UNIVERSIDAD DE GRANADA

Dpto. Teoría de la Señal, Telemática y Comunicaciones
E.T.S. Ingeniería Informática y de Telecomunicación
C/ Periodista Daniel Saucedo Aranda, S/N
18071- Granada

FUNDAMENTOS DE REDES. Teoría. Enero 2024.

Apellidos y nombre: _____ **GRUPO:** _____

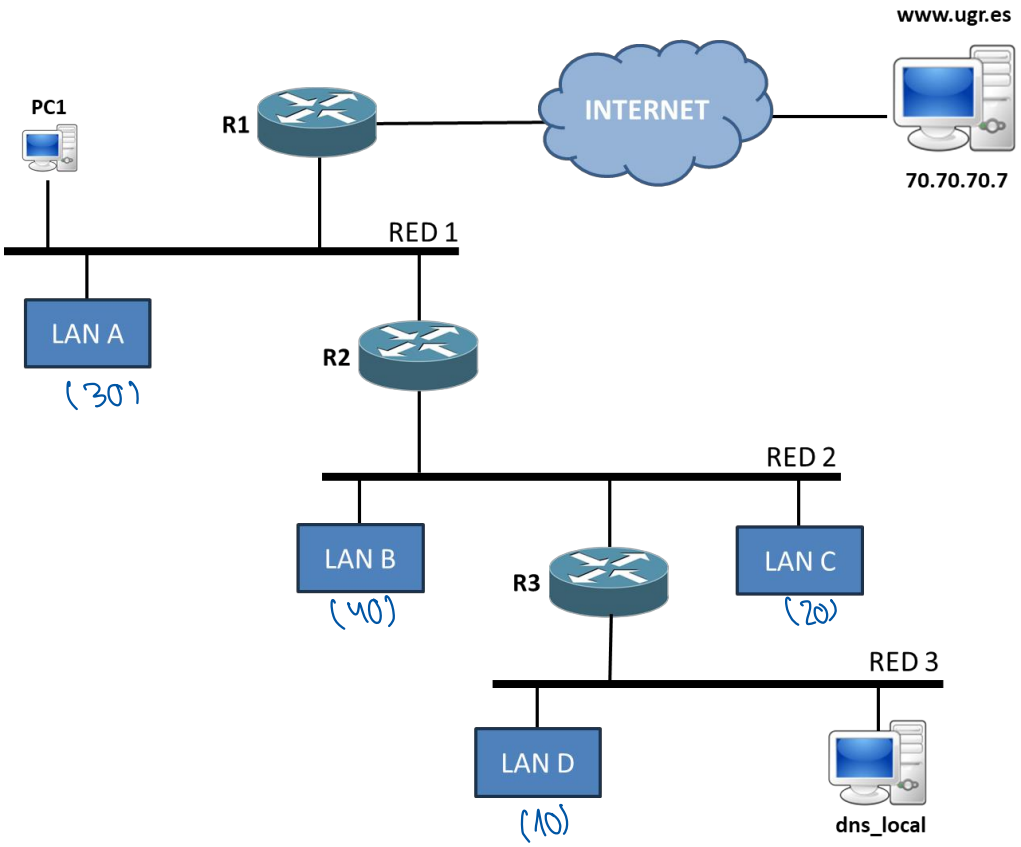
PROBLEMA 1 (3 puntos sobre 10)

En la figura, las distintas LANs tienen respectivamente: A (30 equipos), B (40 equipos), C (20 equipos), D (10 equipos); Suponga que se dispone únicamente de la dirección pública 80.80.80.8

a) *(1 punto)* Realice una **asignación de direcciones IP** a la intranet utilizando direcciones privadas (10.0.0.0) intentando ajustar al máximo los rangos y máscaras.

b) (*0,5 puntos*) Defina las **tablas de encaminamiento** de los tres *routers* y del equipo PC1.

c) (*1,5 puntos*) Suponga que **PC1 solicita la web alojada** en www.ugr.es mediante HTTP. Suponga que PC1 no ha accedido previamente a dicha web y que el servidor de DNS local tiene el registro para ese dominio. Tenga en cuenta que R1 realizará NAT.
Muestre en la tabla la secuencia de todos los mensajes que se producirían para realizar dicha solicitud y para recibir la página HTML de www.ugr.es en PC1.



