EJERCICIO DE SEGURIDAD

Suponga una transacción comercial en Internet con cuatro entidades involucradas: C (cliente), P (proveedor), Bc (entidad bancaria del cliente) y Bp (entidad bancaria del proveedor). Entre ellas se intercambian los mensajes indicados abajo a la derecha; donde Kpb_X se refiere al cifrado con la clave pública de *X*, K_{X-Y} al cifrado con la clave privada entre *X* e *Y*, *producto* a la identificación del producto adquirido/vendido, *importe* a su valor económico, *R* a un reto, *C, P, Bc* y *Bp* a la identidad de las entidades correspondientes y *datos_X* a la información bancaria correspondiente a *X-Bx*.

Aceptadas la disponibilidad y validez de las claves públicas involucradas gracias a la existencia de una entidad superior confiable (es decir, al uso de certificados digitales), responda justificadamente a las siguientes cuestiones:

a) ¿Qué servicios de seguridad se proporcionan en la transacción indicada?

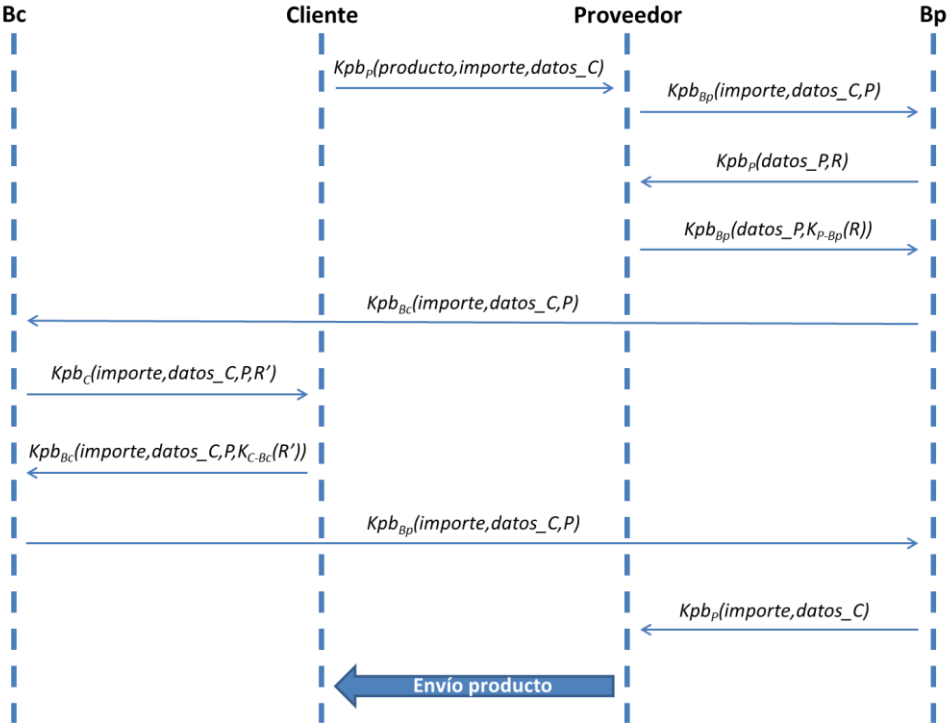
b) ¿Qué debilidades/vulnerabilidades presenta el esquema propuesto y, en su caso, cómo podrían solucionarse?

C→P: $Kpb_P(producto,importe,datos\_C)$
P→Bp: $Kpb_{Bp}(importe,datos\_C,P)$
Bp→P: $Kpb_P(datos\_P,R)$
P→Bp: $Kpb_{Bp}(datos\_P,K_{P-Bp}(R))$
Bp→Bc: $Kpb_{Bc}(importe,datos\_C,P)$
Bc→C: $Kpb_C(importe,datos\_C,P,R')$
C→Bc: $Kpb_{Bc}(importe,datos\_C,P,K_{C-Bc}(R'))$
Bc→Bp: $Kpb_{Bp}(importe,datos\_C,P)$
Bp→P: $Kpb_P(importe,datos\_C)$
P→C: *…entrega del producto…*

MENSAJES:

- ***Kpb$_X$*** → cifrado con la clave pública de *X*
- ***K$_{X-Y}$*** → cifrado con la clave privada entre *X* e *Y*
- ***producto*** → identificación del producto adquirido/vendido
- ***importe*** → valor económico de un producto
- ***R*** → reto
- ***datos_X*** → información bancaria correspondiente a X-Bx

EL PROTOCOLO SERÍA:



a) ¿Qué servicios de seguridad se proporcionan en la transacción indicada?

