

# Práctica 1:

## Wireshark y tráfico

Redes y Sistemas Distribuidos  
Grado de Ingeniería del Software (Grupo A)



UNIVERSIDAD  
DE MÁLAGA





# Analizadores de protocolos

2

- Un **analizador de protocolos** es un programa informático o una pieza de hardware que **puede interceptar y registrar tráfico** que pasa por una red o parte de una red.
  - Analizador de red, analizador de paquetes o *sniffer*
- En **Ethernet** solo capturamos **los paquetes que vengan hacia nosotros** (salvo que estemos en un puerto especial del nodo intermedio o éste esté configurado en modo “repetidor”).
- En **Wifi** podría ser posible capturar **todo el tráfico** (si la tarjeta permite el modo promiscuo o **monitor** )
- Existen múltiples herramientas : **Wireshark**

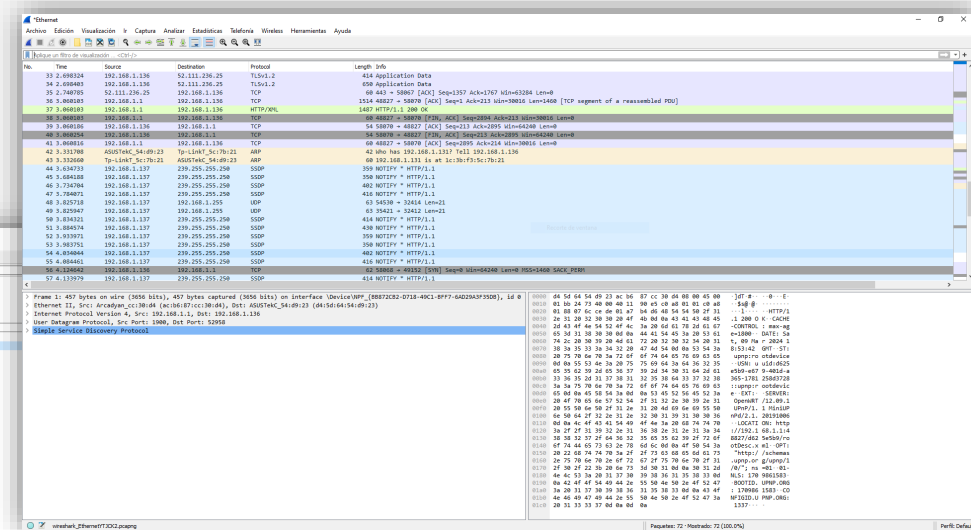
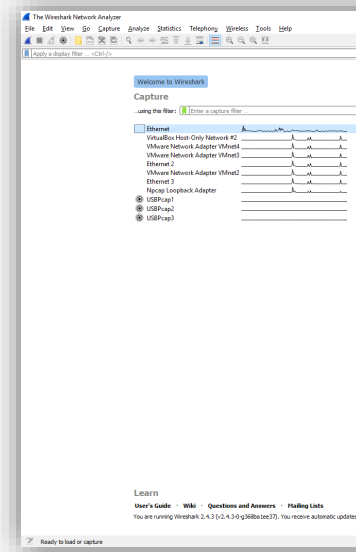


# WIRESHARK



# Proceso de utilización

1. Página inicial : Interfaz de captura
2. Inicio y parada de captura
3. Guardar las trazas
4. Análisis del tráfico : filtrado



¡Demostración en vivo!



