Universidad de Granada
Departamento de Teoría de la Señal,
Telemática y Comunicaciones

FUNDAMENTOS DE REDES. Examen de teoría – Febrero 2017

Apellidos y nombre: _____ **Grupo:**_____

1. *(0,75 ptos)* Describa los mensajes generados desde un equipo correctamente configurado para acceder a Internet desde que solicita una URL en el navegador hasta que se muestra la página web completa.

2. *(0,75 ptos)* Suponga que A y B tienen sus correspondientes K_{PUB_A}/K_{PRIV_A} y K_{PUB_B}/K_{PRIV_B} y una autoridad tiene sus K_{PUB_AUT}/K_{PRIV_AUT}. Explique cómo y qué primitivas se cumplirían en una comunicación segura entre A y B usando dichas claves.

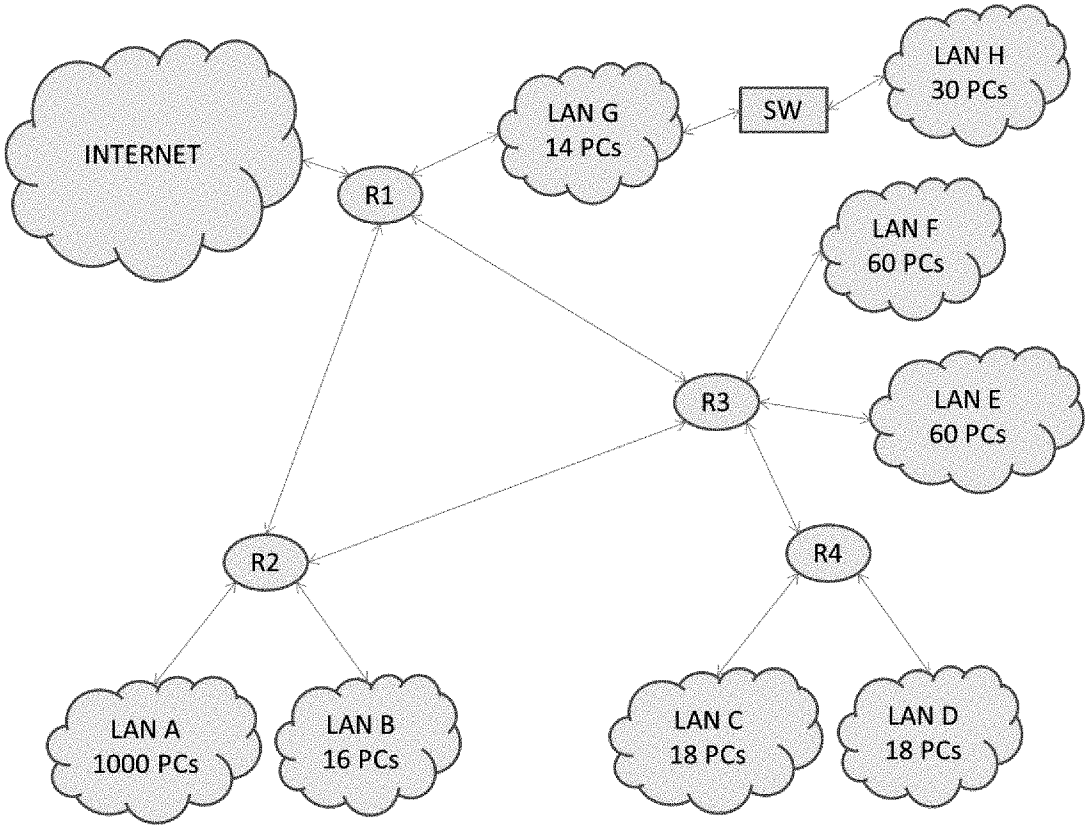
3. *(0,75 ptos)* Se tiene un paquete de 5KB de los que 14 bytes son de cabecera de nivel de Ethernet, 20 de nivel IP y 8 de nivel UDP. Este paquete debe pasar por una red Ethernet con una MTU de 1514Bytes. Si se precisa su fragmentación ¿Cuántos paquetes se generarían y con qué tamaños?