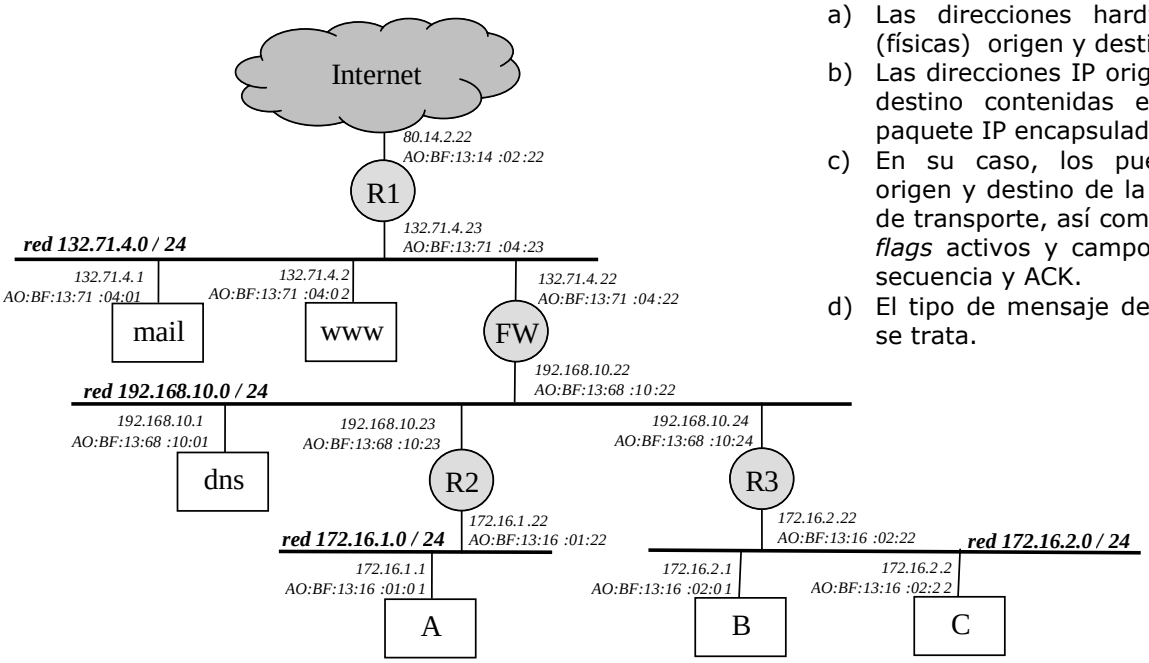
- **Confidencialidad** → sí, ya que todos los mensajes están cifrados con clave pública, por tanto sólo el dueño de la clave privada puede obtener su contenido.
- **Integridad** → no, ya que no se usa firma digital (ni usando compendios ni con doble cifrado).
- **Autenticación** → sólo el cliente/proveedor con sus bancos respectivos, mediante el envío cifrado del reto propuesto (R y R'). Sin embargo, los bancos no se autentican entre ellos ni con sus clientes.
- **No repudio** → no, ya que el cliente no tiene ninguna prueba de que el proveedor haya aceptado la transacción que implica cierto producto y su importe. Ni siquiera de que haya realizado el pago, ya que su banco no le envía la confirmación de la operación con algún campo que sólo hubiese podido incluir él.
- **Disponibilidad** → no, ya que la red podría dejar de funcionar en cualquier momento, por ataques en capas inferiores o por fallos de la misma.

b) ¿Qué debilidades/vulnerabilidades presenta el esquema propuesto y, en su caso, cómo podrían solucionarse?

- **Integridad** → se podría usar una función compendio (hash) para comprobar la integridad de los datos.
- **Autenticación** → podría haber autenticación entre los bancos el cliente/proveedor mediante un reto propuesto por C a Bc y por P a Bp. También podría haber autenticación entre los bancos proponiéndose un reto cada uno.
- **No repudio** → tanto cliente como proveedor podrían firmar digitalmente sus mensajes antes de transmitirlos (con su clave privada) y el receptor del mensaje lo desencriptaría con la clave pública correspondiente. Igualmente, el banco podría mandar una confirmación de la operación realizada firmada digitalmente con su clave privada.
- **Disponibilidad** → el enunciado no da información que permita indicar si hay problemas de disponibilidad (e.g. redundancia de conexiones, posibles problemas ante ataques en capas inferiores, etcétera).

EJERCICIO DE TRÁFICO GENERADO Y CAMPOS EN LOS PAQUETES

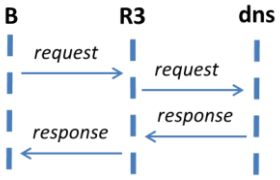
Dada la topología adjunta correspondiente a una red corporativa, en la que se especifican tanto las direcciones IP como las MAC de cada uno de los dispositivos que la forman, analice el tráfico generado al hacer un acceso de correo electrónico desde el *host* "B" al servidor "mail", especificando en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

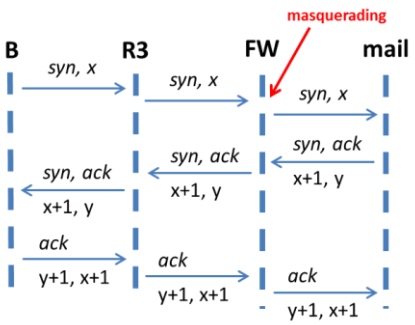


Es una **petición sobre UDP** → no hay establecimiento de conexión previo

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

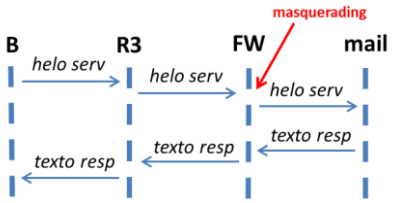
ETH ORI.	ETH DES.	IP ORI.	IP DEST.	PORT ORI.	PORT. DES.	FLAGS	MENSAJE	COMENTARIOS
02:01 (B)	02:22 (R3)	172.16.2.1 (B)	132.71.4.1 (mail)	(1*)	25	SYN x (3*)	Solicitud estab. TCP a mail	A través de R3
10:24 (R3)	10:22 (FW)	172.16.2.1 (B)	132.71.4.1 (mail)	(1*)	25	SYN x (3*)	Solicitud estab. TCP a mail	Retransmisión 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.



