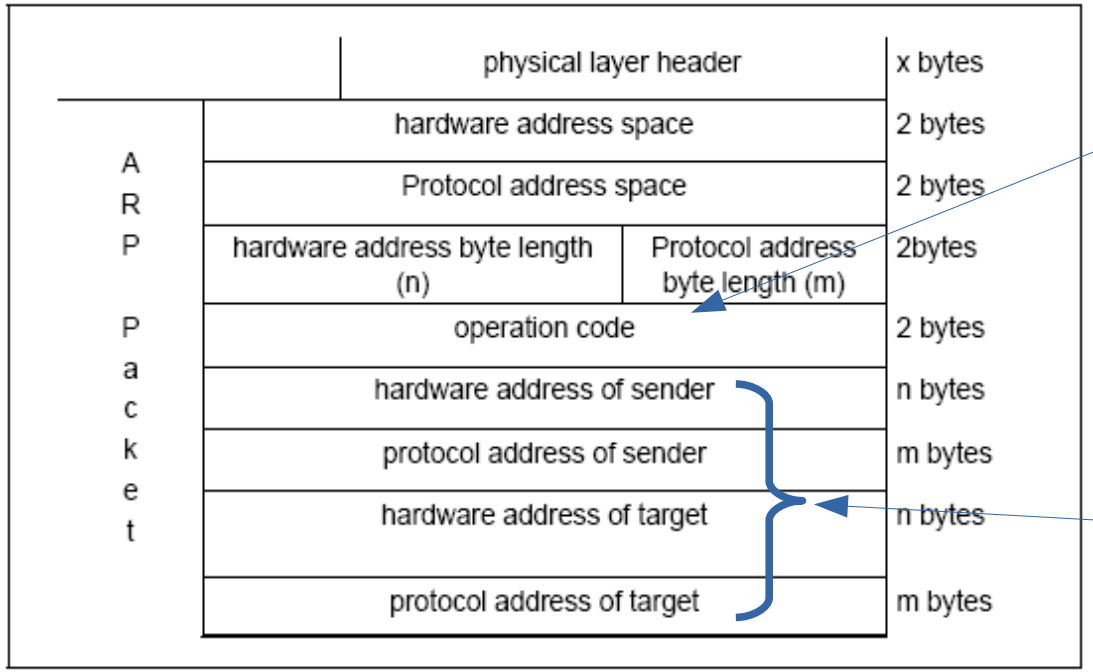
El protocolo ARP, permite localizar las direcciones físicas, basándose en las direcciones IP de los dispositivos, para ello

- Realiza una solicitud de broadcast de un paquete ARP con la ip del dispositivo a localizar
- El dispositivo cuya dirección IP coincida con la del mensaje ARP, enviará una respuesta ARP indicando su dirección física
- El origen, actualiza su tabla ARP, para futuras comunicaciones

Protocolo ARP

Modelo de operación

Paquete ARP



Código de operación:
0001 → Solicitud
0002 → Respuesta
0003 → RARP solicitud
0004 → RARP respuesta