# Filtrado

- Filtros de `captura` vs `filtrado`
- Filtros:
  - **Protocolo** : `arp`
    - Protocolos útiles para la práctica: `eth`, `arp`, `ip`, `dns`, `icmp` y `http`
  - **Campos** : `eth.src == ...`
    - Campos en `eth`: `src`, `dst`, `addr`, `type`
  - **Combinación** : `http or dns`
    - Operadores: `and`, `or`, `not` (`&&`, `||`, `!`)
- Asistente

# Datos de un paquete

5

> Frame 46: 906 bytes on wire (7248 bits), 906 bytes captured (7248 bits) on interface 0  
> Ethernet II, Src: IntelCor\_1f:99:a1 (68:07:15:1f:99:a1), Dst: Cisco\_03:04:00 (00:1b:8f:03:04:00)  
> Internet Protocol Version 4, Src: 192.168.120.255, Dst: 150.214.40.97  
> Transmission Control Protocol, Src Port: 61434, Dst Port: 80, Seq: 2615667219, Ack: 429552808, Len: 852  
> Hypertext Transfer Protocol

Cab Eth

Cab IP

Cab TCP

Cab HTTP

> Frame 46: 906 bytes on wire (7248 bits), 906 bytes captured (7248 bits) on interface 0

Toda la trama (+ resumen ofrecido por Wireshark )

> Ethernet II, Src: IntelCor\_1f:99:a1 (68:07:15:1f:99:a1), Dst: Cisco\_03:04:00 (00:1b:8f:03:04:00)

Cabecera Ethernet II (Capa de Enlace)

> Internet Protocol Version 4, Src: 192.168.120.255, Dst: 150.214.40.97

Cabecera IP (Capa de Red)

> Transmission Control Protocol, Src Port: 61434, Dst Port: 80, Seq: 2615667219, Ack: 429552808, Len: 852

Cabecera TCP (Capa de Transporte)

> Hypertext Transfer Protocol

Cabecera HTTP (Capa de Aplicación)

Hypertext Transfer Protocol

Transmission Control Protocol

Internet Protocol Version 4

Ethernet II

Internet Protocol Version 4, Src: 192.168.120.255, Dst: 150.214.40.97

0100 .... = Version: 4

```
.... 0101 = Header Length: 20 bytes (5)
```

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

▼ Ethernet II, Src: IntelCor\_1f:99:a1 (68:07:15:1f:99:a1), Dst: Zte\_e0:95:28 (44:f4:36:e0:95:28)

▼ Destination: Zte e0:95:28 (44:f4:36:e0:95:28)

Address: Zte e0:95:28 (44:f4:36:e0:95:28)

```
> Flags:      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
```

Fragment .....0 ..... = IG bit: Individual address (unicast)

Source: IntelCor 1f:99:a1 (68:07:15:1f:99:a1)

Address: IntelCor 1f:99:a1 (68:07:15:1f:99:a1)

.....0..... = LG bit: Globally unique address (factory default)

Header      .... 0 .... = IG bit: Individual address (unicast)

[Header] Type: IPv4 (0x0800)

Source: 192.168.120.255

Destination: 150.214.40.97

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Reassembled IPv4 in frame: 8

## Campos extra ofrecidos por wireshark

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
Versión				IHL				Tipo de servicio								Tamaño total															
Identificación																Flags				Fragmento Offset											
Tiempo de vida								Protocolo								Header checksum															
0:95:28 (44:f4:36:e0:95:28)																															
s (factory default)																															
icast)																															
																								Padding							

0010 0000 1011 1001  
flags desplazamiento

185 (x8 = 1480)

Para las prácticas habitualmente se solicita el valor del paquete real (no el interpretado por wireshark)