A7

De mayor a menor tamaño:

- Red 2: 40 equipos + 20 equipos + 2 routers + 1 subred + 1 dif =
  $64 = 2^6 \Rightarrow$ 6 b equipo $\Rightarrow$ 26 b máscara

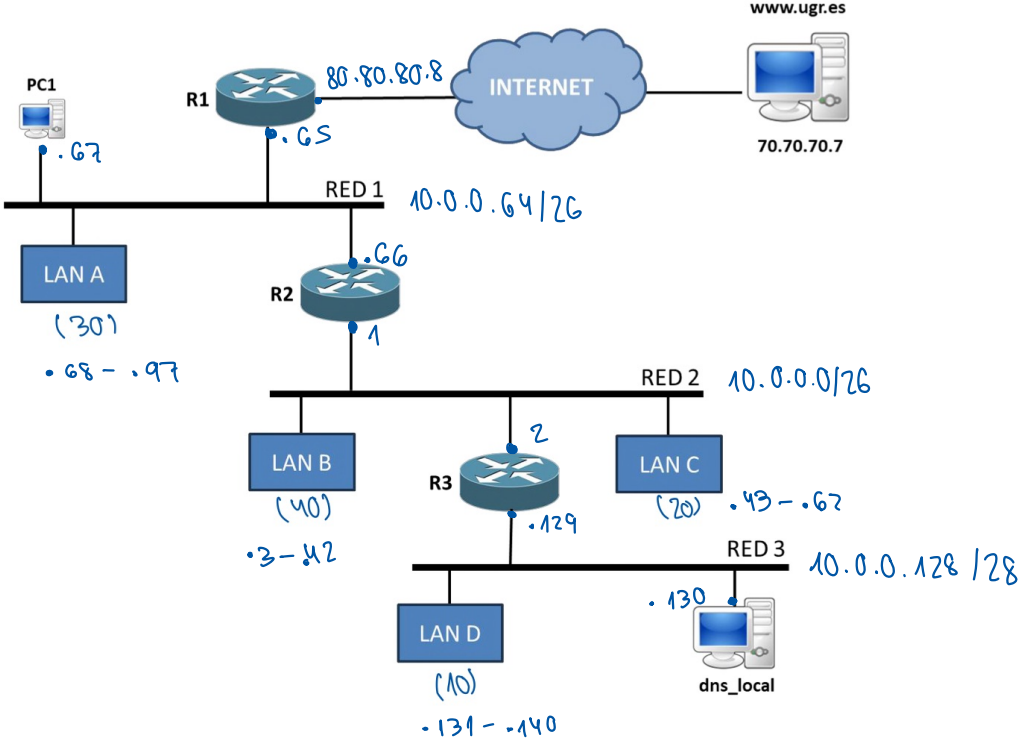
  Red: 10.0.0.0 /26 Difusión: 10.0.0.63

- Red 1: 30 equipos + 1 PC + 2 routers + 1 subred + 1 dif =
  $35 < 2^6 \Rightarrow$ 6 b. equipo $\Rightarrow$ 26 b máscara

  Red: 10.0.0.64/26 Difusión: 10.0.0.127

- Red 3: 10 equipos + 1 DNS + 1 router + 1 subred + 1 dif =
  $14 < 2^4 \Rightarrow$ 4 b equipo $\Rightarrow$ 28 b máscara

  Red: 10.0.0.128/28 Difusión: 10.0.0.143

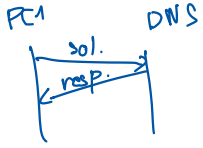


B)

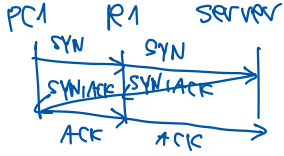
Destino	Mdscara	Sig. Salto	
10.0.0.64	126	*	
0.0.0.0	10	10.0.0.65	PC1
10.0.0.0	126	10.0.0.66	
10.0.0.128	128	10.0.0.66	
10.0.0.64	126	*	
80.80.80.0	124	*	R1
0.0.0.0	10	80.80.80.7	(Router ISP)
10.0.0.0	126	10.0.0.66	
10.0.0.128	128	10.0.0.66	
10.0.0.0	126	*	
10.0.0.64	126	*	R2
0.0.0.0	10	10.0.0.65	
10.0.0.128	128	10.0.0.2	
10.0.0.128	128	*	
10.0.0.0	126	*	R3
0.0.0.0	10	10.0.0.1	

