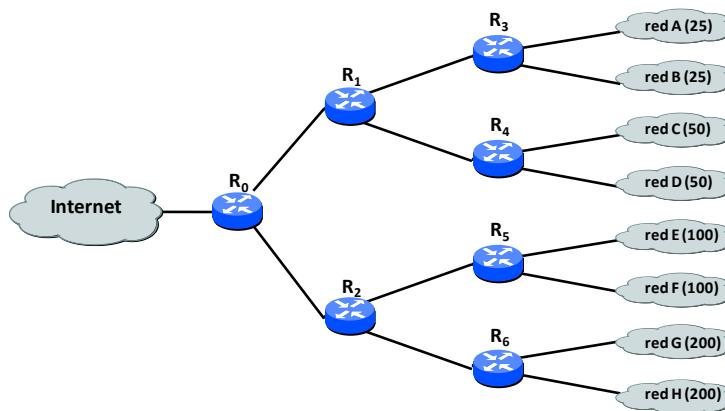


Ejercicios – Tema 5

- En la figura siguiente suponga que R_0 corresponde con el servidor DNS raíz de un espacio de nombres de dominio ficticio, R_1 y R_2 son los servidores de los dominios $.R1$ y $.R2$ respectivamente, R_3 corresponde con el servidor del dominio $.R3.R1$, etc. Suponiendo resolución recursiva, describa paso a paso **los mensajes DNS intercambiados** para enviar un correo desde un MUA situado en la red A, a un destinatario cuya MTA estuviera instalada en MTA.R6.R2.



- ¿Qué tienen en común HTTP y SMTP?
- Discuta breve y razonadamente los principales retos y soluciones para el desarrollo de servicios IP multimedia (voz, vídeo, ...) desde la perspectiva de: (a) consumo de ancho de banda, (b) retardo de transmisión y (c) confidencialidad de los datos.
- Explique detalladamente (incluyendo los mensajes de resolución de nombres que sean necesarios suponiendo resolución recursiva) todos los mensajes de aplicación intercambiados en el envío y recepción de un correo electrónico (suponga IMAP) entre dos MUAs.
- Suponga dos usuarios de correo electrónico, $user1$ y $user2$, situados en sendos puestos de trabajo $H1$ y $H2$. Las estafetas de correo correspondientes son $mailserver.com$ y $servidormail.es$. Describa todos los pasos y protocolos involucrados en los siguientes procesos:
 - Redacción y envío de un email de $user1$ a $user2$, desde el punto de vista del primero de ellos.
 - Recepción del mensaje en $servidormail.es$.
 - Descarga y lectura del correo por parte de $user2$.
- ¿Qué diferencias o semejanzas hay entre POP e IMAP?
- Desde un ordenador se arrancan tres navegadores diferentes, Internet Explorer, Mozilla Firefox y Google Chrome, y se accede desde los tres a un servidor web en la dirección 147.156.1.4 (el mismo desde los tres) ¿Cuántos sockets y cuantas conexiones TCP están implicados, tomando en cuenta tanto el lado servidor como el cliente?
- Discuta las características de las siguientes aplicaciones en términos de su tolerancia a la pérdida de datos, los requisitos temporales, la necesidad de rendimiento mínimo y la seguridad.



- a. La telefonía móvil
- b. WhatsApp
- c. YouTube
- d. Spotify
- e. Comercio electrónico

Nótese que el diseño de una aplicación siempre debe tener en cuenta todas las características anteriores. No obstante, varias de estas características son difíciles de conseguir de forma simultánea, cuando no son antagónicas. Por este motivo, el diseño de una aplicación debe considerar qué características primar en detrimento de otras.

Se propone la siguiente tabla de asignación de prioridades, utilizando la siguiente notación:

Requisito fundamental: ↑ Requisito relevante: ↔ Requisito secundario: ↓

	Tolerancia a pérdidas	Requisitos Temporales (Delay)	Rendimiento (<i>Throughput</i>)	Seguridad
Telefonía móvil	↓	↑	↑	↔
WhatsApp	↑	↓	↓	↔
YouTube	↓	↔	↑	↓
Spotify	↓	↔	↑	↓
Comercio Electrónico	↑	↔	↔	↑

12. ¿Es posible que un host tenga varias direcciones IP y un único nombre de dominio? Discuta un caso.

Sí. Por ejemplo un host que tenga varias interfaces de red.

¿Es posible que un host tenga varios nombres de dominio y una única dirección IP? Discuta un caso.

Sí, típicamente un host tiene un nombre canónico y varios *alias*.

¿Es posible que varios host tengan el mismo nombre de dominio, aunque direcciones IP distintas? Discuta un caso.