# Filtrado reloaded

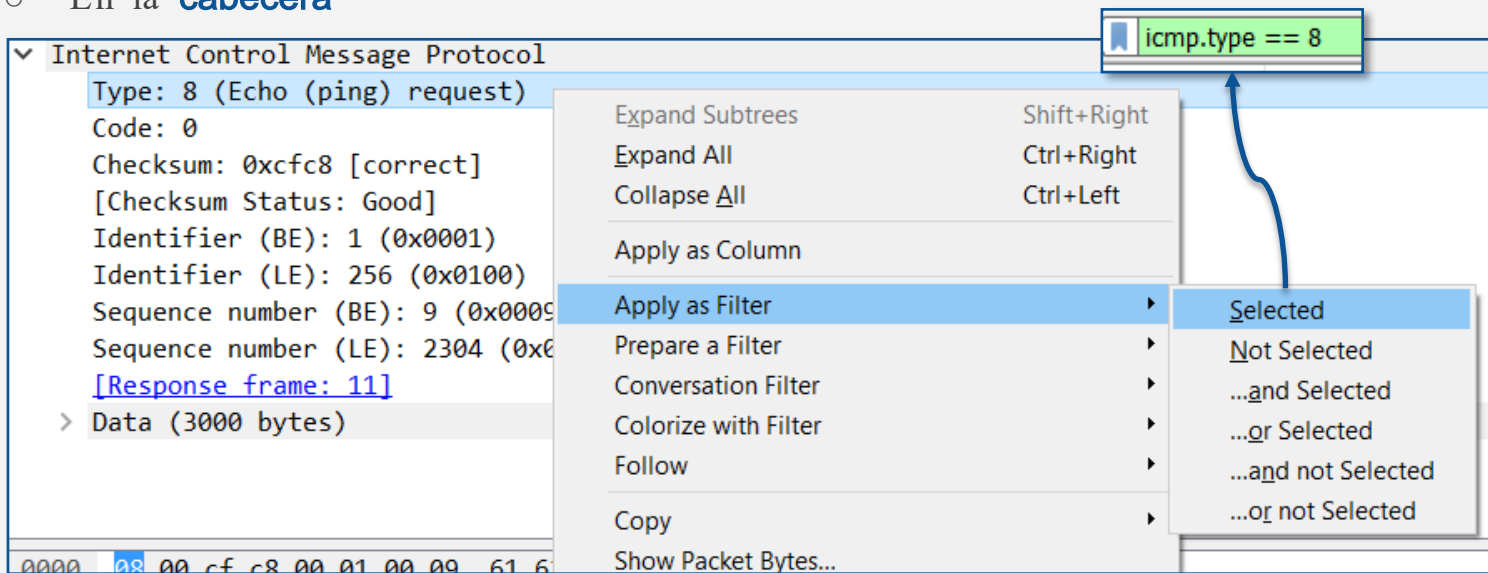
7

- Filtros por protocolo: 
- Filtros campos de protocolos:

- En la barra

*Prepare as Filter* : añade la condición al filtro pero no la aplica

- En la **cabecera**



Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0xcfc8 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence number (BE): 9 (0x0009)
- Sequence number (LE): 2304 (0x0900)
- [Response frame: 11]
- > Data (3000 bytes)

Expand Subtrees Shift+Right

Expand All Ctrl+Right

Collapse All Ctrl+Left

Apply as Column

Apply as Filter

Prepare a Filter

Conversation Filter

Colorize with Filter

Follow

Copy

Show Packet Bytes...

Selected

Not Selected

...and Selected

...or Selected

...and not Selected

...or not Selected

icmp.type == 8



Al capturar tráfico, tomamos mensajes intercambiados entre diferentes equipos. Cada equipo necesita una dirección :

- **URLs**: (ejemplo: `www.uma.es`)
  - Fáciles de recordar para los seres humanos
  - Usadas por protocolos que interactúan con usuarios humanos (capa aplicación)
- **IPs**: (ejemplo: `150.214.33.47`)
  - Configurables, enrutables, longitud fija ...
  - Es el nombre "oficial"
- **MACs**: (ejemplo: `1d:e2:84:00:ff:3d`)
  - Para comunicaciones entre equipos conectados entre sí
  - Habitualmente asignadas por el fabricante