C)

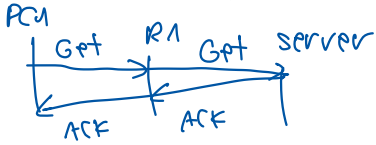
1) Solicitud DNS sobre UDP:



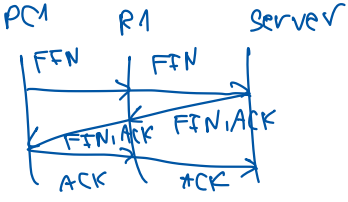
2) Establecimiento conexión TCP:



3) solicitud recurso.



4) Cierre conexión TCP.



IP origen	IP destino	Puerto Origen	Puerto Destino	Flags	Mensaje
10.0.0.67	10.0.0.130	(1*)	53	-	solicitud DNS (UDP)
10.0.0.130	10.0.0.67	53	(1*)	-	respuesta DNS (UDP)
10.0.0.67	70.70.70.7	(2*)	80	SYN	Est. TCP (HTTP)
80.80.80.8 (NAT)	=	(3*)	=	=	=
70.70.70.7	80.80.80.8	80	(3*)	SYN, ACK	1º Resp. TCP (HTTP)
=	10.0.0.67	=	(2*)	SYN, ACK	=
10.0.0.67	70.70.70.7	(2*)	80	ACK	2º resp. TCP (HTTP)
80.80.80.8	=	(3*)	=	=	=
10.0.0.67	70.70.70.7	(2*)	80	-	Get (index.html) (HTTP)
80.80.80.8	=	(3*)	=	=	=
70.70.70.7	80.80.80.8	80	(3*)	ACK	(index.html)
=	10.0.0.67	=	(2*)	=	=
10.0.0.67	70.70.70.7	(2*)	80	FIN, ACK	Fin TCP (HTTP) y confirmación index
80.80.80.8	=	(3*)	=	=	=
70.70.70.7	80.80.80.8	80	(3*)	FIN, ACK	1º Resp. TCP (HTTP)
=	10.0.0.67	=	(2*)	=	=
10.0.0.67	70.70.70.7	(2*)	80	ACK	2º resp. TCP (HTTP)
80.80.80.8	70.70.70.7	(3*)	=	=	=

1* : Puerto de PC1 para UDP - DNS.

2* : Puerto de PC1 para TCP - HTTP

3* : Puerto de R1 (NAT) para TCP - HTTP

EJERCICIO 1

EXAMEN ENERO 2024

a) 10.0.0.0

Ordenamos las redes por su tamaño.

RED 2: LAN B + LAN C + R3 + R2 = 62 + red + difusión = 64 IPs

6 bits → 2^6 = 64 IPs ⇒ /26

(red) 10.0.0.0/26 → 10.0.0.63 (difusión)

RED 1: LAN A + PC1 + R1 + R2 = 33 + red + difusión = 35 IPs

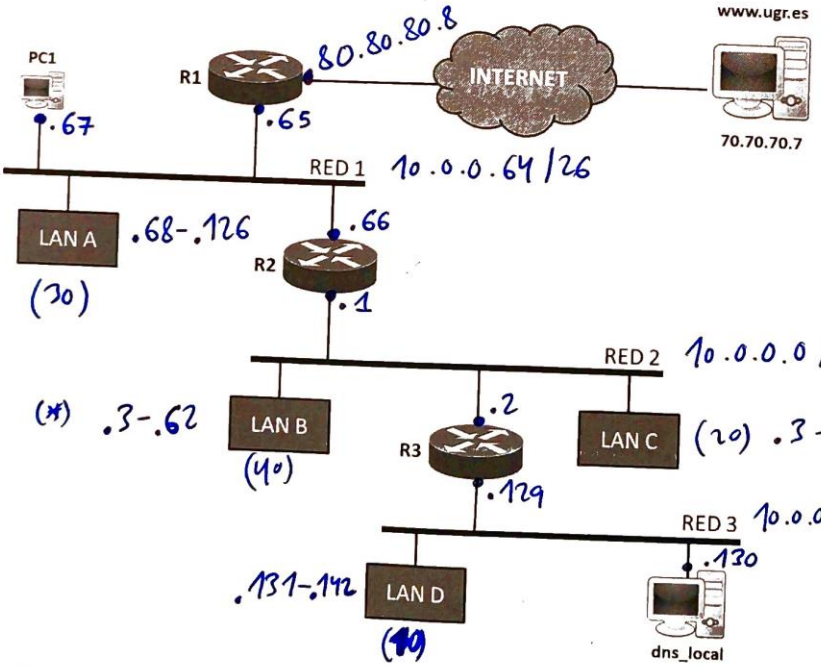
6 bits → 2^6 = 64 IPs ⇒ /26

(red) 10.0.0.64/26 → 10.0.0.127 (difusión)