Dirección hardware e IP de origen y destino

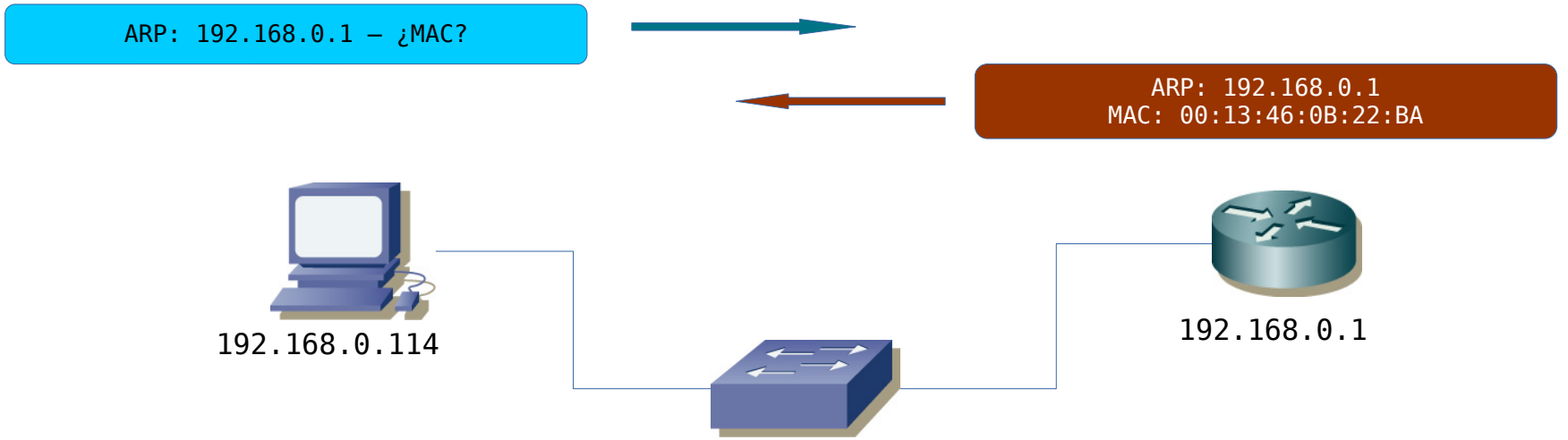
Protocolo ARP

Modelo de operación

Mensajes ARP

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
    Sender IP address: 192.168.0.114 (192.168.0.114)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1 (192.168.0.1)
```

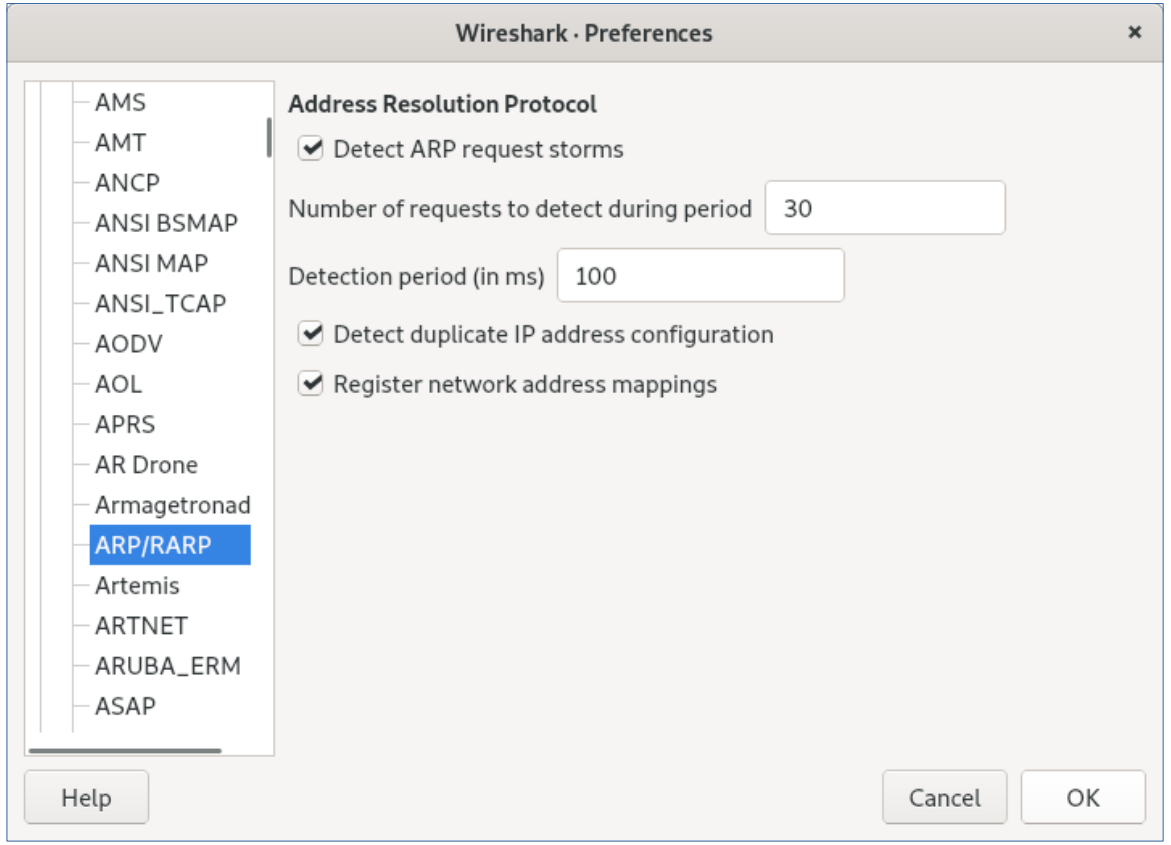
```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: D-Link_0b:22:ba (00:13:46:0b:22:ba)
    Sender IP address: 192.168.0.1 (192.168.0.1)
    Target MAC address: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
    Target IP address: 192.168.0.114 (192.168.0.114)
```



Protocolo ARP

Wireshark y ARP

Ajustes de ARP en Wireshark



Protocolo Internet

Ejemplos de filtrado

Sintaxis de filtros ARP