… Se podrían enviar más mensajes

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)	(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)	25	(2*)	ACK x+1+NB(helo) y+1	texto respuesta servidor	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

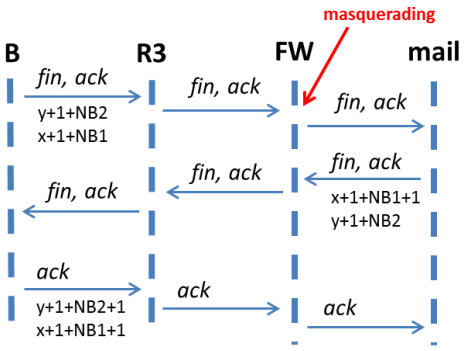
4) PASO 4: Cierre de la conexión TCP

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 ***



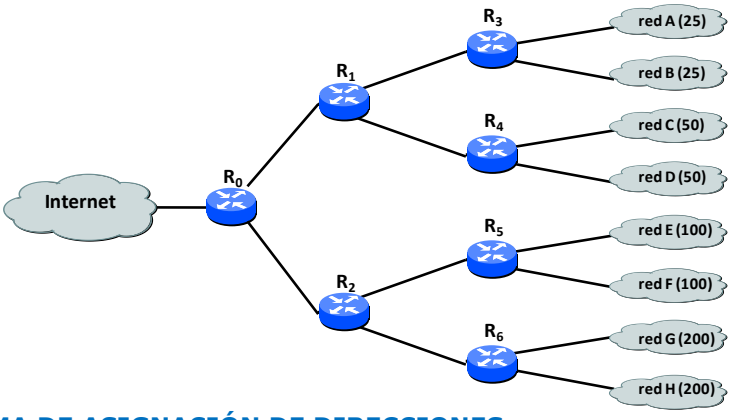
EJERCICIO DE ASIGNACIÓN DE DIRECCIONAMIENTO Y ENCAMINAMIENTO IP

Se dispone de una red con la siguiente topología. Cada una de las redes finales (redes A…H) está compuesta por el número de *hosts* indicado entre paréntesis. Además, se ha contratado el rango de direcciones públicas 168.168.168.0/22.

a) Proponga un **esquema de asignación de direcciones** (de todos los equipos) que cumpla los siguientes requisitos:
   - Todos los *hosts* han de tener asignadas direcciones públicas.
   - La asignación de direcciones ha de minimizar el tamaño de las tablas de encaminamiento.

b) Muestre las **tablas de encaminamiento** de todos los *routers*, suponiendo que se utiliza el esquema de asignación de direcciones del apartado anterior.

***NOTA**: El router R0 tiene una IP pública diferente en su interfaz hacia Internet, e.g. 33.33.33.33/24.*



A) ESQUEMA DE ASIGNACIÓN DE DIRECCIONES

- Para minimizar las tablas de encaminamiento interesa que las subredes conectadas a un mismo router se puedan agrupar mediante máscaras de subred/superred.
- Hay 8 subredes identificadas, más las subredes entre los routers (otras 6). Centrándonos en las señaladas en la figura (A, B, …, H) hay algunas pequeñas y otras grandes. Si se hicieran todas las redes del mismo tamaño, no habría suficientes direcciones IP para asignar.

Máscara /22 ➔ $2^{(32-22)}= 2^{10}$ = 1024 direcciones (incluyendo red y difusión, así como todas las interfaces de los routers).

La red más grande es de 200 equipos + 3 direcciones ➔ necesitaría al menos máscara /24 ⇔ 256 direcciones.
8 subredes x 256 direcciones = 2048 direcciones necesarias ➔ NO TENEMOS SUFICIENTES DIRECCIONES

- Habrá que asignar las máscaras de subred en función del número de equipos de cada una de ellas.

Consideramos la red más pequeña (RED A):
- Tiene 25 equipos + 2 IPs reservadas (red y difusión) + IP router R3 ➔ 28 direcciones IP
- Necesitaría 5 bits mínimo (con 4 bits no tendría suficientes) ➔ 2^5 = 32
- 5 bits ⇔ máscara /27 (32 bits de la dirección IP completa – 5 bits para hosts/interfaces)

- Para poder agrupar las rutas, asignaremos subredes /27.

Ordenamos las redes de mayor a menor tamaño y vamos asignando direcciones. Se comienza de mayor a menor para evitar problemas al asignar direcciones consecutivas a las subredes, es decir, que utilicemos subredes con bits a 1 en la parte de equipo (algo que sería una definición incorrecta de subred).

RED H (200 equipos):

Disponemos de 168.168.168.0/22 ⇔
10101000.10101000.101010|00.00000000 (disponemos de 10 bits para direcciones IP)

- Se necesitarían las subredes:
  …00.000|00000/27 [168.168.168.0/27]
  a
  …00.110|00000/27 [168.168.168.192/27]

  Cada una tiene 32 IPs (5 bits) x 7 subredes = 224 direcciones IP

- Pero para agrupar de manera más sencilla (en una única subred) se asignarán las subredes:
  …00.000|00000/27 [168.168.168.0/27]
  …00.001|00000/27 [168.168.168.32/27]
  …00.010|00000/27 [168.168.168.64/27]
  a
  …00.111|00000/27 [168.168.168.224/27]

  Agrupar:
  …00.|00000000 /24

  *** Para agrupar se buscan los bits iguales en todas las redes, se fija la máscara a ese número y se fijan el resto de bits a 0. ***

  Se agruparían como la subred …00.|00000000/24 [168.168.168.0/24]

RED G (200 equipos):
- Se asignarían las subredes:
  …01.000|00000/27 [168.168.169.0/27]
  a
  …01.111|00000/27 [168.168.169.224/27]

  Se agruparían como la subred …01.|00000000/24 [168.168.169.0/24]

- **G y H se agruparían en la subred …0|0.00000000/23 [168.168.168.0/23]**
  Que sería la única entrada en la tabla del router R_2 hacia estas redes (a través de R_6).