RED 3: LAN D + DNS + R3 = 12 + red + difusión = 14 IPs

4 bits → 2^4 = 16 IPs ⇒ /28

(red) 10.0.0.128/28 → 10.0.0.143 (difusión)



(*) LAN B y LAN C tomarán IPs en un rango común. Se podrían usar los primeros 40 para LAN B y los últimos 20 para LAN C

b)

R1

DESTINO	MÁSCARA	SIGUIENTE
10.0.0.64	/26	–
80.80.80.0	/24	–
10.0.0.0	/26	10.0.0.66 (R2)
10.0.0.128	/28	10.0.0.66 (R2)
default	–	80.80.80.7 (Router_ISP)

R2

DESTINO	MÁSCARA	SIGUIENTE
10.0.0.0	/26	–
10.0.0.64	/26	–
10.0.0.128	/28	10.0.0.2 (R3)
default	–	10.0.0.65 (R1)

R3

DESTINO	MÁSCARA	SIGUIENTE
10.0.0.128	/28	–
10.0.0.0	/26	–
10.0.0.64	/26	10.0.0.1 (R2) X → se podría eliminar
default	–	10.0.0.1 (R2)

PC1

DESTINO	MÁSCARA	SIGUIENTE
10.0.0.64	/26	–
default	–	10.0.0.65 (R1) → default GW

c) - PC1 no ha accedido a "www.ugr.es" previamente ⇒ no tiene entrada en su caché con la IP

- Deberá hacer una consulta DNS a "dns_local"
- Consideramos una consulta DNS sobre UDP ⇒ no hay establecimiento ni cierre de la conexión con el servidor de DNS
- Se consideran mensajes de capa de aplicación y transporte (extremo a extremo). Aunque se mostrarán las traducciones que se harán con NAT en R1.

	IP. ORIGEN	IP DESTINO	PUERTO ORG.	PUERTO DEST.	PROTOCOLO MENSAJE	FLAGS	DATOS
(consulta DNS sobre UDP)	10.10.10.67 (PC1)	10.10.10.130 (DNS_LOCAL)	5000	53	DNS query (UDP)		www.ugr.es
	10.10.10.130 (DNS_LOCAL)	10.10.10.67 (PC1)	53	5000	DNS resp. (UDP)		70.70.70.7
HTTP sobre TCP (Establecim. conexión)	10.10.10.67 (PC1)	70.70.70.7 (www.ugr.es)	4444	80	HTTP/TCP	SYN	
	80.80.80.8 (R1) [NAT]	70.70.70.7 (www.ugr.es)	8008	80	HTTP/TCP	SYN	
	70.70.70.7	80.80.80.8	80	8008	HTTP/TCP	SYN,ACK	
	70.70.70.7	10.10.10.67 (R1)[NAT]	80	4444	HTTP/TCP	SYN,ACK	
	10.10.10.67	70.70.70.7	4444	80	HTTP/TCP	ACK	
	80.80.80.8 (R1) [NAT]	70.70.70.7	8008	80	HTTP/TCP	ACK	
HTTP sobre TCP (petición web y respuesta)	10.10.10.67	70.70.70.7	4444	80	HTTP request (TCP)		GET "index.html"
	80.80.80.8 [NAT]	70.70.70.7	8008	80	HTTP request (TCP)		GET "index.html"
	70.70.70.7	80.80.80.8	80	8008	HTTP response (TCP)	ACK (request)	index.html (*)
	70.70.70.7	10.10.10.67 [NAT]	80	4444	HTTP response (TCP)	ACK (request)	index.html (*)
HTTP sobre TCP (Cierre conexión)	10.10.10.67	70.70.70.7	4444	80	HTTP/TCP	ACK (response) FIN	
	80.80.80.8 [NAT]	70.70.70.7	8008	80	HTTP/TCP	ACK (response) FIN	
	70.70.70.7	80.80.80.8	80	8008	HTTP/TCP	FIN,ACK	
	70.70.70.7	10.10.10.67 [NAT]	80	4444	HTTP/TCP	FIN,ACK	
	10.10.10.67	70.70.70.7	4444	80	HTTP/TCP	ACK	
	80.80.80.8 [NAT]	70.70.70.7	8008	80	HTTP/TCP	ACK	