4. *(0,75 ptos)* Indentifique los niveles del modelo OSI y explique brevemente la funcionalidad de cada nivel

5. *(1 pto)* Una conexión *TCP Tahoe* que se encuentra en el estado de prevención de la congestión tiene una ventana de congestión de 50KB, un tamaño de MSS de 1KB y un tiempo de RTT de 100ms. Suponga que en este punto, se detecta un paquete perdido.

- ¿Cómo cambiaran los valores de ventana de congestión y umbral de congestión?
- ¿Cuánto tiempo transcurrirá antes de que el emisor vuelva al estado de prevención de la congestión?
- Asumiendo que no se pierde ningún otro paquete hasta que la ventana de congestión no exceda de nuevo los 50KB ¿Cuánto tiempo se permanecerá en el estado de prevención de la congestión?

6. *(1 pto)* En la red mostrada en el gráfico siguiente, asigne direcciones privadas y especifique la tabla de encaminamiento para todos los *routers* de forma tal que se minimicen el número de entradas en las mismas.



Solución:

1. El dispositivo origen de la conexión manda los siguiente mensajes:

i) Solicitud DNS para obtener la IP de destino a partir del nombre de dominio.

ii) Inicio de conexión TCP (*3-way handshake*)

- Primer segmento sólo cabeceras con flag SYN
- Segmento ACK ante la recepción de SYN(+ACK) del otro par

iii) Solicitudes HTTP:

- Paquete HTTP con la solicitud GET de la página
- Iterativas solicitudes en este u otros flujos TCP (iniciados según ii)) de los objetos incrustados en la página

2. Organizaré la respuesta a partir de las primitivas:

- Confidencialidad: Típicamente, se utiliza la criptografía simétrica para encriptar el tráfico. La criptografía asimétrica se usa para negociar la clave simétrica. Así, en dicha negociación cada par usa la clave pública del otro par para encriptar la información.
- Responsabilidad / Autenticación: La clave pública de cada par es asociada a su identidad, típicamente en un certificado, firmado con la clave privada (K_{PRIV_AUT}) de una autoridad certificadora.
- Integridad: Para evitar la modificación de los mensajes no autorizada, cada par firma un resumen (Message Autentication Code o MAC) con su clave privada, permitiendo que el otro par compruebe la integridad del mensaje con su la pública del firmador.

3.

NOTA ACLARATORIA: Se suele expresar la MTU como el tamaño máximo de Protocol Data Unit (PDU) de la capa de red, es decir, el tamaño máximo desde la cabecera IP, inclusive, hasta el *payload*. Considerando que la MTU de Ethernet es 1500 B, este enunciado es confuso y parece que la cabecera Ethernet (14B) está incluida en la MTU.

La fragmentación ocurre en capa IP, por lo que es necesario fragmentar la SDU del datagrama, es decir, todo lo que queda tras la cabecera IP, por tanto:

$$SDU = 5 \cdot 1024\ B - (14 + 20)\ B = 5086\ B$$

Cada datagrama tiene espacio para: 1480 B

Finalmente, tendremos 3 datagramas de $1480 + 20 + 14 = 1514$ B y un datagrama de $646 + 20 + 14 = 680$ B

4.