NOTA: Estas redes ya no podrían agruparse con E y F a nivel de R_0, ya que el siguiente

nivel de agrupamiento (/22) define todas las direcciones disponibles en la red completa (para todas las subredes), según el rango de direcciones de que se dispone.

RED F (100 equipos):

- Se asignarían las subredes:
  …10.000|00000/27 [168.168.170.0/27]
  a
  …10.011|00000/27 [168.168.170.96/27]

  Cada una tiene 32 IPs (5 bits) x 4 subredes = 128 direcciones IP

  Se agruparían como la subred …10.0|00000000/25 [168.168.170.0/25]

RED E (100 equipos):

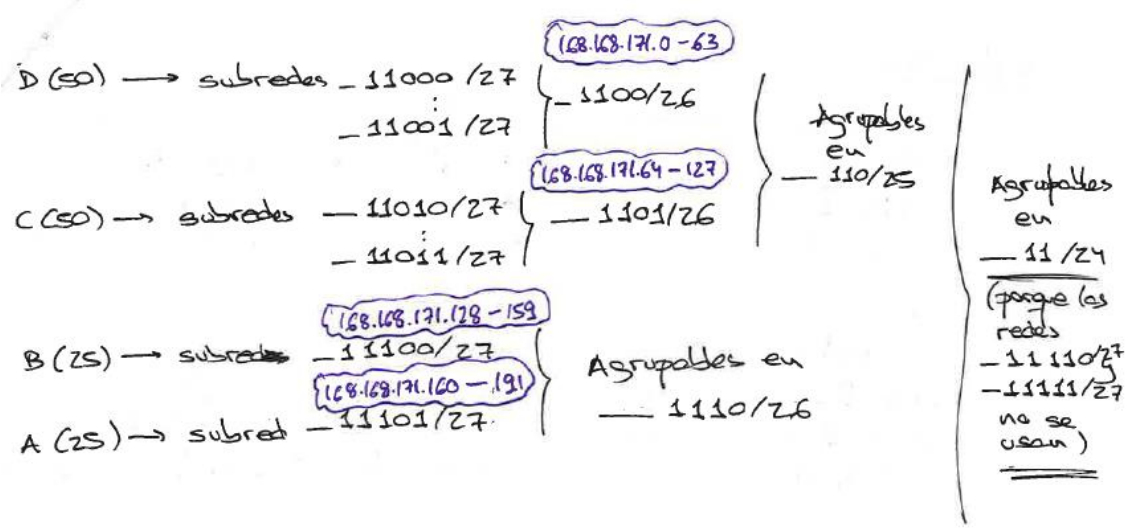
- Se asignarían las subredes:
  …10.100|00000/27 [168.168.170.128/27]
  a
  …10.111|00000/27 [168.168.170.224/27]

  Se agruparían como la subred …10.1|00000000/25 [168.168.170.128/25]

- **E y F se agruparían en la subred …10.|00000000/24 [168.168.170.0/24]**
  Que sería la única entrada en la tabla del router R_2 hacia estas redes (a través de R_5).

Las redes D, C, B y A se asignarían y agruparían de la siguiente forma:

*** Considere que sólo se muestran los bits de subred (a la derecha habría 5 bits más para equipos, al ser /27) ***



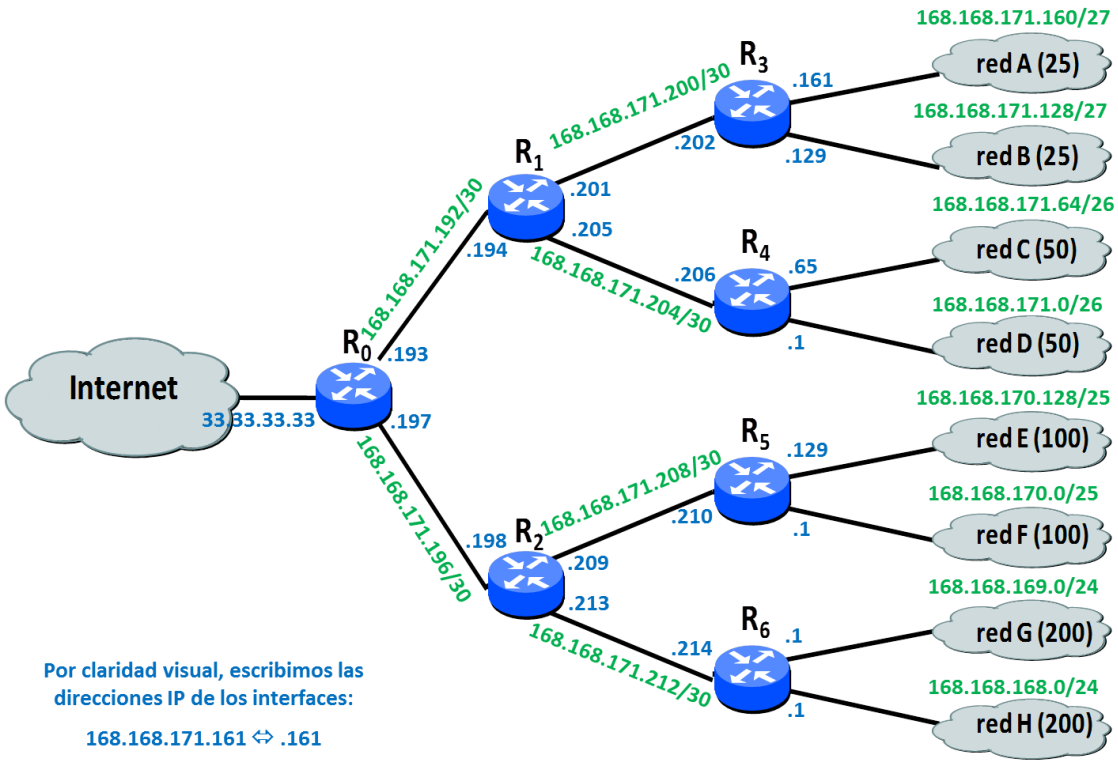
Como la última subred asignada (a la red A) es 168.168.171.160/27, cuya última dirección es 168.168.171.191, usamos las direcciones siguientes para las redes entre routers. Estas redes necesitan 4 direcciones (subred, difusión, router X y router Y), por lo que utilizarán una máscara /30. Una posible asignación sería la siguiente:

- Subred R_0-R_1: 168.168.171.192/30 → direcciones 192 a 195
- Subred R_0-R_2: 168.168.171.196/30 → direcciones 196 a 199
- Subred R_1-R_3: 168.168.171.200/30 → direcciones 200 a 203
- Subred R_1-R_4: 168.168.171.204/30 → direcciones 204 a 207
- Subred R_2-R_5: 168.168.171.208/30 → direcciones 208 a 211
- Subred R_2-R_6: 168.168.171.212/30 → direcciones 212 a 215

Sobrarían las direcciones 168.168.171.216 a 168.168.171.255.

La asignación de direcciones IP sería:

*** Asignando las primeras IPs del rango de cada subred al/los router/routers que haya en dicha subred ***



B) TABLAS DE ENCAMINAMIENTO

ROUTER R_0

Destino	Máscara	Sig. Salto (interfaz)	
168.168.168.0	/23	R_2 (168.168.171.198)	Hacia redes G y H
168.168.170.0	/24	R_2 (168.168.171.198)	Hacia redes E y F
168.168.171.0	/24	R_1 (168.168.171.194)	Hacia redes A, B, C y D
168.168.171.192	/30	*	Conexión directa (subred R_0-R_1)
168.168.171.196	/30	*	Conexión directa (subred R_0-R_2)
default	-	IP Gateway ISP	Hacia Internet

ROUTER R_1

Destino	Máscara	Sig. Salto (interfaz)	
168.168.171.0	/25	R_4 (168.168.171.206)	Hacia redes C y D
168.168.171.128	/25	R_3 (168.168.171.202)	Hacia redes A y B
168.168.171.200	/30	*	Conexión directa
168.168.171.204	/30	*	Conexión directa
default	-	R_0 (168.168.171.193)	Hacia Internet y otras subredes

ROUTER R_2

Destino	Máscara	Sig. Salto (interfaz)	
168.168.168.0	/23	R_6 (168.168.171.214)	Hacia redes G y H
168.168.170.0	/24	R_5 (168.168.171.210)	Hacia redes E y F
168.168.171.208	Máscara	*	Conexión directa
168.168.171.212	Máscara	*	Conexión directa
default	-	R_0 (168.168.171.197)	Hacia Internet y otras subredes

ROUTER R_3

Destino	Máscara	Sig. Salto (interfaz)	
168.168.171.160	/27	*	Hacia red A
168.168.171.128	/27	*	Hacia red B
default	-	R_1 (168.168.171.201)	Hacia Internet y otras subredes

ROUTER R_4

Destino	Máscara	Sig. Salto (interfaz)	
168.168.171.64	/26	*	Hacia red C
168.168.171.0	/26	*	Hacia red D
default	-	R_1 (168.168.171.205)	Hacia Internet y otras subredes

ROUTER R_5

Destino	Máscara	Sig. Salto (interfaz)	
168.168.170.128	/25	*	Hacia red E
168.168.170.0	/25	*	Hacia red F
default	-	R_2 (168.168.171.209)	Hacia Internet y otras subredes

ROUTER R_6

Destino	Máscara	Sig. Salto (interfaz)	
168.168.169.0	/24	*	Hacia red G
168.168.168.0	/24	*	Hacia red H
default	-	R_2 (168.168.171.213)	Hacia Internet y otras subredes

EJERCICIO SOBRE VENTANA DE CONGESTIÓN TCP

Dadas dos entidades TCP (A y B) conectadas por una red cuya velocidad de transmisión es 100 Mbps, suponga segmentos de 1024 bytes y un RTT (Round Trip Time) constante de 2 mseg. Si A transmite masivamente datos a B ¿Cuánto tiempo tardará en transmitir 8 tramas? Incluya el número de secuencia y de acuse en todos los segmentos TCP. Haga las suposiciones que estime necesarias.