(*) Suponemos que la web no tiene más objetos (imágenes, vídeos, etc). Si los tuviese, www.ugr.es se los enviaría al PC1 de la misma forma que el fichero "index.html"

PROBLEMA 2 (3 puntos sobre 10)

Suponga dos entidades TCP A **y** B con la siguiente configuración: MSS = 1.250 bytes; la ventana de congestión inicial es de 2.500 bytes; el umbral de congestión está fijado inicialmente a 10.000 bytes. Ambas entidades utilizan TCP Tahoe.

a) **Muestre el diagrama de intercambio de segmentos de TCP** que se produciría para que A envíe un fichero de tamaño 60.000 bytes a B. Calcule el **tiempo requerido total**, considerando que el tiempo de propagación es de 5 ms y la velocidad de transmisión es de 10 Mbps. En el diagrama incluya en cada momento el **valor de la ventana de congestión** y en qué **fase del control de congestión** se encuentra el transmisor. Suponga que la ventana del control de flujo es arbitrariamente grande. **Explique detalladamente su respuesta**.

b) ¿Cuánto sería el **tiempo requerido total si usara UDP**? Explique detalladamente su respuesta.

$MSS = 1250\ B$

$CWIN_0 = \frac{2500\ B}{1250\ B/MSS} = 2\ MSS$

$Umbral = \frac{10\,000\ B}{1250\ B/MSS} = 8\ MSS$

$t_p = 5\ ms$

$V_t = 10\ Mbps$

$t_t = \frac{1250\ B \cdot 8\ b/B}{10 \cdot 10^6\ b/s} = 1\ ms$

$t_t(ACK, SYN, FIN) \simeq 0$

$Fichero = \frac{60\,000\ B}{1250\ B/MSS} = 48\ MSS$

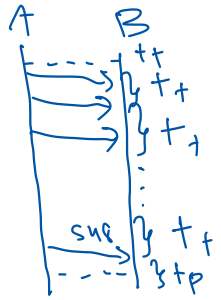
$RTT = 2t_t + 2t_p = 12\ ms$

A partir de cuándo no se producen interrupciones por esperas de ACK's.

$CW \cdot t_t \geq RTT = 2t_t + 2t_p \Rightarrow CW \geq 2 + 2\frac{t_p}{t_t} = 12$

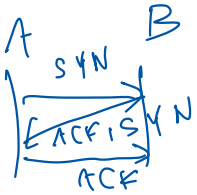
B)

Dado que no se realiza establecimiento de conexión ni se esperan confirmaciones, el tiempo total de transmisión será:

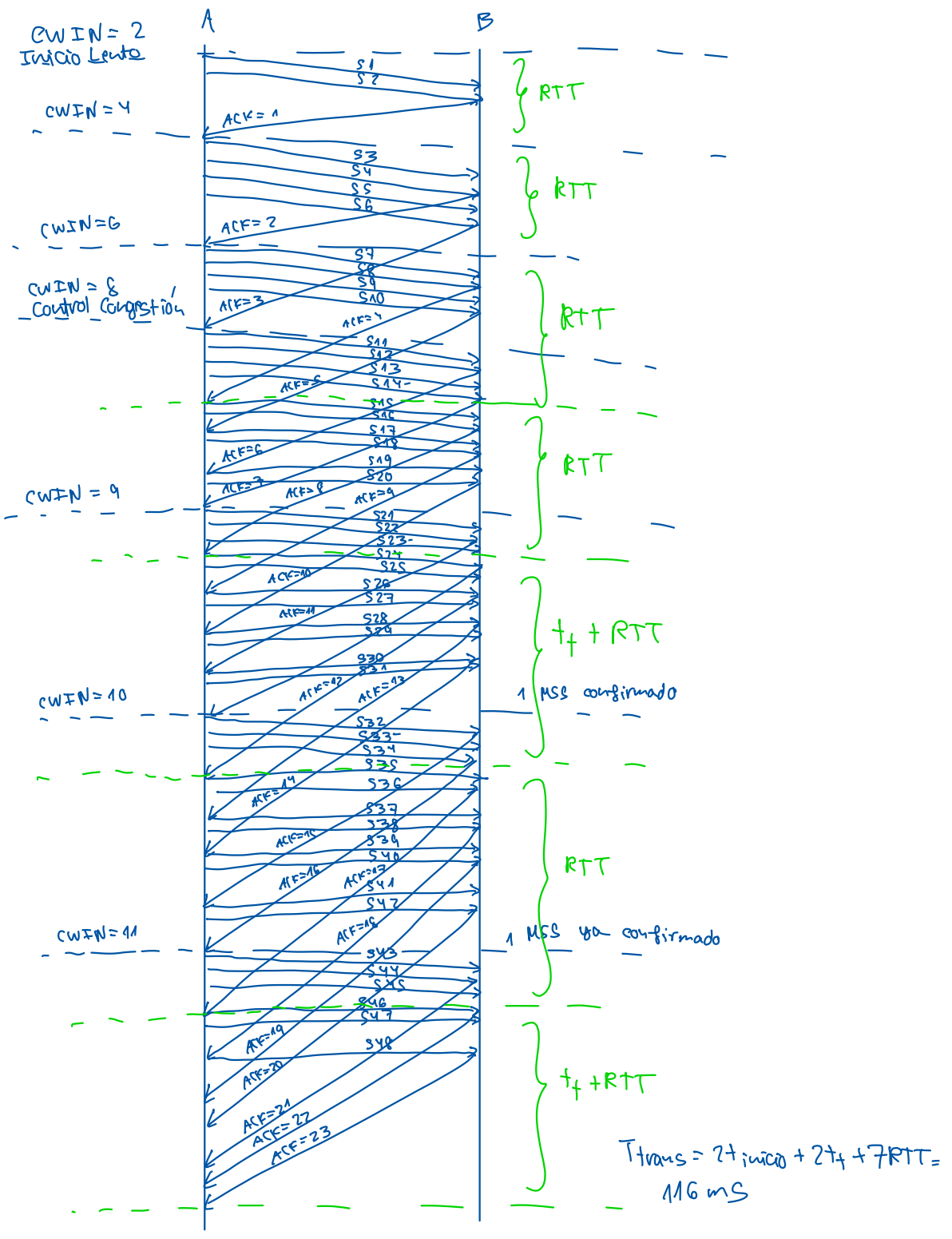


$T_{trans} = t_p + 48\ t_t = 5 + 48 = 53\ ms.$

A)



$t_{inicio} \simeq t_{fin} \simeq 3t_p = 15\ ms$


A
B
CWIN = 2
Inicio Lento
CWIN = 4
CWIN = 6
CWIN = 8
Control Congestión
CWIN = 9
CWIN = 10
CWIN = 11
S1
S2
ACK = 1
S3
S4
S5
S6
ACK = 2
S7
S8
S9
S10
ACK=3
ACK=4
S11
S12
S13
S14
ACK=5
S15
S16
S17
S18
ACK=6
S19
S20
ACK=7
ACK=8
ACK=9
S21
S22
S23
S24
S25
ACK=10
S26
S27
ACK=11
S28
S29
S30
S31
ACK=12
ACK=13
S32
S33
S34
S35
S36
ACK=14
S37
S38
ACK=15
S39
S40
ACK=16
ACK=17
S41
S42
ACK=18
S43
S44
S45
S46
S47
ACK=19
S48
ACK=20
ACK=21
ACK=22
ACK=23
RTT
RTT
RTT
RTT
t_f + RTT
1 MSS confirmado
RTT
1 MSS ya confirmado
t_f + RTT
$T_{trans} = 2t_{inicio} + 2t_f + 7RTT =$
116 ms

Ejercicio 1 enero 2023

DATOS

MSS = 1250 bytes
CWini = 2500 bytes = 2 MSS
Umbral = 10000 bytes = 8 MSS
T_p = 5 ms, U_t = 10 Mbps → $T_t = \frac{1250 \times 8}{10 \cdot 10^6} = 10^{-3}\,s = 1\,ms$
fichero = 60000 bytes = 48 MSS