```
# Código de operación
arp.opcode == 1

# Dirección hardware
arp.src.hw_mac == 00:aa:bb:cc:dd:ee

# Dirección IP
arp.src.proto_ipv4 == 192.168.10.1

# Tamaño de la dirección hardware
arp.hw.size == 6
```

Protocolo ARP

Análisis con Wireshark

El funcionamiento normal de ARP, encontraremos ARP request (solicitudes) y ARP reply (respuestas), ¿qué debemos comprobar?

- Solicitudes de diferentes fuentes no son un problema, muchas solicitudes de un mismo dispositivo, hay que averiguar el origen, puede ser un escaneo
- Si no se identifica la fuente, puede ser un problema, mirar detalles
- Podemos ver respuestas en las que no hay solicitudes, mirar detalles

Protocolo ARP

Análisis con Wireshark

ARP gratuito, se lleva a cabo cuando un dispositivo desea verificar si algún otro dispositivo, tiene su misma dirección IP

- En este caso, se verá un ARP con la misma dirección de origen y destino, pero sin respuesta

Protocolo ARP

Análisis con Wireshark

ARP sweep (barrido), se utiliza cuando vemos dispositivos que escanean la red con solicitudes o respuestas ARP, con el fin de obtener información o atacar la red

- Tenemos que localizar el emisor

Protocolo ARP

Análisis con Wireshark