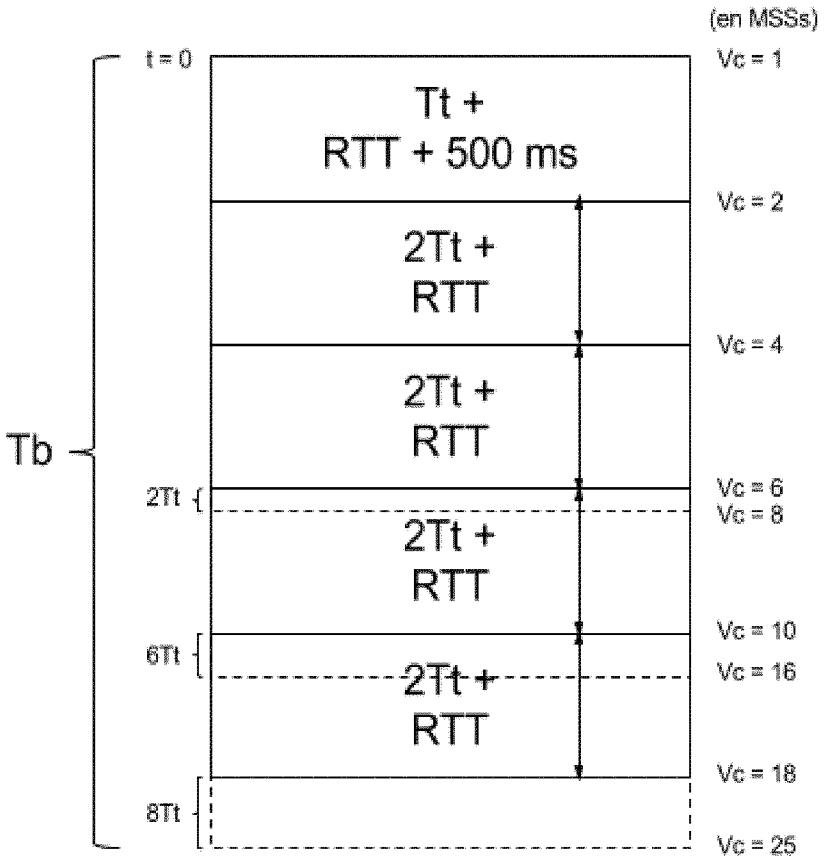
Aplicación: Funcionalidades de las aplicaciones

Presentación: Representación de datos (Traducción desde datos red a SO)

Sesión: Turno de palabra