$RTT = 2 \cdot T_p + 2 \cdot T_t = 12\,ms$

Establecimiento TCP

SYN
SYN+ACK
ACK
} $3T_p = 15\,ms$

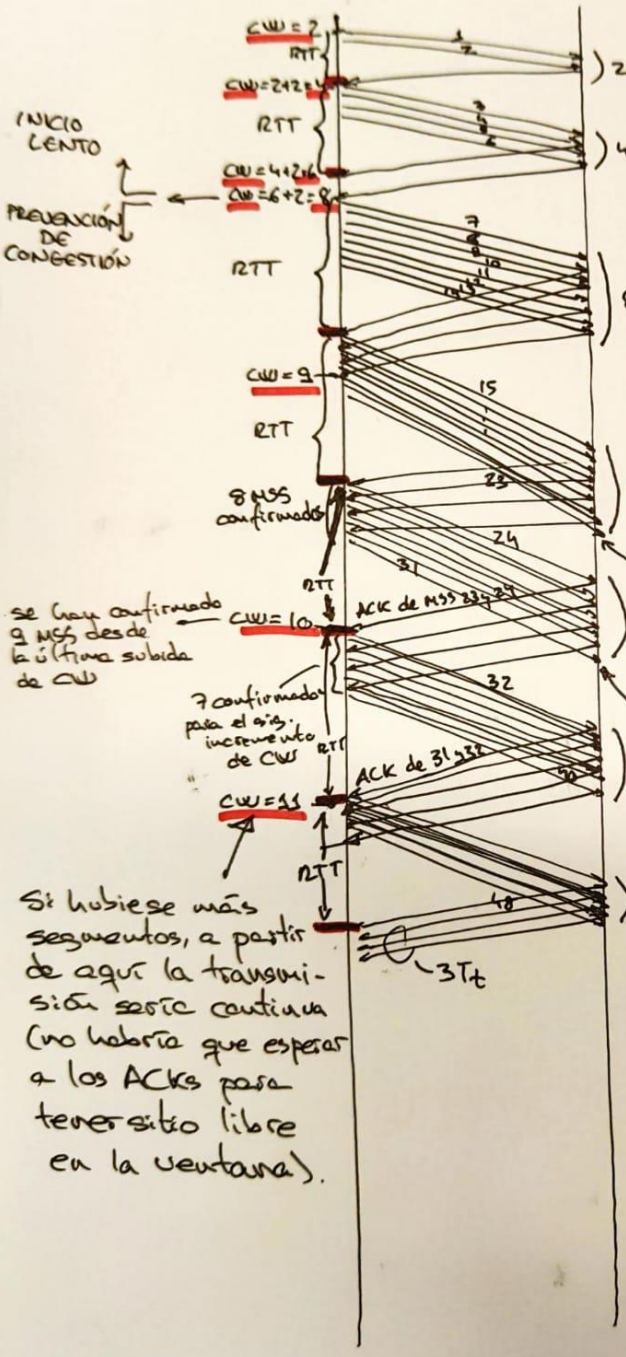
Cierre TCP → igual → 15 ms

¿Cuándo no habría interrupciones por el control de congestión?

$CW \cdot T_t \geq 2T_p + 2T_p$

→ $CW \geq 2 + \frac{2T_p}{T_t} = 12$

A partir de CW = 12 no hay tiempos muertos esperando ACKs.



Este envío de mensajes dura
$7RTT + 3T_t = 87\,ms$.

A eso hay que sumarle el tiempo de establecimiento y cierre de la conexión TCP:

$T_{TOTAL} = 15 + 87 + 15 = 117\,ms$

En el caso de UDP, no hay establecimiento ni cierre, ni control de congestión. Es decir, se mandan todos los paquetes seguidos, por lo que el tiempo total (en recepción, el emisor no recibe confirmaciones) será Tp + 48 * Tt = 5 + 48 = 53 ms.

Contestar las siguientes preguntas usando exclusivamente los huecos reservados.
P1 (1 punto sobre 10) ¿Qué es la congestión en la red? ¿Dónde se origina?

La congestión en la red se origina en los routers y produce por el desbordamiento de los buffers de los mismos. Si llegan demasiados paquetes para que puedan ser servidos (e.g. porque la capacidad de procesamiento no sea elevada, o porque los interfaces de salida no sean lo suficientemente rápidos para reenviar todos los paquetes entrantes), los buffers donde se guardan antes de ser encaminados se van llenando hasta que se desbordan, provocando que no lleguen a su destino. Los protocolos de transporte fiables como TCP tienen mecanismos para reducir la velocidad cuando detectan que hay congestión (e.g. por pérdidas de ACKs en el caso de TCP Tahoe).