Es difícil calcular el número exacto de ARP por unidad de tiempo en una red, teniendo en cuenta que cuando un dispositivo quiere comunicar con otro, envía una solicitud ARP para conocer su dirección física

La cantidad de tráfico ARP, dependerá del número de dispositivos y del tipo de aplicaciones que tengamos funcionando en la red.

Protocolo ARP

Análisis con Wireshark

Cuando analizamos problemas de conectividad, podemos ver muchas solicitudes ARP sin respuesta

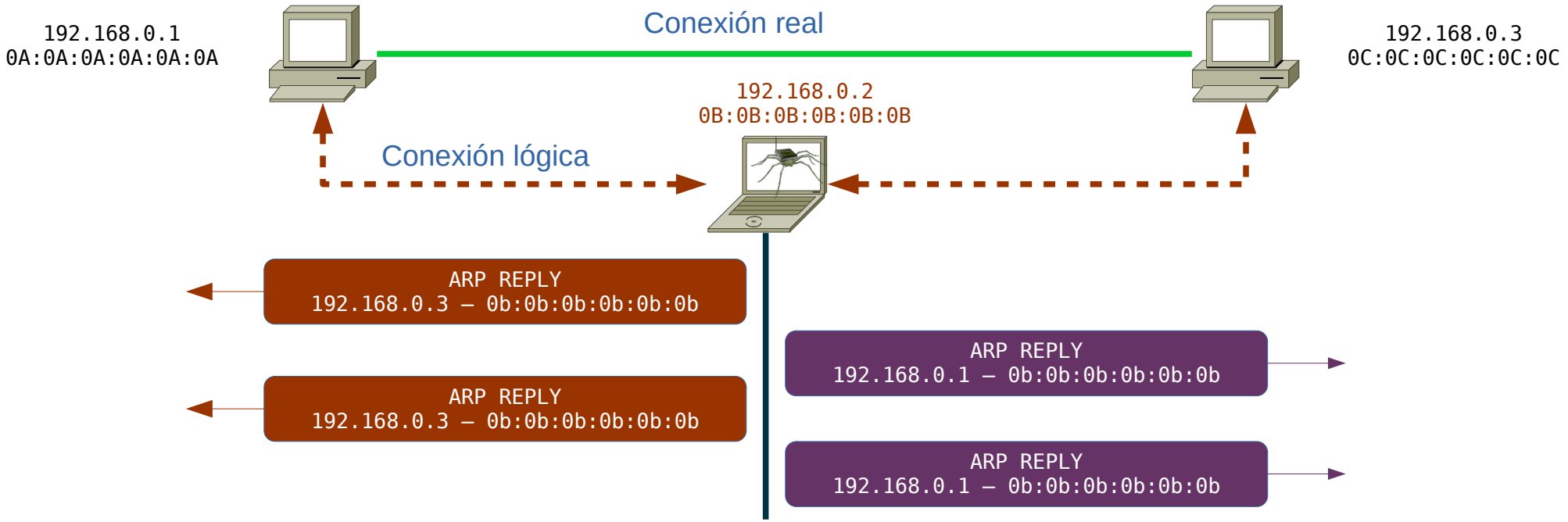
Un ARP request sin respuesta, puede ser debido a una mala configuración de la máscara de red en un equipo, detecta que un dispositivo está en su red local, cuando debería buscar un router para alcanzarlo, el tráfico ARP, no puede ser enrutado

Puede ser que no estemos situados en el lugar adecuado, vemos las solicitudes broadcast, pero no las respuestas unicast

Protocolo ARP

Debilidad ARP

ARP spoofing, es utilizado por atacantes, para interponerse entre una o varias máquinas, con el fin de interceptar, modificar o capturar paquetes



Protocolo ARP

Laboratorio 2

Familiarizarse con la estructura del protocolo ARP

¿Qué se ve en los siguientes archivos?

¿Cuantas máquinas hay en esta red?

¿Qué está pasando en la captura?

Arquitectura TCP/IP