# Tráfico: Servidores y redes

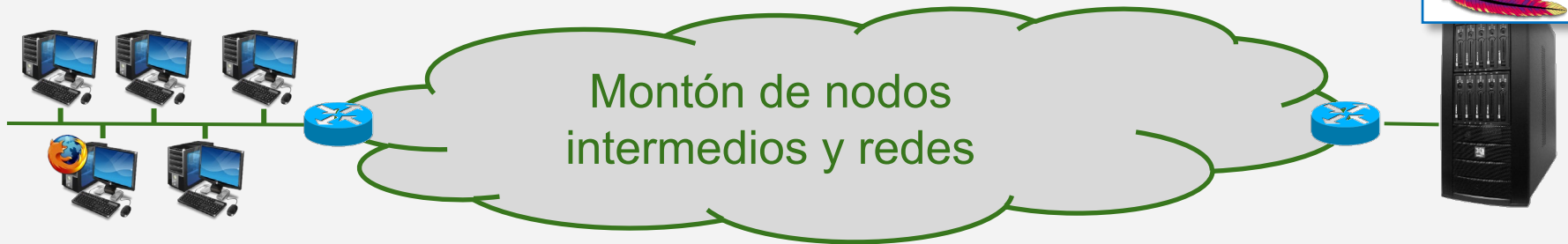
En nuestra red podemos comunicarnos directamente (capa enlace )

Pero habitualmente nos comunicamos con equipos que no están en nuestra red (no podemos comunicarnos directamente )

Tenemos un (o varios) nodos intermedios que nos permiten salir a otras redes : **routers**

Principalmente veremos dos tipos de tráfico (a bajo nivel : enlace) :

- Nosotros <-> Otros equipos de nuestra red
- Nosotros <-> Router (que irá a equipos externos)





# Generando y capturando tráfico

10

- Arranque su navegador favorito
- Arranque una línea de comandos (cmd)
- Arranque Wireshark, elija su interfaz de red y empiece a capturar
- En la línea de comando, copie estos tres comandos:  

```
ipconfig /flushdns
```

```
ping www.informatica.uma.es
```
- En el navegador acceda a la siguiente URL:  

```
http://www.informatica.uma.es
```
- Pare de capturar tráfico con Wireshark
- Guarde la traza como p1.pcapng



# ¿Qué pasa cuando pedimos una web?

11



Quiero conectarme a  
**www.informatica.uma.es**

Puff, yo necesito IPs, no  
URLs, pero no problema

Torre  
TCP/IP  
(Mi equipo)

Torre  
TCP/IP  
(Mi equipo)