Si, esto puede hacerse para que el servidor DNS realice balanceo de tráfico, rotando su respuesta ante solicitudes de un determinado nombre de dominio (ej. www.google.com es, en realidad, un grupo de hosts con diferentes direcciones IP)

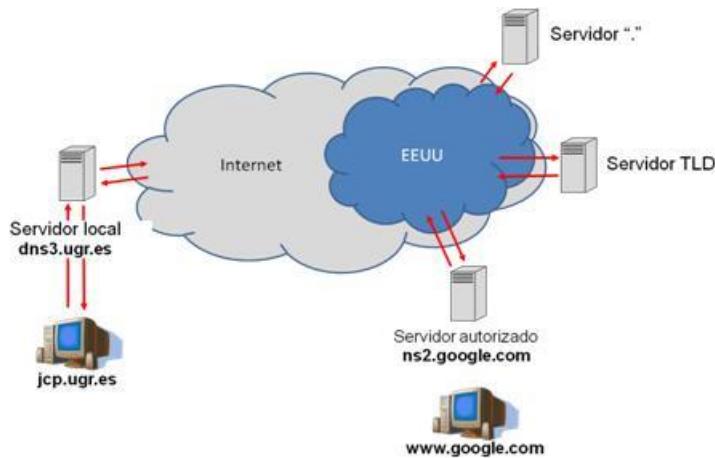
13. ¿Qué carga más un servidor DNS, accesos iterativos o recursivos?

Desde el punto de vista de un servidor DNS que debe solicitar la traducción de un nombre a otro servidor, al primero le cargarán más accesos iterativos que recursivos, pues en el primer caso es él mismo el que se encarga de ir contactando con los respectivos servidores DNS hasta resolver completamente la petición del cliente. Si bien es cierto que un servidor que resuelve iterativamente está liberando de carga a los servidores DNS con los que contacta.

¿Cuál de estos dos accesos carga más la red?

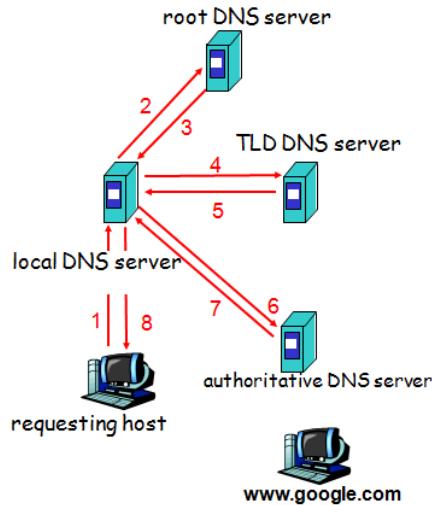
Los dos por igual, ya que el número de solicitudes y respuestas necesario para resolver una determinada solicitud de DNS es la misma.

14. En la siguiente figura se ilustra un ejemplo de acceso DNS por parte de una máquina (jcp.ugr.es) que quiere acceder a los servicios de www.google.com. Para obtener la dirección IP del servidor, es necesario que la consulta pase por todos los servidores del gráfico. Considerando unos retardos promedio de 8 µs dentro de una red LAN, de 12 ms en cada acceso a través de Internet (4 ms si la conexión se restringe a EEUU) y de 1 ms de procesamiento en cada servidor:



- Calcule el tiempo que se tardaría si la solicitud al servidor local es recursiva, pero el propio servidor local realiza solicitudes iterativas.

En definitiva, el esquema que se propone analizar es el siguiente:



El tiempo total invertido en la resolución es:

$$r_{resolución} = ret_{LAN} + ret_{Internet};$$

Donde:

$$\begin{aligned} ret_{LAN} &= 2 \cdot r_{LAN} + r_{servidor}; \\ ret_{Internet} &= 6 \cdot r_{España-EEUU} + 3 \cdot r_{servidor}; \end{aligned}$$

Teniendo en cuenta los datos del ejercicio:

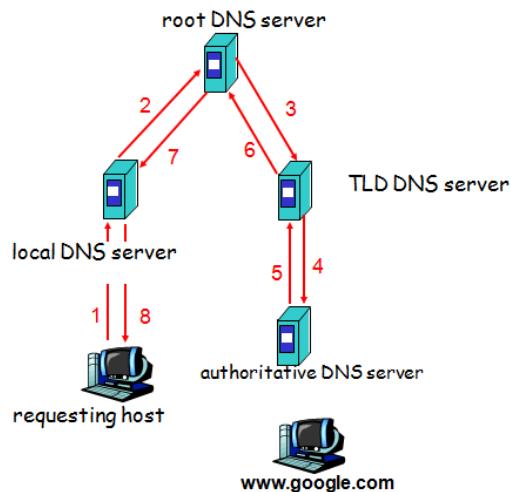
$$\begin{aligned} r_{LAN} &= 8\mu s; \\ r_{España-EEUU} &= 12 \cdot 10^3 \mu s; \quad r_{EEUU-EEUU} = 4 \cdot 10^3 \mu s; \quad r_{servidor} = 1 \cdot 10^3 \mu s \end{aligned}$$

Tenemos que:

$$r_{resolución} = 76,016 ms$$

- b. Especifique una política (recursiva-iterativa) más rápida de solicitudes y el tiempo que tardaría la solicitud en ser respondida. ¿Qué desventaja tiene sobre la solución anterior?