Protocolo DHCP

Protocolo DHCP

Modelo de operación

Las demandas de conectividad, cambios y reconfiguraciones que exigen el entorno de red actual, generan la necesidad de mecanismos que permitan automatizar la configuración de máquinas y la distribución del sistema operativo

Algunos equipos, necesitan pocas variables de configuración, otras, una lista más detallada. A veces, se necesita descargar el sistema operativo completo

DHCP, es una mejora del protocolo **BOOTP**

Protocolo DHCP

Modelo de operación

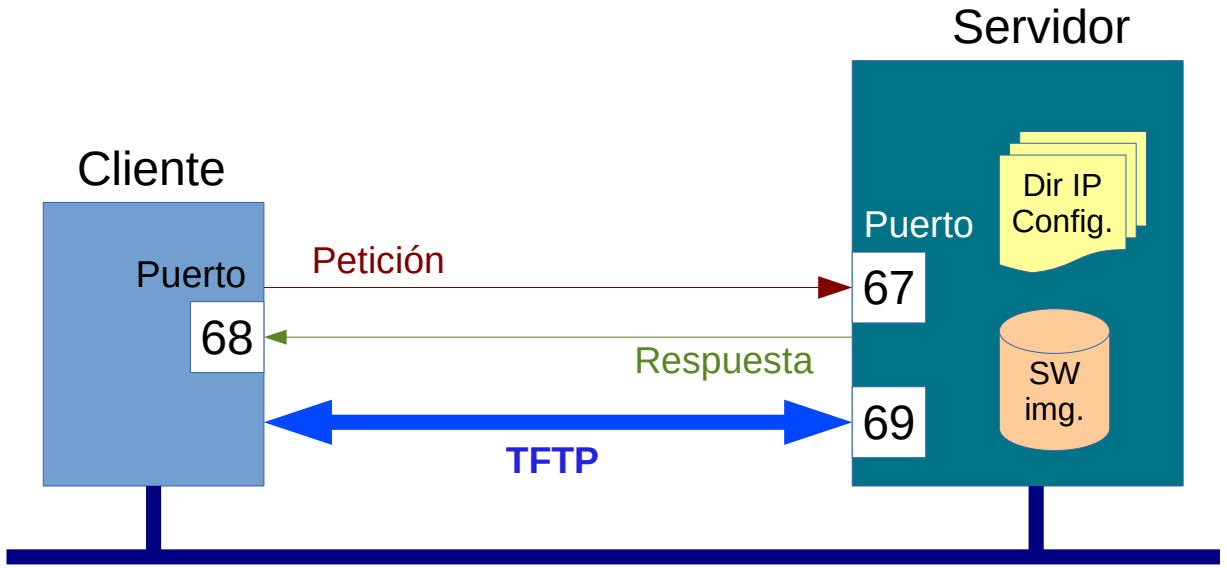
DHCP, es una mejora del protocolo **BOOTP**, algunas mejoras son:

- Administración más sencilla
- Configuración automatizada
- Posibilidad de que el cliente solicite los valores de ciertos parámetros
- Nuevos tipos de mensajes

Protocolo DHCP

Modelo de operación

BOOTP se diseño para estaciones de trabajo sin disco, el objetivo, era permitir un arranque automático con lo básico

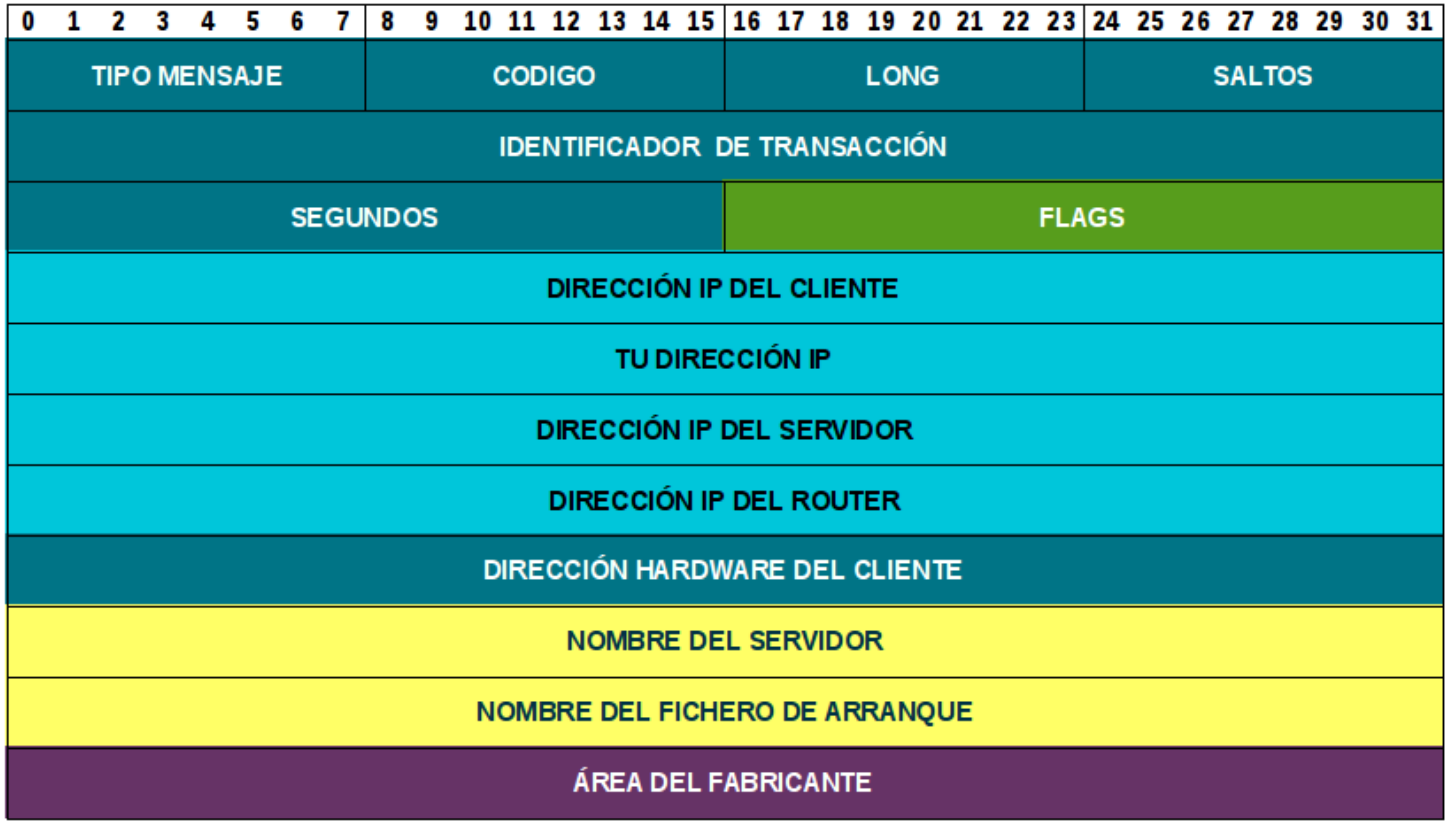


1. cliente difunde una petición de información en un mensaje UDP
2. El servidor devuelve la dirección IP del cliente y opcionalmente el archivo a descargar

Protocolo DHCP

Modelo de operación

Se usa el mismo formato de mensaje para la petición y respuesta