P2 (1.5 puntos sobre 10).

a) Explique los mensajes que se generarían en la resolución del dominio **www.ejemplo.jp** con el protocolo DNS suponiendo que **.jp** ha delegado la autoridad a **.ejemplo**.
b) ¿Qué significa ser la autoridad de una zona?
c) ¿Qué significa delegar la autoridad?

a) El cliente DNS tiene configurado la IP de su DNS local (DNS1), al que le mandaría un DNS query preguntando por la IP de www.ejemplo.jp. Suponiendo que no tiene esa información (ni en su base de datos ni en su caché) y que la resolución es recursiva (también sería válido explicar la solución con resolución iterativa), el DNS local reenvía la DNS query a un DNS raíz (DNS2). Este, a su vez, reenvía la petición al DNS responsable del dominio jp (DNS3). Como este delegó la autoridad de ejemplo.jp a otro DNS, le reenvía a este último la solicitud (DNS4). DNS4 tiene la información en su base de datos (es autoridad de esa zona), por lo que envía un DNS query response con la respuesta (la IP de www.ejemplo.jp) a DNS3, este a DNS2, este a DNS1 y este, finalmente, al cliente DNS.

b) Un servidor con autoridad (SOA, Start of Authority) es un servidor al que le han delegado la responsabilidad de una zona (conjunto de nombres de dominio consecutivos) y tiene toda la información de su zona en su base de datos (no en su caché).

c) Un servidor DNS con autoridad en una zona (conjunto de nombres de dominio consecutivos) puede ceder la autoridad de una subzona a otro servidor DNS, que se convertirá en autoridad de dicha subzona.

P3 (1,5 puntos sobre 10). Explique y justifique todas las propiedades (o aspectos) de seguridad que se garantizan si para enviar el mensaje T, una entidad A envía a B:

$$DES\_{K\text{-}SECRETA}\,[\ K_{PRI\_A}(\,MD5\,(\,T\,)\,) + T\,]\ + K_{PUB\_B}(\,K\text{-}SECRETA\,)$$

Siendo

K-SECRETA una clave secreta
K_{PUB_B} ( ) el cifrado usando la clave pública de B
MD5 ( ) una función hash o compendio.
K_{PRI_A} ( ) el cifrado usando la clave privada de A
$DES\_{K\text{-}SECRETA}$ [ ] el cifrado usando DES con la clave K-SECRETA
+ concatenar o unir

El mensaje T incluye varias partes:

- Envío de una clave secreta K-SECRETA cifrando con la clave pública del receptor K_{PUB_B}. Como solo puede descifrar B (es el único que conoce su clave privada), se está distribuyendo esta clave secreta con confidencialidad. No se manda un resumen o compendio de esta parte con alguna función hash, por lo que no se consigue integridad en dicha parte. Tampoco se consigue no repudio (no hay ninguna prueba de que A ha mandado esta parte, o que B la ha recibido).

- La primera parte incluye el texto a mandar T cifrado con DES y usando la clave secreta explicada en el punto anterior K-SECRETA. Además del texto, se manda un resumen (MD5(T)) y el texto nuevamente, todo cifrado con la clave privada del emisor. Esto da 1) integridad (gracias al resumen, ya que podemos comprobar si se ha modificado el texto o no) y 2) autenticación (ya que solo puede haberlo cifrado A, y B puede descifrarlo con la clave pública de A). No se garantiza no repudio porque no se indica que haya una entidad fiable que garantice la asociación entre la identidad y su clave pública (i.e. el equivalente a un certificado digital).

En términos generales, como necesitamos la clave secreta para descifrar la primera parte y ahí tenemos un resumen que nos permite asegurarnos de la integridad del texto T, indirectamente nos sirve como integridad de la clave secreta. Es decir, si comprobamos la integridad del texto T, necesariamente la clave secreta cifrada con la clave pública de B tiene que estar bien, porque si no, no podríamos descifrar la primera parte y no funcionaría la comprobación de la integridad de T.

Resumen: este mensaje consigue enviar una clave secreta con confidencialidad (e indirectamente con integridad), y un texto con confidencialidad, autenticación e integridad.