Una política más rápida en el supuesto que nos ocupa es esta:



$$2 \cdot r_{LAN} + r_{Serv} + 2 \cdot r_{int} + 4 \cdot r_{red_EEUU} + 3 \cdot r_{serv}$$

En este caso tenemos que:

$$ret_{Internet} = 2 \cdot r_{España-EEUU} + 4 \cdot r_{EEUU-EEUU} + 3 \cdot r_{servidor}$$

Con lo cual:

$$r_{resolución} = 44,016 \text{ ms}$$

El principal problema de esta estrategia es la sobrecarga del servidor raíz, aunque en todo caso se ha intentado minimizar haciendo a su vez una solicitud recursiva al servidor TLD.

15. Compare el rendimiento en términos temporales de HTTP persistente y no persistente considerando los siguientes parámetros:
- Descarga de una página web con 10 objetos incrustados
 - Tiempo de Establecimiento de conexión TCP → 5 ms
 - Tiempo de Cierre de conexión TCP → 5 ms
 - Tiempo de solicitud HTTP → 2 ms
 - Tiempo de respuesta HTTP (página web u objeto) → 10 ms

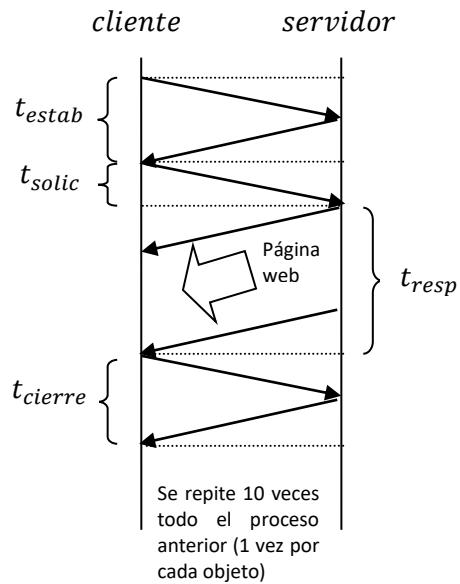
Para HTTP no persistente tenemos que el proceso de descarga sería el siguiente:

Persistente

1. Establecimiento
2. Solicitud HTTP } × 10
3. Respuesta HTTP }
4. Cierre

No persistente

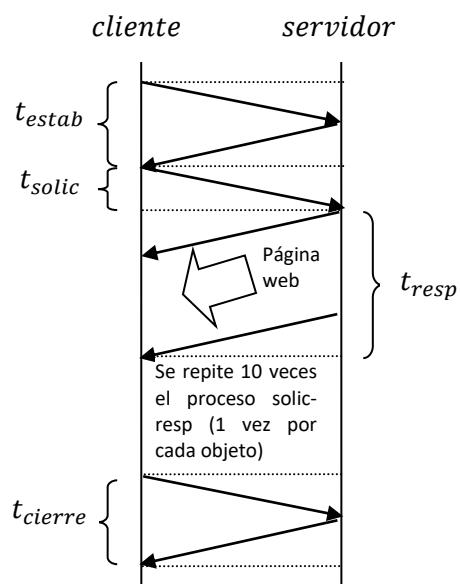
1. Establecimiento
 2. Solicitud HTTP }
 3. Respuesta HTTP }
 4. Cierre
- } × 10



El tiempo de descarga para el modo HTTP no persistente es por lo tanto:

$$r_{descarga}^{np} = 11 \times (t_{estab} + t_{solic} + t_{resp} + t_{cierre}) = 242ms$$

Para HTTP persistente tenemos que el proceso de descarga sería el siguiente:



El tiempo de descarga para el modo HTTP persistente es por lo tanto:



$$r_{descarga}^p = t_{estab} + 11 \times (t_{solic} + t_{resp}) + t_{cierre} = 142ms$$

16. Una sucursal con 50 empleados en Granada tiene una red interna basada en *FastEthernet* (100Mbps) que se conecta a Internet con una red de acceso ADSL de 0,5 Mbps de subida y 1,5 Mbps de bajada. Cada empleado, en el desempeño de su trabajo, realiza un promedio de 2000 solicitudes de información a la hora a un servidor de Base de Datos ubicado en la central del banco, en Madrid, donde cada solicitud supone el envío por parte del servidor de un promedio de 10 registros de 1KB cada uno. Adicionalmente, la modificación de datos tras algunas de estas solicitudes supone el envío promedio de 100 actualizaciones, de 10 registros de media, a la hora desde la sucursal al servidor. El resto de los servicios telemáticos se restringe.

Calcule el promedio de la velocidad de transmisión requerida. ¿Es la velocidad del enlace de acceso suficiente?