Campos obligatorios

Protocolo DHCP

Modelo de operación

DHCP, permite tres tipos de asignación

- Asignación manual
- Asignación automática
- Asignación dinámica

Protocolo DHCP

Modelo de operación

DHCP, presenta nuevos conceptos

- Alquiler, el servidor concede al cliente un alquiler que indica el período de tiempo que puede disponer la dirección IP
- Enlace, correspondencia entre el cliente y sus parámetros de configuración

Protocolo DHCP

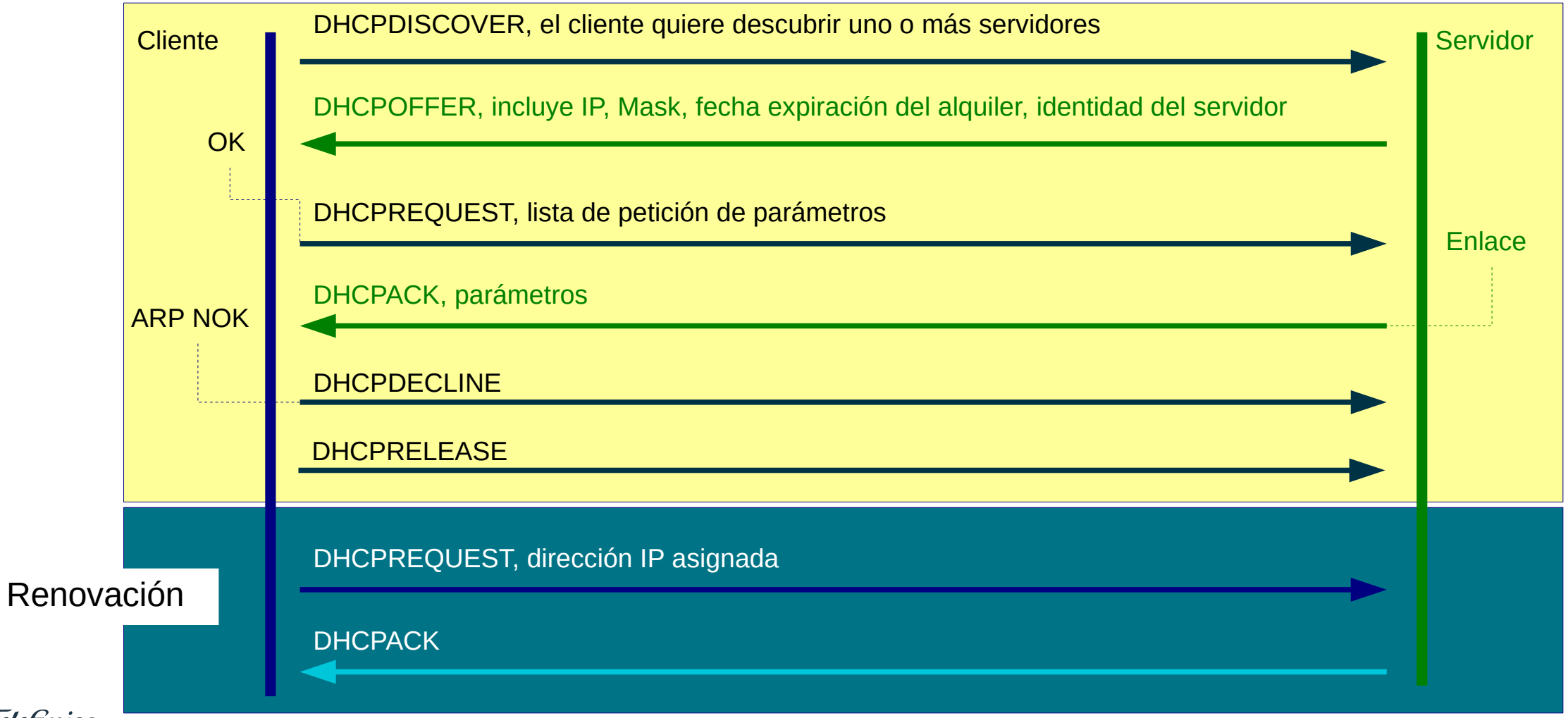
Modelo de operación

El tipo de mensaje, se define en el campo opción

- DHCPDISCOVER
- **DHCPOFFER**
- DHCPREQUEST
- **DHCPACK**
- **DHCPNACK**
- DHCPINFO
- DHCPDECLINE
- DHCPRELEASE

Protocolo DHCP

Modelo de operación

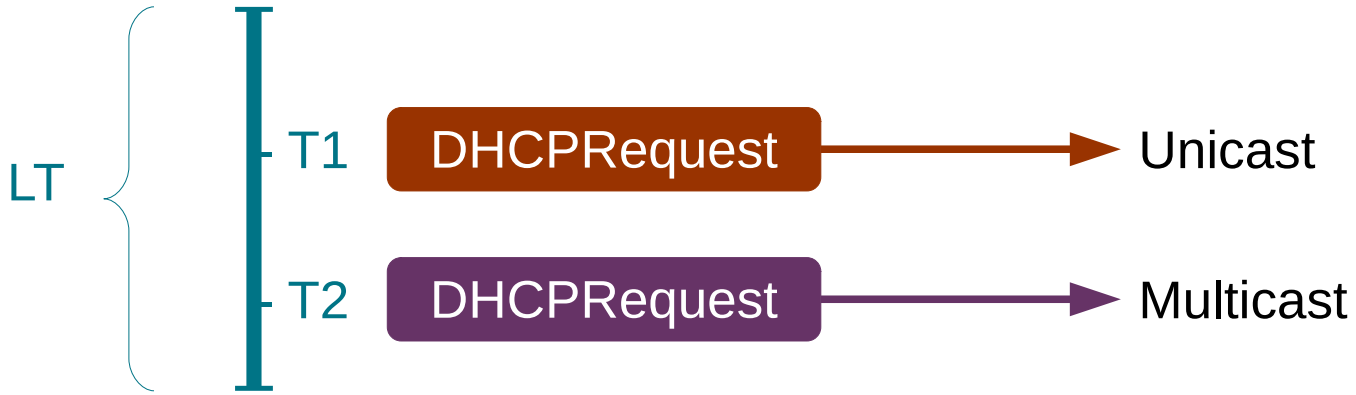


Protocolo DHCP

Modelo de operación

En la asignación dinámica, entran en juego, tres temporizadores

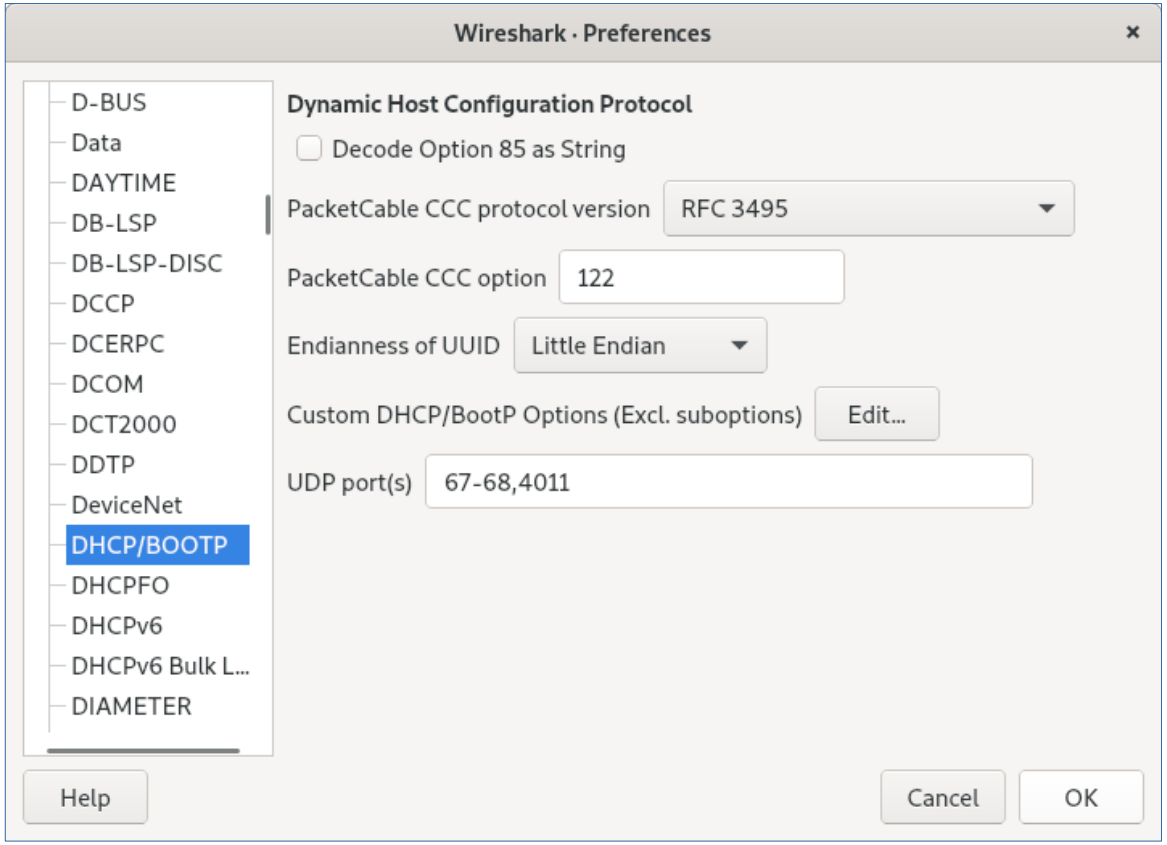
- **Lease Time (LT)**, define cuanto tiempo permite a un cliente usar la dirección IP asignada
- **Renewal Time (T1)**, por defecto es 0,5 * LT
- **Rebind Time (T2)**, por defecto es 0,875 * LT



Protocolo DHCP

DHCP y Wireshark

Ajustes de DHCP desde Wireshark



Protocolo DHCP

DHCP y Wireshark

Sintaxis de filtros para DHCP