Transporte: Control de Errores y Flujo entre finales, Multiplexación de aplicaciones

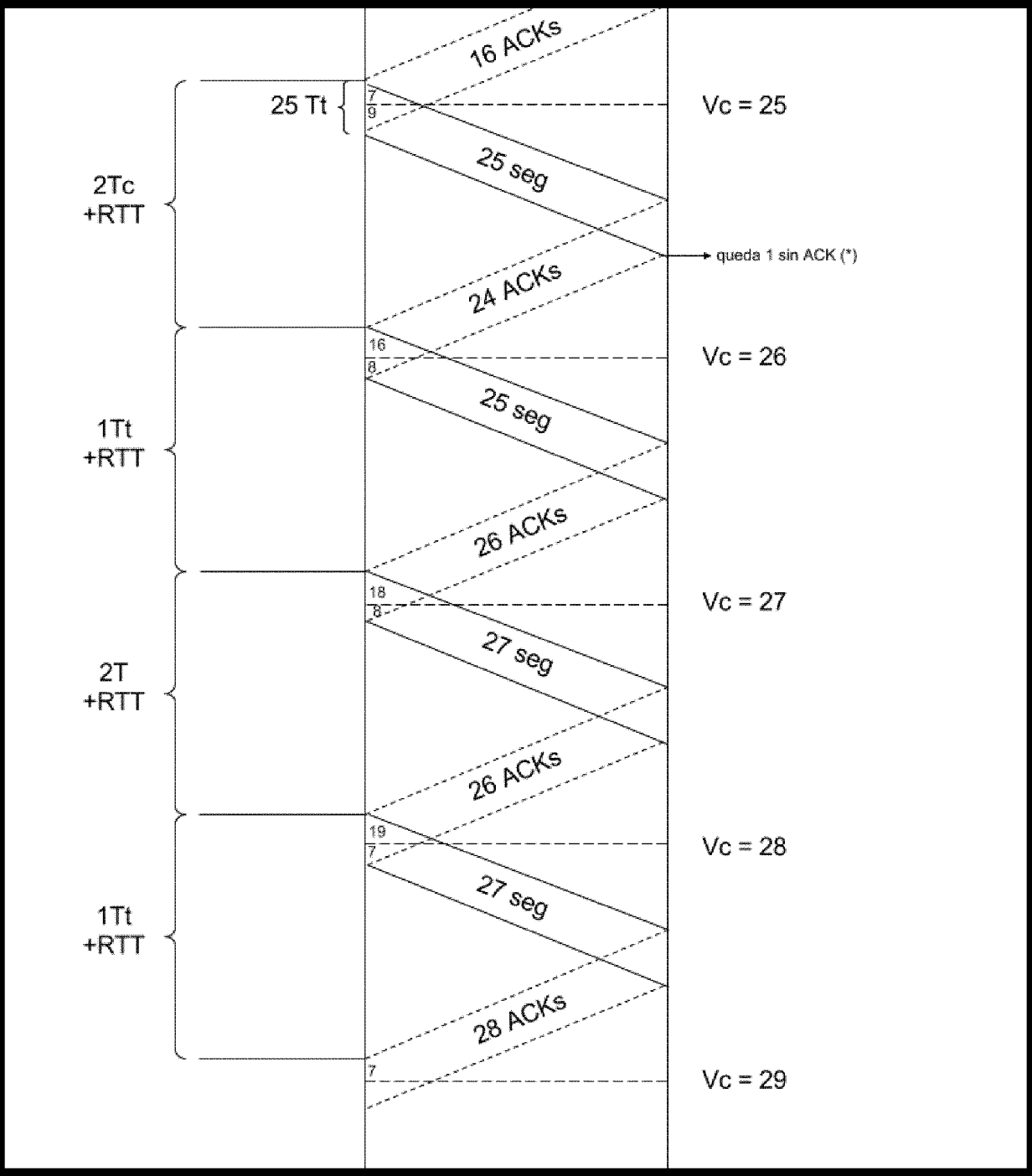
Red: Enrutamiento y Control de Congestión