Despreciando los paquetes de solicitud y confirmación, que contarán simplemente con cabeceras, podemos ver la velocidad requerida en promedio:

$$\begin{aligned} v_{download} &= 10 \frac{KB}{sol} \times (8 \times 1024) \frac{b}{KB} \times 2000 \frac{sol}{emp \times hora} \times 50 emp \\ &\quad \times \frac{1}{3600} \frac{hora}{s} \end{aligned}$$

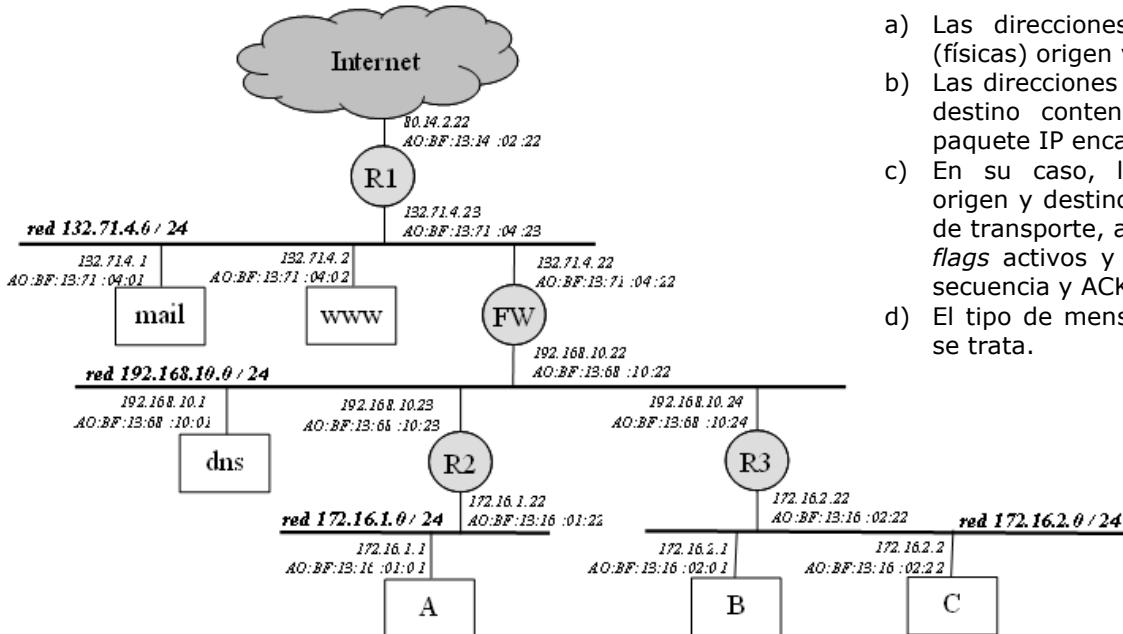
$$v_{download} = 2,28 \cdot 10^6 bps = 2,28Mbps$$

$$\begin{aligned} v_{upload} &= 10 \frac{KB}{act} \times (8 \times 1024) \frac{b}{KB} \times 100 \frac{act}{emp \times hora} \times 50 emp \\ &\quad \times \frac{1}{3600} \frac{hora}{s} \end{aligned}$$

$$v_{upload} = 0,11Mbps$$

La velocidad del enlace es insuficiente, ya que el download requerido en promedio es menor que el de la red.

17. Dada la topología adjunta correspondiente a una red corporativa, en la que se especifican tanto las direcciones IP como las MAC de cada uno de los dispositivos que la forman, analice el tráfico generado al hacer un acceso de correo electrónico desde el host "B" al servidor "mail", especificando en una tabla, y para cada trama Ethernet generada:

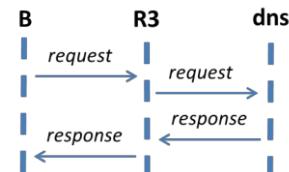


- a) Las direcciones hardware (físicas) origen y destino.
- b) Las direcciones IP origen y destino contenidas en el paquete IP encapsulado.
- c) En su caso, los puertos origen y destino de la PDU de transporte, así como los flags activos y campos de secuencia y ACK.
- d) El tipo de mensaje de que se trata.

NOTA: suponga todas las tablas ARP son conocidas y, por simplicidad utilice sólo el último de los 6 octetos de las direcciones físicas de las NIC (interfaces o tarjetas de red)

1) PASO 1: Petición DNS y Respuesta

Es una **petición sobre UDP** □ no hay establecimiento de conexión previo



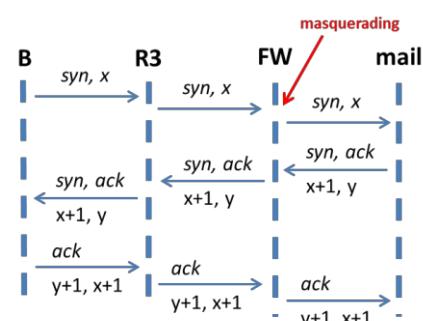
ETH ORI.	ETH DES.	IP ORI.	IP DEST.	PORT ORI.	PORT DES.	FLAGS	MENSAJE	COMENTARIOS
01 (B)	22 (R3)	172.16.2.1 (B)	192.168.10.1 (dns)	(1*)	53	---	Solicitud DNS. Dominio mail	A través de R3
24 (R3)	01 (dns)	172.16.2.1 (B)	192.168.10.1 (dns)	(1*)	53	---	Solicitud DNS. Dominio mail	Retransmisión a dns
01 (dns)	24 (R3)	192.168.10.1 (dns)	172.16.2.1 (B)	53	(2*)	---	Respuesta DNS IP de mail	A través de R3
22 (R3)	01 (B)	192.168.10.1 (dns)	172.16.2.1 (B)	53	(2*)	---	Respuesta DNS IP de mail	Retransmisión a B