TIEMPO EN EL QUE EMPIEZA LA TRANSMISIÓN DEL 8º SEGMENTO

L → Segmento TCP → 1024 bytes
(+20 bytes de cabecera IP + X bytes de cabeceras de otras capas inferiores)

Vt = 100 Mbps
RTT = 2 ms

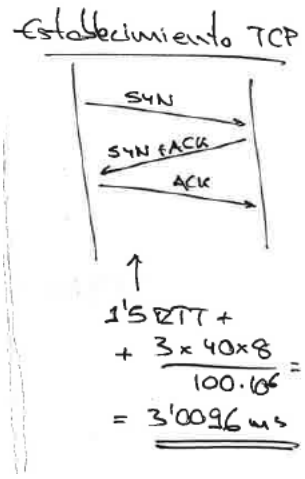
SUPOSICIONES:

- Tiempo ida = Tiempo vuelta (RTT/2)
- Tiempo de generación/procesamiento de tramas/ACK ≈ 0
- Consideramos los tamaños de cabecera de TCP=20 bytes e IP=20 bytes.
- Las cabeceras de capas inferiores no se considerarán en los cálculos.
- Se desprecia el tamaño de las cabeceras y colas de las capas inferiores a IP

- Hay que considerar ***el tiempo de establecimiento de conexión de TCP***
- Hay que considerar ***control de congestión de TCP***
- Supondremos un tamaño de ventana de congestión inicial de 2, ya que será más eficiente (no habría que esperar los 500ms para confirmar el primer segmento en caso de que el tamaño de ventana de congestión fuese 1).

- **Control de flujo**: La ventana ofertada por el receptor será suficiente para recibir todos los segmentos en cada momento.

Establecimiento de conexión:

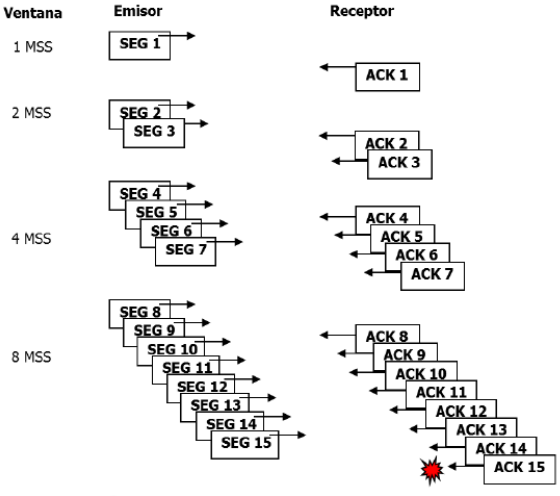


*** 40 es la suma de la cabecera TCP + la cabecera IP (estos mensajes sólo tienen cabecera) ***

Tiempo = L/Vt

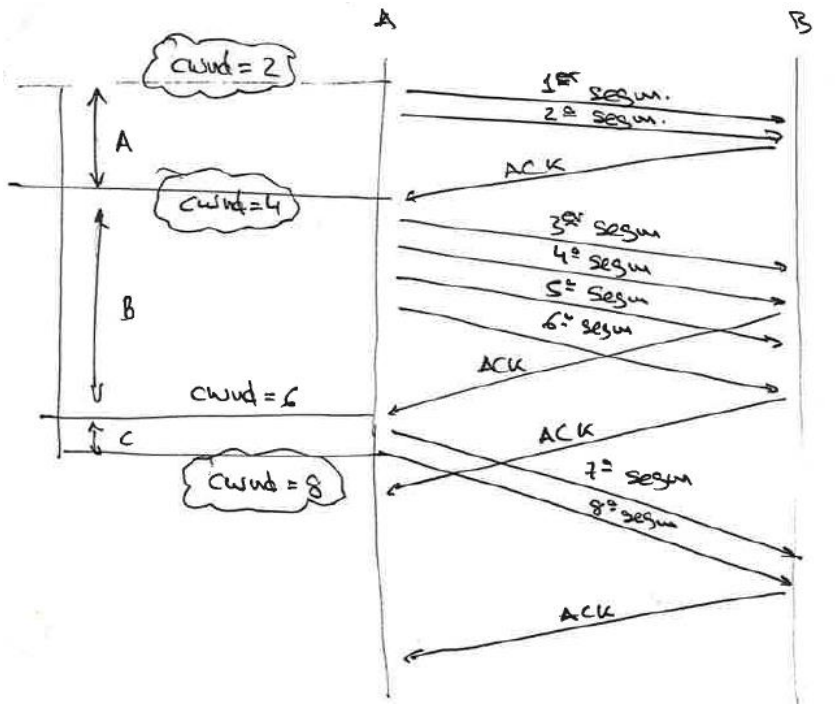
Envío de mensajes considerando el **inicio lento (*slowstart*)** del control de congestión de TCP:

Inicio lento:



*** Inicialmente la ventana de congestión tiene el tamaño de un MSS (Maximum Segment Size) ***

*** Por cada segmento enviado con éxito la ventana se amplía en un MSS ***



Según el protocolo de generación de ACKs:

El receptor se espera a recibir el siguiente segmento 500ms, si no lo recibe envía el ACK.

Si llega un segmento ordenado y ya había otro sin confirmar, se genera un ACK acumulado para los dos.

*** **cwind** se refiere al tamaño de la ventana de congestión ***

$T_A = T_{ida} + \frac{8\cdot(1024+20)}{100\cdot10^6} + T_{vuelta} + \frac{8\cdot40}{100\cdot10^6} = 2{,}087ms$ ** 20 → cabecera IP, 40 → cabecs IP + TCP **

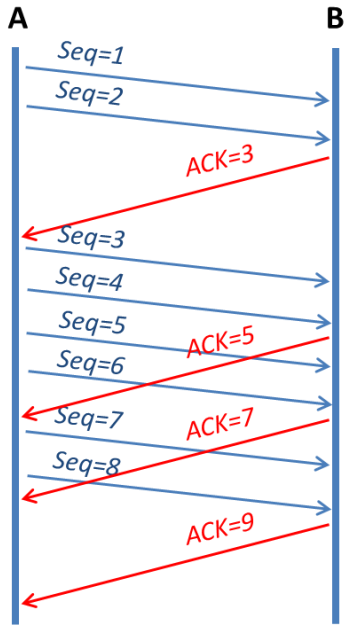
$T_B = T_{ida} + \frac{2\cdot8\cdot(1024+20)}{100\cdot10^6} + T_{vuelta} + \frac{8\cdot40}{100\cdot10^6} = 2ms + 167{,}04\mu s + 3{,}2\mu s = 2{,}169ms$