$$T_t = \frac{1\,kB}{V_t} = \frac{1024 \cdot 8\,b}{10^7\,bps} = 0{,}82\,ms$$

$$T_b = 5\,RTT + 17\,t_t + 500\,ms = 1014\,ms \approx 1\,seg$$

$$t_c \approx (50-25)\cdot(1{,}5\,T_t + RTT) \approx 25\,RTTs = 2{,}5\,s$$



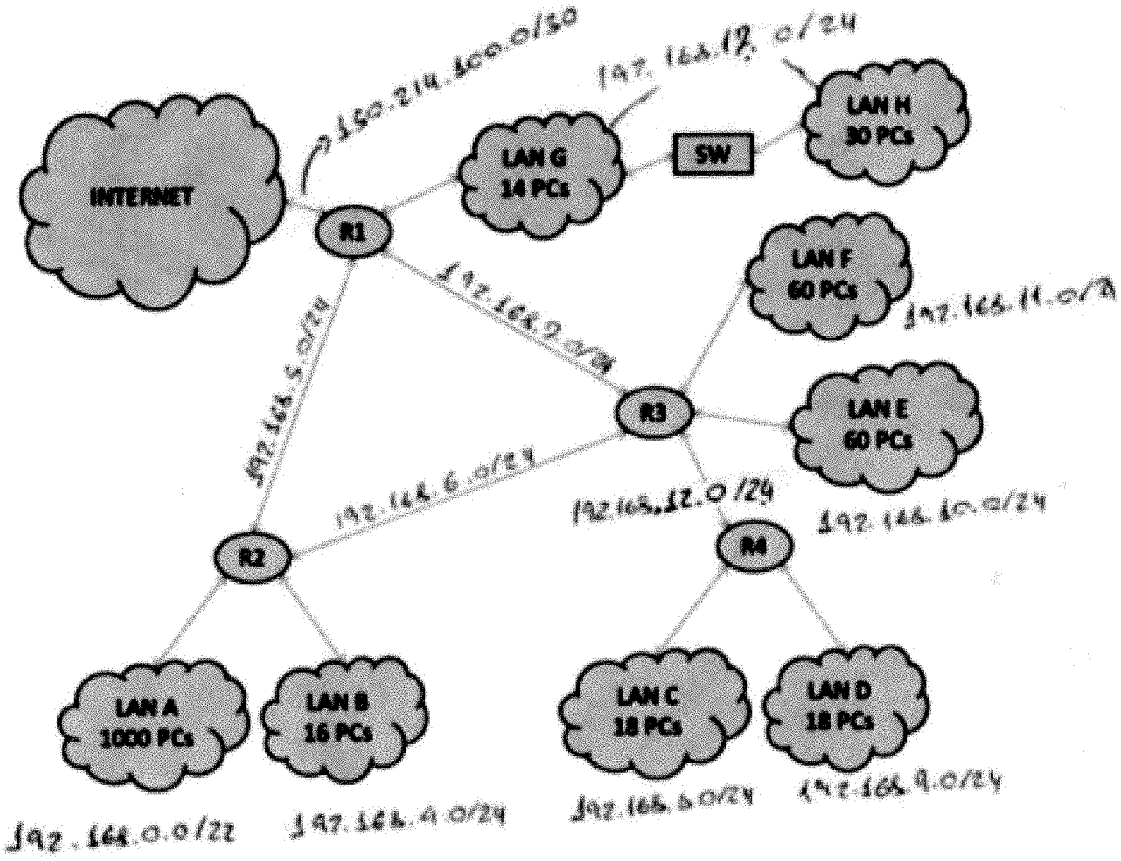
6. La idea para hacer esto es que las direcciones debajo de cada router sean agregables. Como vamos a usar direcciones privadas, por simplicidad usaremos direcciones /24 donde podamos, y /22 en la LAN 1 (esto es sólo una posible solución, hay infinitas pero es importante que el número de entradas en las tablas de encaminamiento sea el mismo). Las direcciones se han dibujado en el gráfico (sig. pag). Las tablas son:

R1	**DD**	**MR**	**SN**
	192.168.17.0	/24	-
	192.168.5.0	/24	-
	192.168.7.0	/24	-
	150.214.100.0	/30	-
	0.0.0.0	/0	150.214.100.1 (ISP)
	192.168.0.0	/21	192.168.5.2 (R2)
	192.168.8.0	/21	192.168.7.2 (R3)

R2	**DD**	**MR**	**SN**
	192.168.5.0	/24	-
	192.168.6.0	/24	-
	192.168.0.0	/22	-
	192.168.4.0	/24	-
	0.0.0.0	/0	192.168.5.1 (R1)
	192.168.8.0	/21	192.168.6.2 (R3)

R3	**DD**	**MR**	**SN**
	192.168.6.0	/24	-
	192.168.7.0	/24	-
	192.168.11.0	/24	-
	192.168.10.0	/24	-
	192.168.12.0	/24	-
	0.0.0.0	/0	192.168.7.1 (R1)
	192.168.0.0	/20	192.168.6.1 (R2)
	192.168.8.0	/23	192.168.12.2 (R4)

R4	**DD**	**MR**	**SN**
	192.168.12.0	/24	-
	192.168.8.0	/24	-
	192.168.9.0	/24	-
	0.0.0.0	/0	192.168.12.1 (R3)


INTERNET
150.214.200.0/30
R1
LAN G
14 PCs
197.168.12.0/24
SW
LAN H
30 PCs
LAN F
60 PCs
197.168.11.0/24
192.168.2.0/24
192.168.5.0/24
R3
LAN E
60 PCs
192.168.10.0/24
192.168.6.0/24
192.168.12.0/24
R2
R4
LAN A
1000 PCs
LAN B
16 PCs
LAN C
18 PCs
LAN D
18 PCs
192.168.0.0/22
192.168.4.0/24
192.168.8.0/24
192.168.9.0/24