(1*) Asignado por el S.O. . (2*) Puerto elegido en (1*)

2) PASO 2: Establecimiento conexión TCP

SMTP → sobre TCP en el puerto 25

Masquerading es una traducción de IPs entre subredes. Hay que hacerlo para poder salir a la zona de direcciones públicas de la red



ETH ORI.	ETH DES.	IP ORI.	IP DEST.	PORT ORI.	PORT. DES.	FLAGS	MENSAJE	COMENTARIOS
02:01 (B)	02:22 (R3)	172.16.2.1 (B)	132.71.4.1 (mail)	(1*)	25	SYN x (3*)	Solicitud estab. TCP a mail	A través de R3
10:24 (R3)	10:22 (FW)	172.16.2.1 (B)	132.71.4.1 (mail)	(1*)	25	SYN x (3*)	Solicitud estab. TCP a mail	Retransmisión a FW
04:22 (FW)	04:01 (mail)	132.71.4.22 (FW)	132.71.4.1 (mail)	(5*)	25	SYN x (3*)	Solicitud estab. TCP a mail	Masquerading (4*) FW entrega a mail
04:01 (mail)	04:22 (FW)	132.71.4.1 (mail)	132.71.4.22 (FW)	25	(5*)	SYN, ACK x+1, y	Aceptación y estab. en el otro sentido	mail hacia FW
10:22 (FW)	10:24 (R3)	132.71.4.1 (mail)	172.16.2.1 (B)	25	(2*)	SYN, ACK x+1, y	Aceptación y estab. en el otro sentido	Deshace Masquerading (4*) FW retransm. a R3
02:22 (R3)	02:01 (B)	132.71.4.1 (mail)	172.16.2.1 (B)	25	(2*)	SYN, ACK x+1, y	Aceptación y estab. en el otro sentido	R3 retransm. a B
02:01 (B)	02:22 (R3)	172.16.2.1 (B)	132.71.4.1 (mail)	(2*)	25	ACK x+1, y+1	Aceptación en el otro sentido	A través de R3
10:24 (R3)	10:22 (FW)	172.16.2.1 (B)	132.71.4.1 (mail)	(2*)	25	ACK x+1, y+1	Aceptación en el otro sentido	Retransmisión a FW
04:22 (FW)	04:01 (mail)	132.71.4.22 (FW)	132.71.4.1 (mail)	(5*)	25	ACK x+1, y+1	Aceptación en el otro sentido	Masquerading (4*) FW entrega a mail

(1*) Asignado por el S.O. (2*) Puerto elegido en (1*) (3*) Num. Aleatorio elegido por el emisor

(4*) FW al hacer masquerading mapea

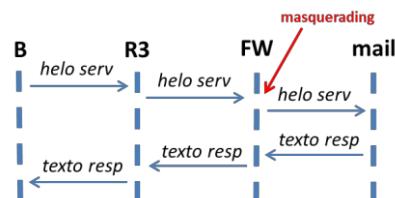
[IP intranet, puerto host intranet] → [IP pública FW, puerto libre en FW]

(5*) Puerto elegido por FW en (4*)

3) PASO 3: Acceso a correo electrónico

SMTP → sobre TCP en el puerto 25

Masquerading es una traducción de IPs entre subredes.



Sólo se inicia la conexión...Se podrían enviar más mensajes

ETH ORI.	E TH DES.	IP ORI.	IP DEST.	P ORT ORI.	. PORT DES.	FLAGS	MENS AJE	COMENTARIOS
02:01 (B)	02:22 (R3)	172.16.2.1 (B)	132.71.4.1 (mail)	(2*)	25	x+1	helo servidor	Conexión inicial a servidor SMTP. A través de R3
10:24 (R3)	10:22 (FW)	172.16.2.1 (B)	132.71.4.1 (mail)	(2*)	25	x+1	helo servidor	Retransmisión a FW
04:22 (FW)	04:01 (mail)	132.71.4.22 (FW)	132.71.4.1 (mail)	(5*)	25	x+1	helo servidor	Masquerading (4*) FW entrega a mail
04:01 (mail)	04:22 (FW)	132.71.4.1 (mail)	132.71.4.22 (FW)	25	(5*)	ACK x+1+NB(helo) y+1	texto respuesta servidor	mail hacia FW
10:22 (FW)	10:24 (R3)	132.71.4.1 (mail)	172.16.2.1 (B)	25	(2*)	ACK x+1+NB(helo) y+1	texto respuesta servidor	Deshace Masquerading (4*) FW retransm. a R3
02:22 (R3)	02:01 (B)	132.71.4.1 (mail)	172.16.2.1 (B)	5	2	(2*)	ACK x+1+NB(helo) y+1	R3 retransm. a B

(2*) Puerto elegido por el S.O. en el paso anterior

(4*) FW al hacer masquerading mapea

[IP intranet, puerto host intranet] → [IP pública FW, puerto libre en FW]

(5*) Puerto elegido por FW en (4*)