Mi amigo DNS (150.214.57.7)  
me convierte URLs a IPs

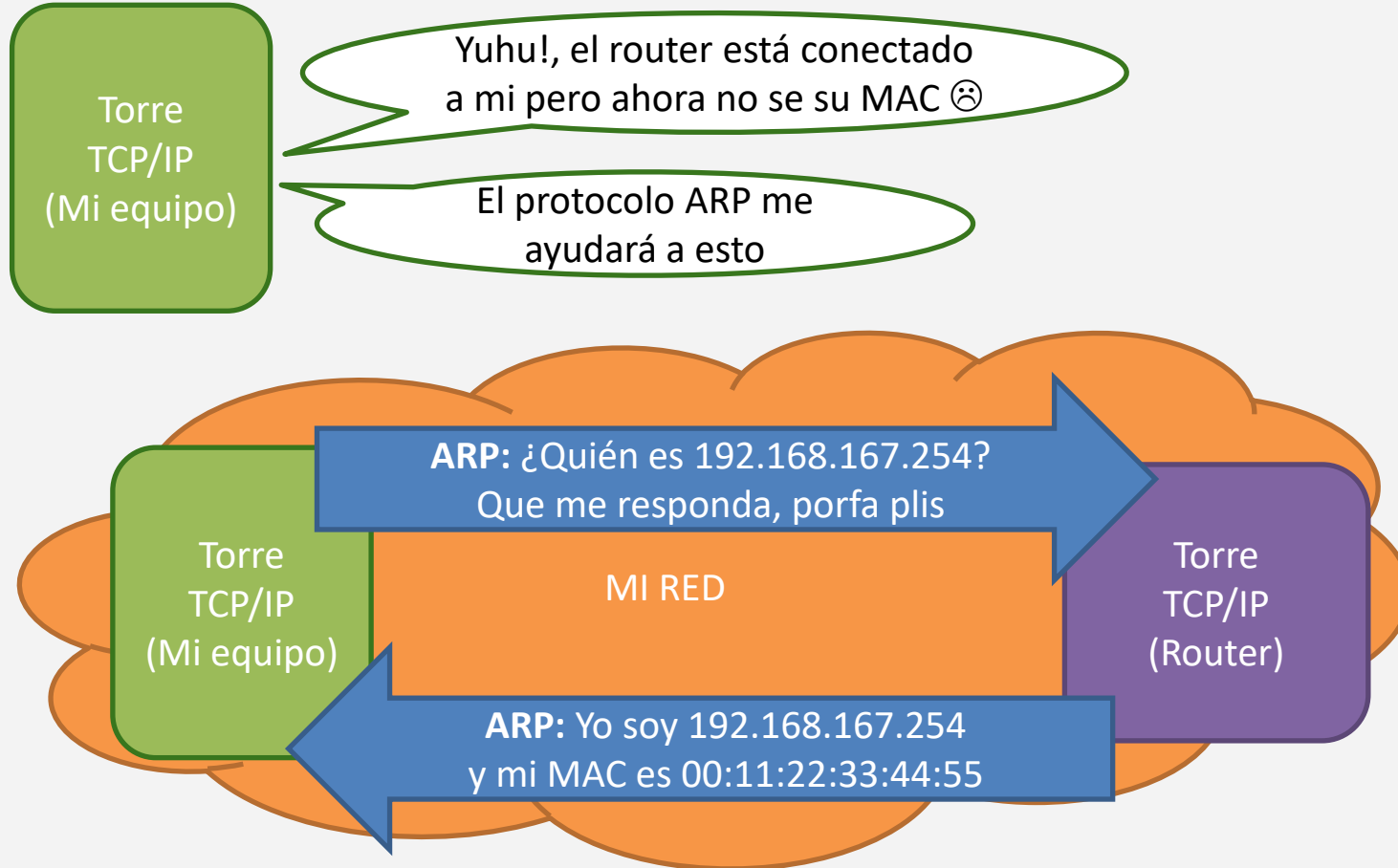
Mi amigo DNS no está  
conectado a mi ☹

Para llegar a él debo enviar  
al router (192.168.167.254)