```
# Depende de la versión de Wireshark
bootp o dhcp

# Mensaje DHCPDISCOVER
dhcp.option.dhcp == 1

# Mensaje conteniendo la dirección MAC y la dirección IP
dhcp.hw.mac_addr == 00:aa:bb:cc:dd:ee
dhcp.ip.your == 192.168.10.1

# Mensaje que contiene un agente para DHCP Relay
dhcp.ip.relay != 0.0.0.0
```

Protocolo DHCP

Debilidad DHCP

DHCP no proporciona mecanismos de autenticación que permita verificar el origen del servidor

- **DHCP spoof**, consiste en instalar un servidor DHCP falso o un software que lo emule y responda a peticiones DHCPDISCOVER
- **DHCP flooding**, consiste en enviar multitud de paquetes DHCPDISCOVER con direcciones físicas aleatorias, con el fin de acabar con el rango de IP disponibles en el servidor

Protocolo DHCP

Laboratorio 3

Estudiar proceso DHCP

- Secuencia correcta de una petición IP a un servidor
- ¿Qué parámetros solicita el cliente?¿Cuales devuelve el servidor?
- Está el servidor en la misma red
- Problemas con el servidor

Arquitectura TCP/IP

Protocolo ICMP

Protocolo ICMP

Modelo de operación

ICMP desempeña un papel fundamental de asistente en la red, informando de errores en el procesamiento de datagramas IP

Hay situaciones en las que se descartan datagramas

- Un enlace o un dispositivo caído
- Ha expirado el contador de vida
- No se puede enviar, porque no se permite la fragmentación

Protocolo ICMP

Modelo de operación

Los mensaje ICMP, se transmiten como datagramas IP, con el campo de protocolo igual a 1