NB: Número de bytes del mensaje

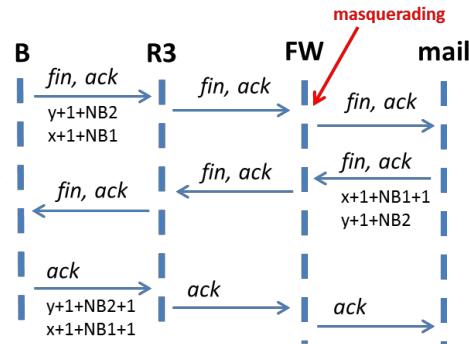
4) PASO 4: Cierre de la conexión TCP

Se envía confirmación del último mensaje del servidor, junto con la solicitud de cierre de conexión

NB1 → longitud en bytes del mensaje "helo"
NB2 → longitud en bytes de la respuesta

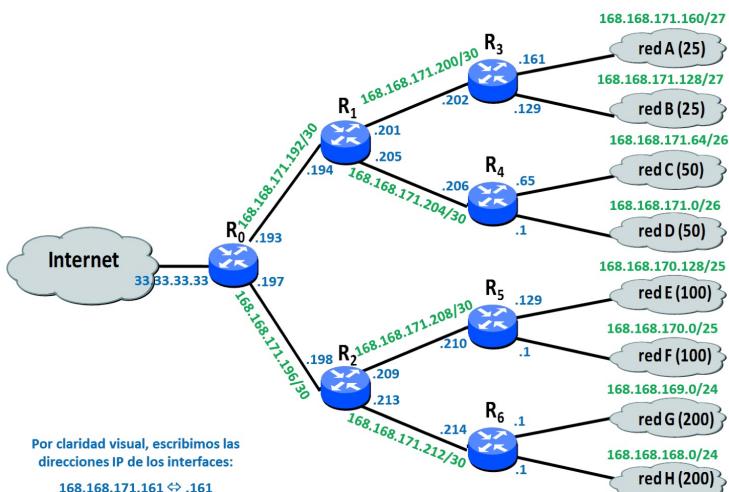
- La tabla y los campos son iguales que los del establecimiento de la conexión, salvo los flags, números de acuse y acks que se muestran en la figura.

** Primero se indican los acuses y luego los identificadores (números de secuencia) de cada segmento **



1. En la figura siguiente suponga que R_0 corresponde con el servidor DNS raíz de un espacio de nombres de dominio ficticio, R_1 y R_2 son los servidores de los dominios $.R1$ y $.R2$ respectivamente, R_3 corresponde con el servidor del dominio $.R3.R1$, etc. Suponiendo resolución recursiva, describa paso a paso **los mensajes DNS intercambiados** para enviar un correo desde un MUA situado en la red A, a un destinatario cuya MTA estuviera instalada en MTA.R6.R2.

Usamos las direcciones IP de las soluciones del tema 2:



otras MAC nos las inventaríamos

MUA = agente de usuario
 $(168.168.171.162)$

MTA = servidor de correo
 MTA.R6.R2

Suponemos que DNS se apoya en UDP, que es lo común

IP Src	IP Dest	MACsrc	MACdst	Sport	Dport	Flags	Msg
$168.168.171.162$	$168.168.171.193$	MAC-E1	MAC-R3-N	(*) 50	53	-	DNS request
"	"	MAC-R3-O	MAC-R1-N	"	"	"	"
"	"	MAC-R1-O	MAC-R0-N	"	"	"	"
171.197	171.198	MAC-R0-S	MAC-R2-O	"	"	"	"
171.213	171.214	MAC-R2-S	MAC-R6-O	"	"	"	"
171.214	171.213	MAC-R6-O	MAC-R2-S	53	(*) 50	"	DNS response
171.198	171.197	MAC-R2-O	MAC-R0-S	"	"	"	"
171.193	171.192	MAC-R0-N	MAC-R1-O	"	"	"	"
"	"	MAC-R1-N	MAC-R3-O	"	"	"	"
"	"	MAC-R3-N	MAC-E1	"	"	"	"

2. ¿Qué tienen en común HTTP y SMTP?

Ambos son protocolos de aplicación de dominio público.

HTTP (Navegación Web)

- Es un protocolo de transferencia de hipertexto.
- Transfiere archivos entre servidor web y cliente web.
- Se usa para web (soportado por TCP) y para streaming multimedia (soportado por TCP y/o UDP).
- Usa TCP en el puerto 80.
- Es stateless: el servidor no mantiene información sobre las peticiones de los clientes, sino que el equipo del cliente almacena cookies.
- Hay dos tipos de servidores:
 - Persistente: No mantiene la conexión TCP abierta.
 - No persistente: Mantiene la conexión TCP abierta.
- Hay dos tipo de mensaje: request y response.

SMTP (Correo electrónico)

- Es un protocolo de transferencia simple de correo orientado a conexión que consta de tres fases: three-way handshake, comunicación y cierre).
- Transfiere correos a través de servidores de correos.
- Es soportado por TCP.
- Usa TCP en el puerto 25.
- Siempre se usa este protocolo para envío de e-mail, pero no para descarga/lectura.
- Se implementa mediante dos programas: cliente SMTP y servidor SMTP.
- El servidor es persistente (mantiene la conexión abierta).
- Los mensajes están codificados en ASCII de 7 bits.