$T_C = \frac{8\cdot(1024+20)}{100\cdot10^6} = 83{,}52\ \mu s$ [Tiempo de transmisión del séptimo segmento]

$T_{TOTAL} = T_{CONEXIÓN} + T_A + T_B + T_C = 3{,}0096ms + 4{,}3398ms = 7{,}3494ms$

- A esto se le podría sumar el tiempo de generación de los segmentos.
- También el tiempo de generación y procesamiento de ACKs.
- Además, en cada suma de tamaños de cabeceras, habría que considerar el tamaño de las cabeceras de capas inferiores.

Números de secuencia y acuse (numeración simple):



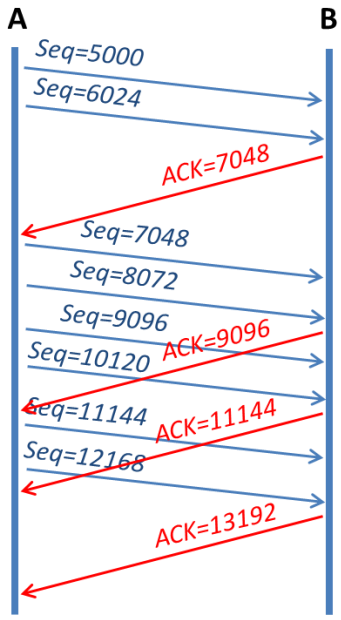
Usando una numeración simple para los números de secuencia y considerando que el receptor B no enviaría datos a A (sólo confirmaciones), el intercambio de segmentos y acuses sería el mostrado en la figura.

(Piense en un servicio de subida de archivos, por ejemplo, en el que el servidor B únicamente confirma que se han subido correctamente los datos)

Debemos recordar que se trata de confirmaciones acumulativas, es decir, un acuse confirma varios segmentos recibidos.

El acuse se referirá al número de secuencia del siguiente segmento a recibir.

Números de secuencia y acuse (numeración realista):



Consideramos que el ISN es actualmente 5000, por lo que el primer segmento se asocia a ese número.

Cada segmento tiene un tamaño de 1024 bytes, según el enunciado.

Consideramos nuevamente que el receptor B no enviaría datos a A (sólo confirmaciones).

Se trata de confirmaciones acumulativas.

El acuse se referirá al número de secuencia (byte de comienzo) del siguiente segmento a recibir.

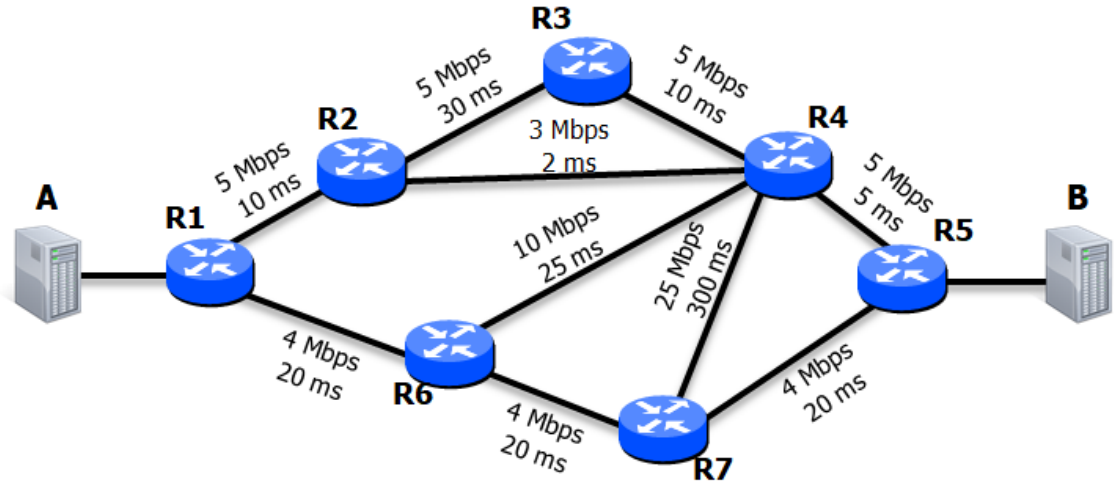
*** Hay que destacar que, tanto este, como el diagrama anterior no son precisos en cuanto a la representación de los tiempos, ya que, por ejemplo, el tiempo de transmisión del ACK será en realidad menor que el del envío de los segmentos de datos.*
*Se ha hecho de esta forma para mayor claridad. ***

EJERCICIO DE ENCAMINAMIENTO DINÁMICO

Dada la topología de la figura, explique qué ruta se utilizaría para mandar información entre el *host* A y el *host* B suponiendo:

a) que los routers implementan RIP y

b) que los routers implementan OSPF. En el caso de que haya varias rutas posibles, explique cómo se elegiría la ruta a seguir en un caso real.