El protocolo ICMP, proporciona un conjunto de mensajes de control y error, que permite detectar y resolver problemas en la red

Protocolo ICMP

Modelo de operación

El protocolo, especifica que los mensajes ICMP, deberían enviarse en todas las situaciones que contempla, pero no requiere que todos los errores tengan que generar un mensaje ICMP

Es importante asegurar que el tráfico ICMP no inunda la red, empeorando la situación

Protocolo ICMP

Modelo de operación

Mensajes de error debidos al encaminamiento

- Destino inalcanzable
- Plazo superado
- Problemas con parámetros
- Redirección

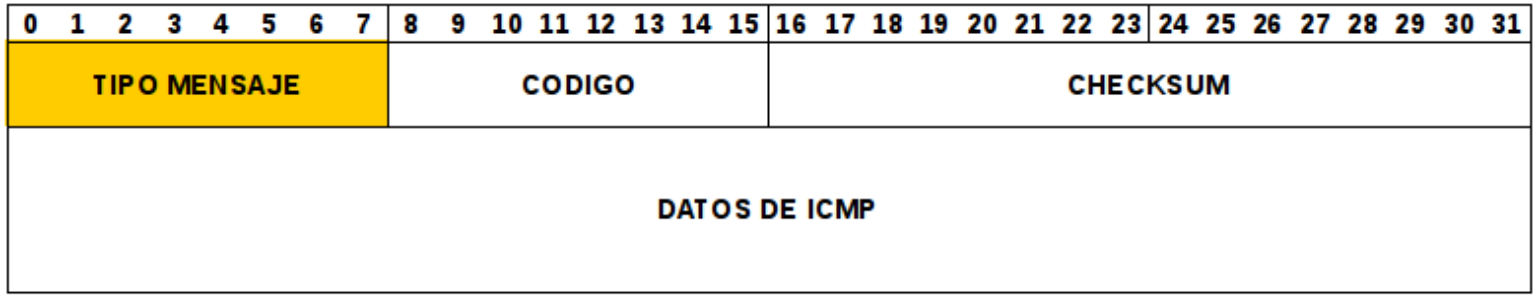
Mensajes para obtener información de la red

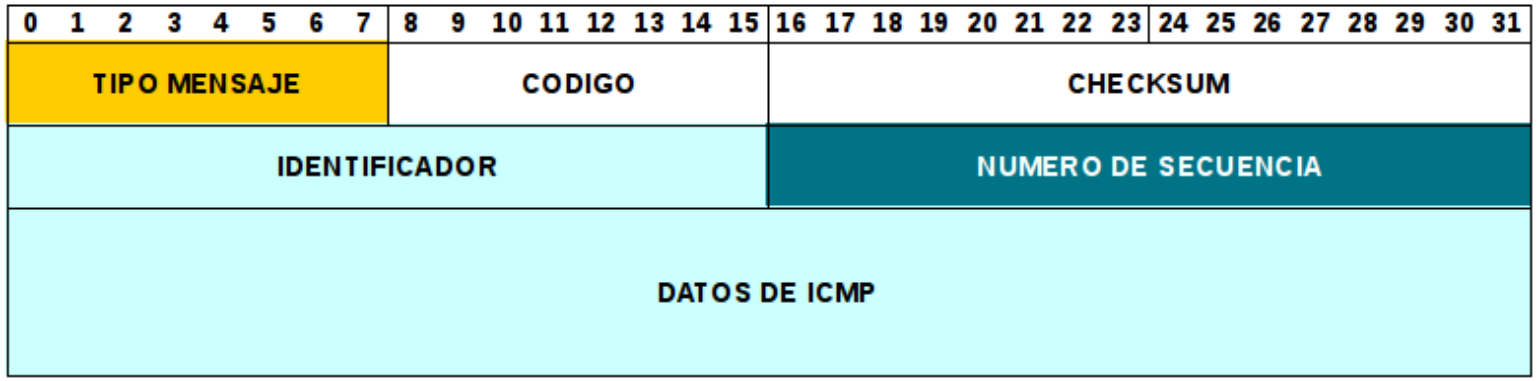
- Echo
- Timestamp

Protocolo ICMP

Modelo de operación

Los mensajes ICMP, incluyen la cabecera IP y los primeros 8 octetos del datagrama que causó el error

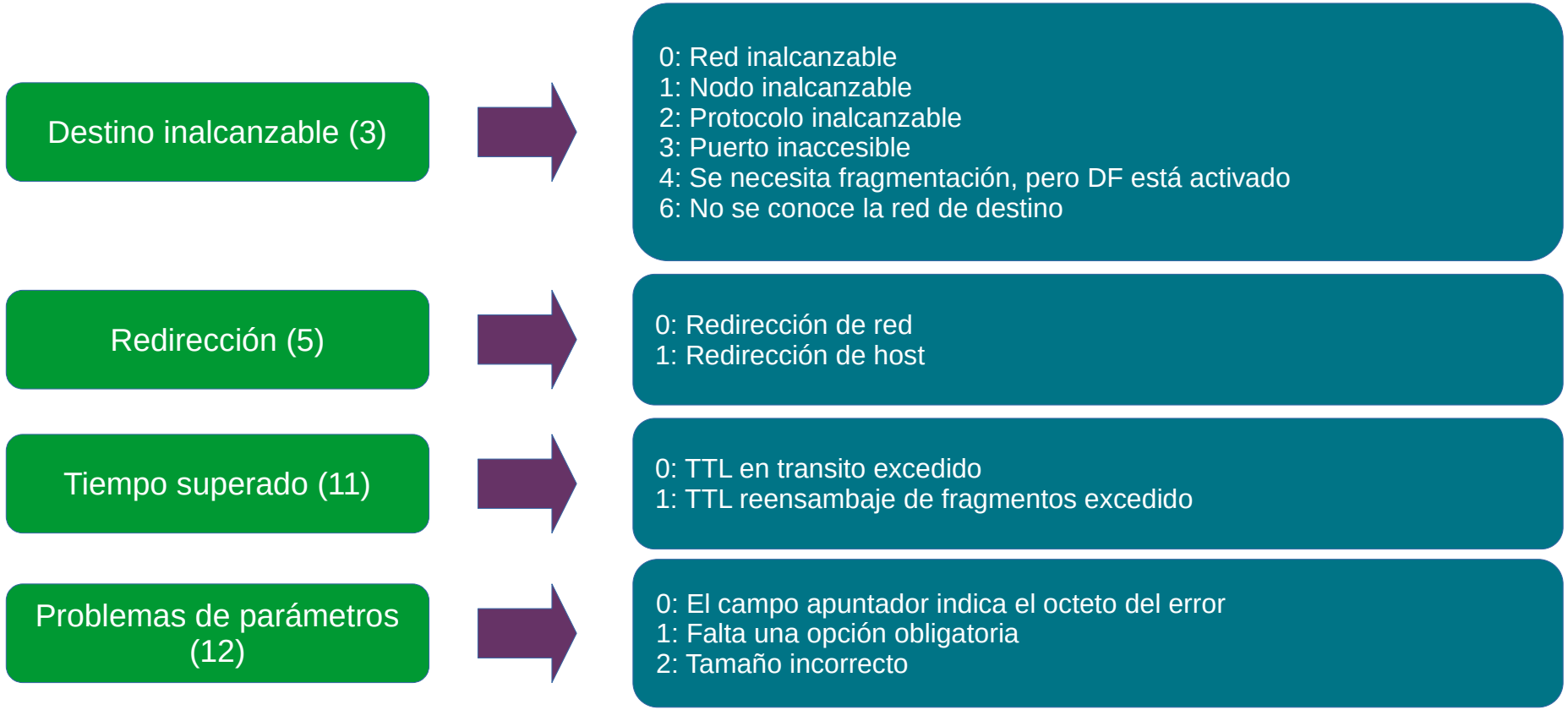




Protocolo ICMP

Modelo de operación

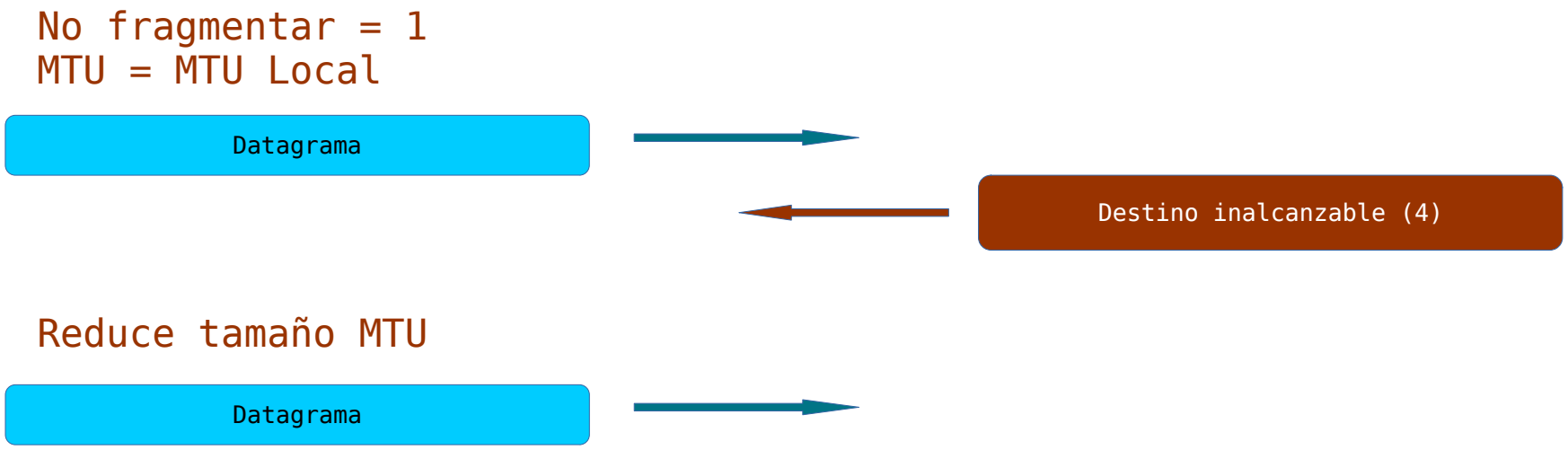
Los datos ICMP, dependerán del tipo de mensaje



Protocolo ICMP

Modelo de operación

Cómo conocer el mayor datagrama que se puede enviar por una ruta



Protocolo DHCP

ICMP y Wireshark

Sintaxis de filtros para ICMP

```
# ICMP echo request o echo response
icmp.type == 8 || icmt.type == 0

# Ping inusual
(icmp.type == 8) && !(icmp.code == 0)
```

Protocolo ICMP

Laboratorio 4

Estudiar mecanismo ICMP

- Ping clásico
- Destino inalcanzable, observar el motivo del rechazo y los datos que reporta ICMP
- Operación clásica de traceroute


Telefónica