Concluimos con los esquemas de envío/recepción de mensajes en HTTP y SMTP:

Tema 5. Capa de aplicación

3. La navegación web

MENSAJES HTTP



1. El cliente HTTP (navegador) solicita un objeto identificado por su URL, en el ejemplo www.ugr.es/pages/universidad. Según la configuración del servidor, si no se especifica nada, por defecto se sirve el fichero index.html
2. El cliente consulta al resolver de DNS por la dirección IP de www.ugr.es
3. DNS contesta 150.214.27.71 (IP virtual de un servicio balanceado)
4. El cliente abre una conexión TCP al puerto 80 de 150.214.27.71 (3 bandas)
5. El cliente envía una petición "GET /pages/universidad/ ..." (más otra información adicional: cabeceras, cookies, variables, etc)
6. El servidor responde enviando el fichero "index.html" por la misma conexión TCP
7. Al usar TCP el cliente y servidor de HTTP reciben un servicio orientado a conexión, fiable, sin errores, con control de flujo, con control de congestión, etc. Es decir una comunicación TRANSPARENTE y FIABLE.
8. Si es persistente se siguen solicitando objetos de la página ("GET...") por la conexión
9. Se cierra la conexión TCP y se liberan recursos en el servidor y cliente
10. El cliente visualiza el contenido

Fundamentos de Redes - Curso 2021-2022
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

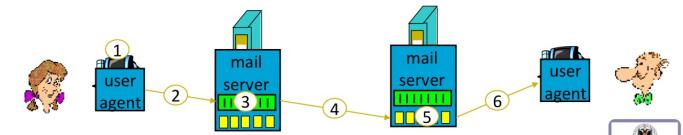
Tema 5. Capa de aplicación

4. El correo electrónico

SMTP (RFC 2821)

Pasos en el envío/recepción de correo

- 1) El usuario origen compone mediante su Agente de Usuario (MUA) un mensaje dirigido a la dirección de correo del usuario destino
- 2) Se envía con SMTP (ó HTTP) el mensaje al servidor de correo (MTA) del usuario origen que lo sitúa en la cola de mensajes salientes
- 3) El cliente SMTP abre una conexión TCP con el servidor de correo (MTA) (obtenido por DNS) del usuario destino
- 4) El cliente SMTP envía el mensaje sobre la conexión TCP
- 5) El servidor de correo del usuario destino ubica el mensaje en el mailbox del usuario destino
- 6) El usuario destino invoca su Agente de Usuario (MUA) para leer el mensaje utilizando POP3, IMAP ó HTTP



Fundamentos de Redes - Curso 2021-2022
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

3. Discuta breve y razonadamente los principales retos y soluciones para el desarrollo de servicios IP multimedia (voz, vídeo, ...) desde la perspectiva de: (a) consumo de ancho de banda, (b) retardo de transmisión y (c) confidencialidad de los datos.

a) Los archivos de vídeo son los que más consumen ancho de banda. Esto implica que las aplicaciones de red necesiten mucho ancho de banda para soportar el envío, descarga y subida de archivos de este tipo.

b) El retraso de transmisión de los datos se debe a que los archivos multimedia son más grandes que otros. Surgen distintos tipos de aplicaciones, que se distinguen por cómo gestionan el ancho de banda:

- Aplicaciones time-sensitive (inelásticas), como audio y vídeo en tiempo real (streaming), juegos interactivos... Requieren un delay acotado para ser efectivas. Se basan en UDP.

- Aplicaciones elásticas: Para documentos web, mails... y que son menos exigentes temporalmente. Se basan en TCP. No suelen ser de tiempo real, por lo que precisan de un delay acotado para poder ser efectivas.

c) Aunque las aplicaciones han de ser seguras, el nivel de seguridad depende de la importancia de esta.

4. Explique detalladamente (incluyendo los mensajes de resolución de nombres que sean necesarios suponiendo resolución recursiva) todos los mensajes de aplicación intercambiados en el envío y recepción de un correo electrónico (suponga IMAP) entre dos MUAs.

Tema 5. Capa de aplicación

4. El correo electrónico

SMTP (RFC 2821)

Pasos en el envío/recepción de correo

```

    graph LR
        A[User agent] -- 1. SMTP --> B[mail server]
        B -- 2. --> C[mail server]
        C -- 3. --> D[User agent]
        D -- 4. SMTP --> E[mail server]
        E -- 5. --> F[User agent]
        F -- 6. --> G[User agent]
    
```

1) El usuario origen compone mediante su Agente de Usuario (MUA) un mensaje dirigido a la dirección de correo del usuario destino

2) Se envía con SMTP (ó HTTP) el mensaje al servidor de correo (MTA) del usuario origen que lo sitúa en la cola de mensajes salientes

3) El cliente SMTP abre una conexión TCP con el servidor de correo (MTA) (obtenido por DNS) del usuario destino