# ¿Qué pasa cuando pedimos una web?

12



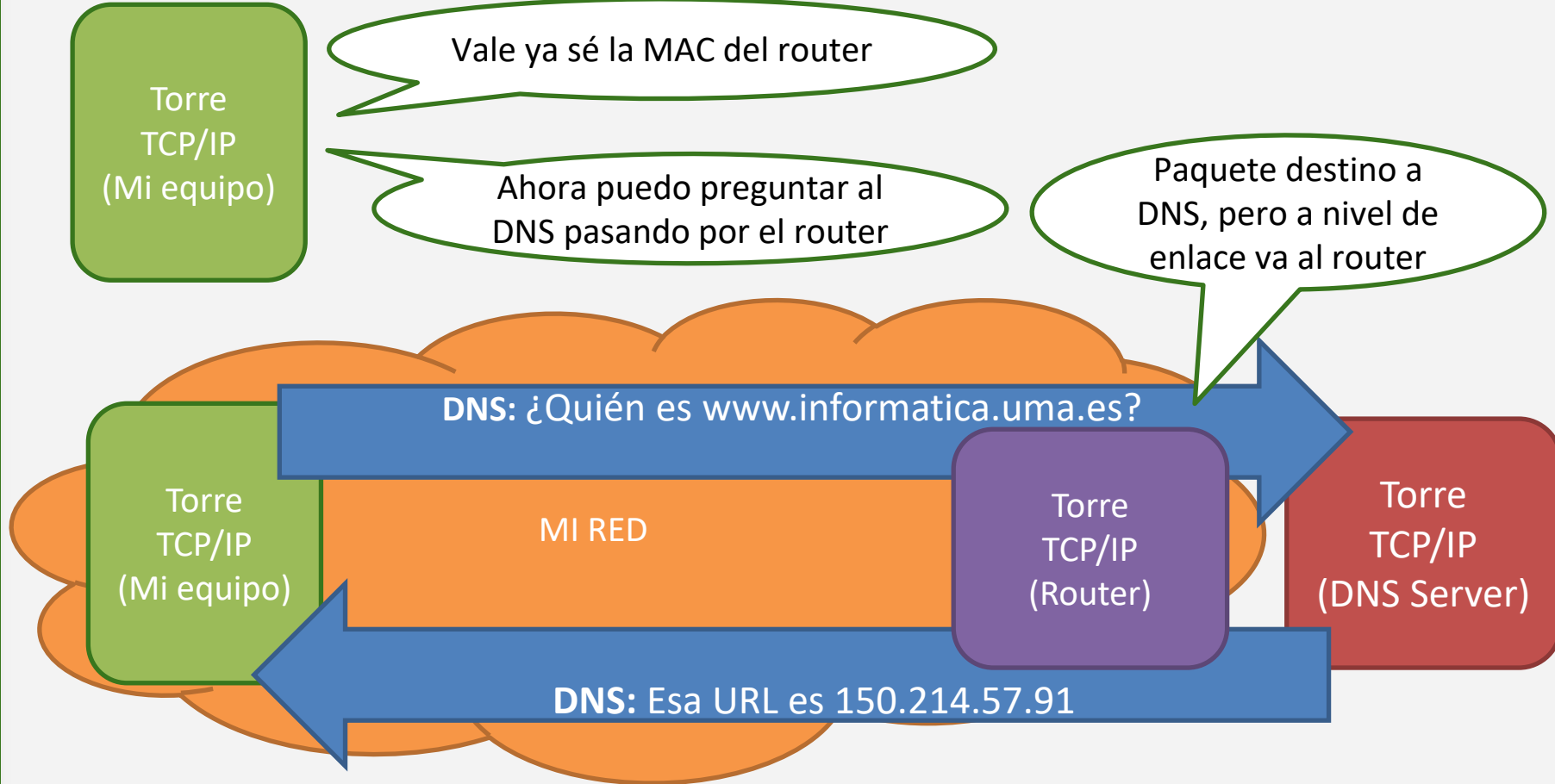


# ¿Qué pasa cuando pedimos una web?

13

Tráfico

Práctica 1  
Redes y Sistemas Distribuidos (GI Software A))