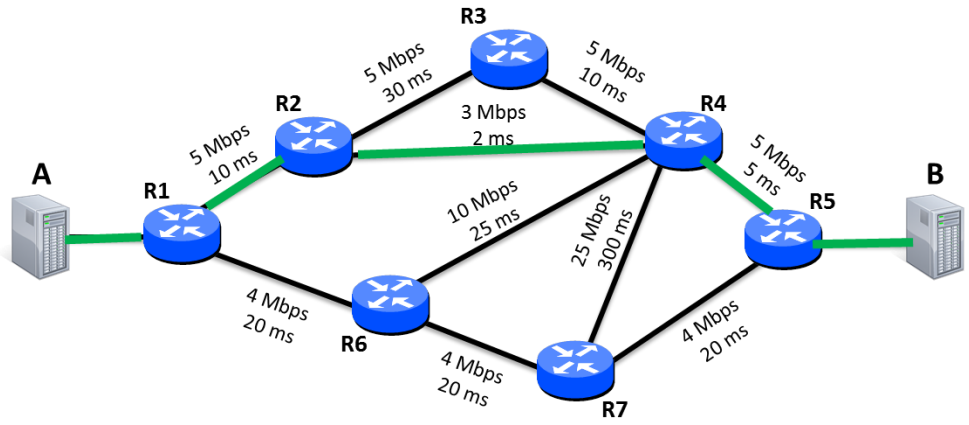


RIP:

RIP se basa en la distancia medida como número de saltos (1 salto = 1 envío entre routers). En la topología propuesta hay varias posibilidades con el mismo coste. Para elegir una ruta u otra **NO** se utilizan los valores de latencia o ancho de banda de los enlaces, sino que nos quedamos con la primera ruta anunciada. Es decir, si un router recibe una ruta con un cierto coste, modificará su ruta actual si y solo si la nueva ruta tiene un coste menor. Si tiene un coste igual o superior, no cambiará la ruta. Por tanto, se elegirá la primera ruta anunciada sin tener en cuenta otras consideraciones. La primera ruta anunciada dependerá del orden

en el que se enciendan los routers y manden/procesen los mensajes RIP, por lo que a priori no podemos saber cuál será. Lo que se espera de este ejercicio es que se indique que habría varias rutas posibles y se elige una concreta suponiendo que es la primera anunciada.

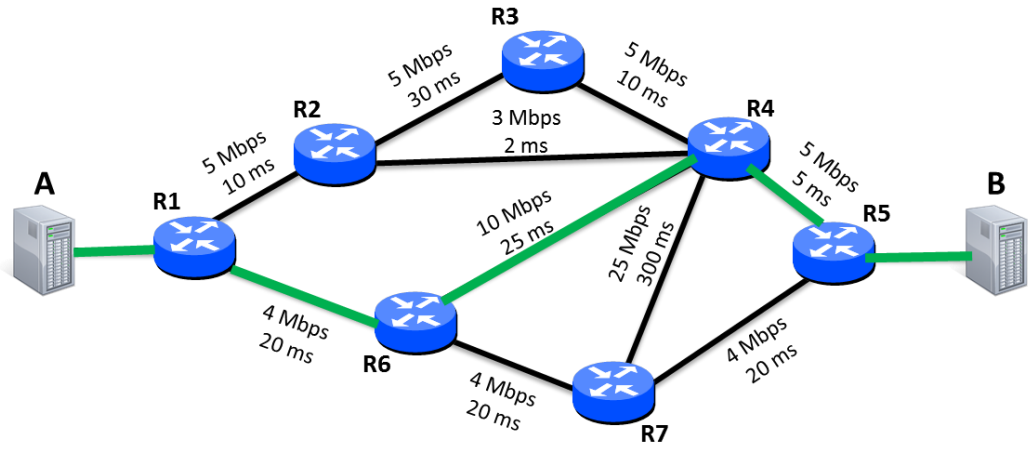
En la topología, hay varias rutas con un número de saltos igual a 3. Por ejemplo, A → R1 → R2 → R4 → R5 → B. Otra podría ser A → R1 → R6 → R4 → R5 → B. Otra sería A → R1 → R6 → R7 → R5 → B. La ruta elegida dependerá del orden de arranque de los routers, pero podríamos suponer, por ejemplo, la primera: A → R1 → R2 → R4 → R5 → B



OSPF:

OSPF utiliza como métrica por defecto el inverso del ancho de banda (concretamente $\frac{10^8}{BW\ (bps)}$, aunque la constante 10^8 no nos afecta a la hora de minimizar el coste total). OSPF utiliza el algoritmo de Dijkstra para buscar el grafo con menor coste total, pero nosotros lo haremos probando ya que la topología tiene muy pocos caminos posibles. El objetivo NO es coger los enlaces con el mayor ancho de banda sino coger el camino cuyo coste total sea mínimo ($min\left\{\sum_{enlace\ i}\left(\frac{10^8}{BW\ (bps)}\right)\right\} = min\left\{\sum_{enlace\ i}\left(\frac{1}{BW\ (Mbps)}\right)\right\}$).

Por ejemplo, el camino que habíamos elegido para RIP tendría como coste en OSPF $\frac{1}{5}+\frac{1}{5}+\frac{1}{5}+\frac{1}{5} = 0.8$. Habría que probar los diferentes posibles caminos para encontrar el de mínimo coste. Después de hacer varias pruebas sobre la topología, el camino de coste mínimo sería A → R1 → R6 → R4 → R5 → B, que tendría un coste $\frac{1}{4}+\frac{1}{10}+\frac{1}{5} = 0.55$.



NOTA IMPORTANTE: La latencia no se utiliza para nada, ni en RIP ni en OSPF. Se ha puesto en el ejercicio para comprobar que el estudiante tiene los conceptos claros.