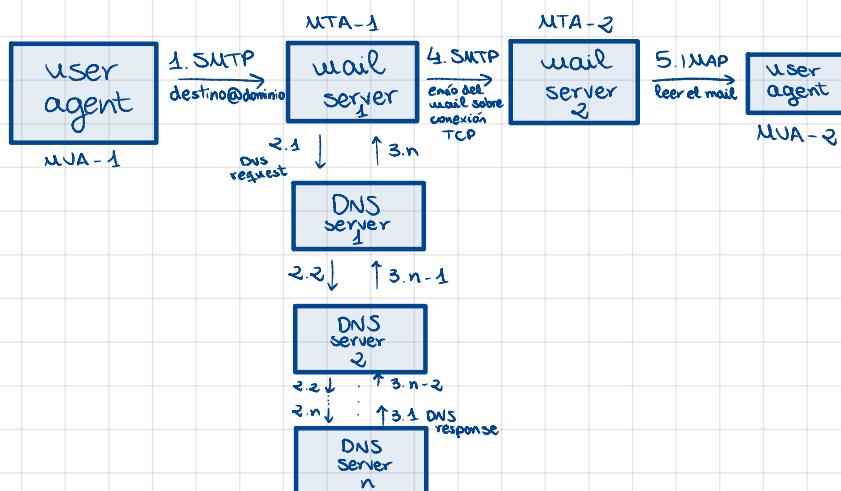
4) El cliente SMTP envia el mensaje sobre la conexión TCP

5) El servidor de correo del usuario destino ubica el mensaje en el *mailbox* del usuario destino

6) El usuario destino invoca su Agente de Usuario (MUA) para leer el mensaje utilizando POP3, IMAP ó HTTP

Fundamentos de Redes - Curso 2021 - 2022
© 2022 v1.0 - Juan M. López-Soler y Jorge Navarro Ortiz

Universidad de Granada



6. ¿Qué diferencias o semejanzas hay entre POP e IMAP?

Ambos son protocolos de aplicación usados para la entrega de mensajes desde un servidor de correo a un usuario final. Sin embargo, tienen bastantes diferencias:

- POP bloquea las bandejas de entrada, permitiendo sólo que un usuario pueda acceder a una bandeja de entrada, mientras que IMAP permite accesos concurrentes en los que se detectan las modificaciones de los otros usuarios (sincronización).
- Ambos usan TCP pero en puertos distintos: 110 (POP3) y 143 (IMAP).
- En POP3 los correos son almacenados en la máquina local del usuario, borrándose automáticamente del servidor de correo, mientras que en IMAP es el servidor el que almacena la información de forma indefinida.
- En POP3 se debe hacer descarga de todo lo que hay para el usuario, mientras que en IMAP se pueden hacer descargas parciales (de partes de mensajes).
- IMAP permite organización en carpetas en el servidor, mientras que POP3 no lo permite, pues el correo se borra del servidor una vez descargado por el agente de usuario.

7. Desde un ordenador se arrancan tres navegadores diferentes, Internet Explorer, Mozilla Firefox y Google Chrome, y se accede desde los tres a un servidor web en la dirección 147.156.1.4 (el mismo desde los tres) ¿Cuántos sockets y cuantas conexiones TCP están implicados, tomando en cuenta tanto el lado servidor como el cliente?

Al ejecutar tres navegadores distintos desde una misma máquina, habrá 3 clientes distintos. Por ello, por cada cliente habrá una conexión TCP con el servidor distinta, por lo que habrá 3 conexiones TCP distintas.

Cada cliente necesitará un socket para conectarse con el servidor (se inicializará con la IP del servidor más el puerto asociado a la aplicación), teniendo así 3 sockets distintos.

En el servidor será necesario un socket por cada conexión TCP, por lo que serán necesarios otros tres sockets.

En resumen, se establecen 3 conexiones TCP y se usan 6 sockets (un par por cada conexión, siendo uno del cliente y otro del servidor).

IP Origen	IP Destino	MAC Origen	MAC Destino	Sport	Dport	Flags	Tipo mensaje
172.16.2.1	192.168.10.1	02:01	02:22	(*) 50	53	-	"
"	"	10:24	10:01	(*) 50	53	-	"
192.168.10.1	172.16.2.1	10:01	10:24	53	(*) 50	-	DNS response
"	"	02:22	02:01	"	"	-	"

172.16.2.1	132.71.4.1	02:01	02:22	1(*) 50	25	SYN, X	Solic.estab.
"	"	10:24	10:22	"	"	"	"
132.71.4.22	"	04:22	04:01	2(*) 50	"	"	"
132.71.4.1	132.71.4.22	04:01	04:22	25	2(*) 50	SYN, ACK 4, X+1	Acept.est. Sol.est. otro sentido
"	172.16.2.1	10:22	10:24	"	1(*) 50	"	"
"	"	02:22	02:01	"	"	"	"
172.16.2.1	132.71.4.1	02:01	02:22	1(*) 50	25	ACK 4+1 X+1	Acept.est otro sentido
"	"	10:24	10:22	"	"	"	"
132.71.4.22	"	04:22	04:01	2(*) 50	"	"	"