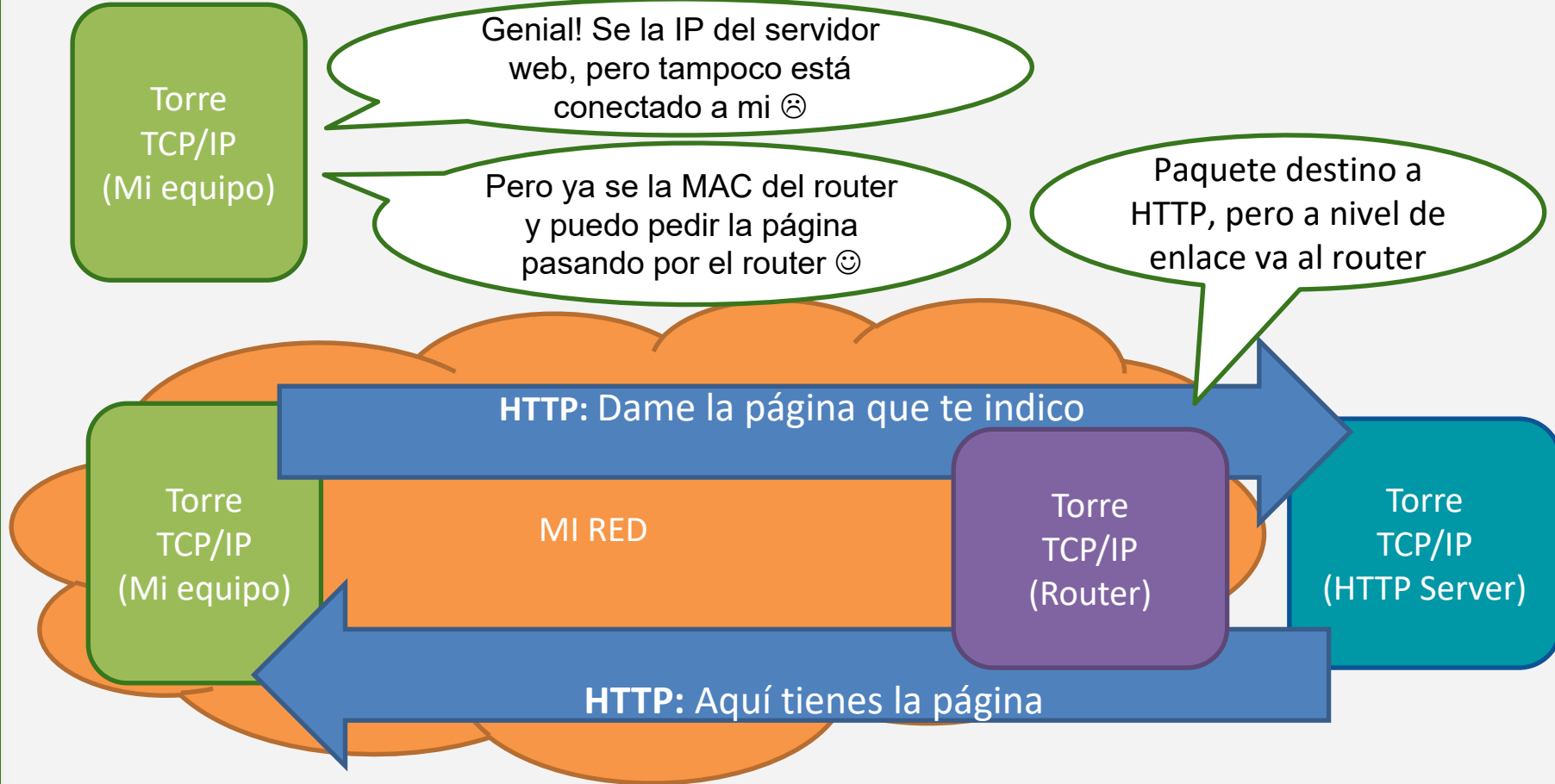


# ¿Qué pasa cuando pedimos una web?

14

Tráfico

Práctica 1  
Redes y Sistemas Distribuidos (GI Software A))





# Y, ¿si hago ping?

15



Quiero hacer un ping a  
**www.informatica.uma.es**

Ajá, esta vez tengo todo 😊

Torre  
TCP/IP  
(Mi equipo)

ICMP: Hooooooooaaaaa, ¿estás vivo?

Torre  
TCP/IP  
(Mi equipo)

MI RED

Torre  
TCP/IP  
(Router)

Torre  
TCP/IP  
(HTTP Server)

ICMP: Hola, por aquí estoy



# Resumen de tráfico que generamos

16

Tráfico

- ➡ Petición **ARP** (Dada la IP del router buscamos su MAC. Envía a todos)
- ⬅ Respuesta **ARP** (El router nos informa de su MAC)

- ➡ Petición **DNS** (Pedimos la IP de informatica.cv.uma.es)
- ⬅ Respuesta **DNS** (El servidor de DNS nos informa de la IP)

- ➡ Petición **HTTP** (Pedimos la página inicial de `www.informatica.uma.es` )
- ⬅ Respuesta **HTTP** (Nos devuelve la página y recursos) }xN

- ➡ Petición **ICMP** (Hacemos ping a `www.informatica.uma.es` )
- ⬅ Respuesta **ICMP** (Respuesta al ping) }x4





¿Hay que entregar algo?

- No

¿Cómo se evalúa?

- Prueba en la siguiente sesión práctica
- Unos 15 minutos
- Preguntas similares a las de la práctica pero con datos que os facilitamos nosotros

**Se recomienda hacerlas, entenderlas y rellenar la memoria (digital o manual) para repaso interno**