Universitat Politècnica de Catalunya
Departament d'Arquitectura de Computadors

XARXES DE COMPUTADORS
PROBLEMAS RESUELTOS

Davide Careglio

Mayo 2011

Edición borrador.

ISBN:
Registration number

Universitat Politècnica de Catalunya (UPC)
Departament d'Arquitectura de Computadors (DAC)
C/ Jordi Girona, 1-3
08034 Barcelona, Spain

Índice

Capítulo 1.
Preguntas cortas.

1.1. - Preguntas redes IP

1.1.1. Un host H está transmitiendo a un servidor S pasando por el router R. El MTU de H es de 576 bytes mientras que el MTU de R es de 200 bytes. Determinar la longitud del último fragmento que llega a S (comprendida la cabecera IP).

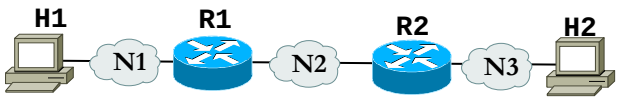
1.1.2. Sabiendo que la MTU de una red es de 320 bytes y llega un datagrama de 1500 bytes, deducir el tamaño del último fragmento incluida la cabecera IP.

1.1.3. Sabiendo que la MTU de una red es de 460 bytes y llega un datagrama de 1500 bytes, deducir el tamaño del último fragmento incluida la cabecera IP.

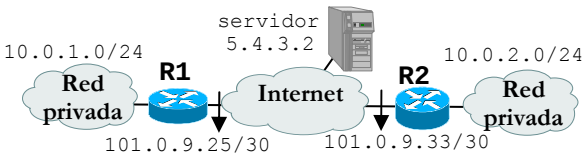
1.1.4. Sabiendo que la MTU de una red es de 250 bytes y llega un datagrama de 1500 bytes, deducir el tamaño del último fragmento incluida la cabecera IP

1.1.5. Un datagrama de 1500 bytes pasa por una red con MTU de 576 bytes y sucesivamente por una de 250. Calcular la longitud del último fragmento (cabecera IP incluida) cuando llega al destino

1.1.6. Determinar el número de mensajes ARP se intercambian los dispositivos de la figura sabiendo que H1 hace un ping a H2 y que todas las tablas ARP están vacías.

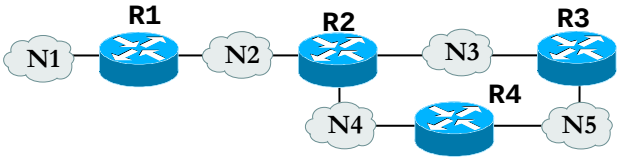


1.1.7. Sabiendo que entre R1 y R2 hay un túnel y que R1 aplica PAT para traducir las direcciones privadas a las públicas, deducir:



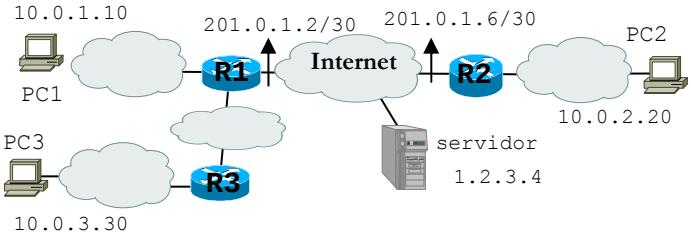
a) Las direcciones IP origen y destino de los datagramas que de R1 van al servidor con origen un host de la red 10.0.1.0/24.
b) Las direcciones IP origen y destino de los datagramas que de R2 van al servidor con origen un host de la red 10.0.2.0/24.
c) Las direcciones IP origen y destino de los datagramas que de R1 van al R2 con origen un host de la red 10.0.1.0/24.

1.1.8. La red de la figura usa RIPv1, deducir:



a) La tabla de encaminamiento de R4.
b) Si la red N2 falla, el mensaje que envía el router R2 a R3 si tiene activo split horizon y poison reverse pero no triggered update.
c) El mensaje de actualización que el router R1 envía a R2 si tiene split horizon activo.
d) El mensaje de actualización que el router R2 envía a R4 si tiene split horizon activo

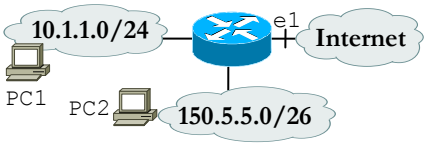
1.1.9. La red de la figura usa un túnel entre R1 y R2 y ambos routers usan NAT dinámico usando el rango de direcciones 201.0.1.100-201.0.1.109. Deducir:



a) La dirección origen de los datagramas que llegan al servidor si PC1 le hace un ping.
b) Las direcciones origen y destino de los datagramas que pasan por Internet si PC3 hace un ping a PC2.
c) Las direcciones origen y destino de los datagramas que pasan por las redes privadas si PC2 hace un ping a PC1.
d) Las direcciones origen y destino de los datagramas que pasan por Internet si PC2 hace un ping al servidor

1.1.10. De acuerdo con la siguiente ACL aplicada a la interfaz e1 del router y la figura de la derecha, deducir:

a) Si el cliente 10.1.1.10 puede bajarse una página web de un servidor en Internet
b) Si el cliente 147.7.7.7 en Internet puede conectarse al servidor 10.1.1.254
c) Si el servidor DNS 150.5.5.5 puede resolver un nombre en Internet
d) Si el cliente 10.1.1.10 puede hacer un ping al servidor 150.5.5.5
e) Si el host 147.7.7.7 puede hacer un ping al host 10.1.1.10



	acción	IP origen	IP destino	protocolo	puerto origen	puerto destino	estado
1.	permitir	any	150.5.5.0/26	TCP	>1023	<1024	any
2.	permitir	150.5.5.0/26	any	TCP	<1024	>1023	established
3.	permitir	10.1.1.0/24	any	TCP	>1023	<1024	any
4.	permitir	any	10.1.1.0/24	TCP	<1024	>1023	established
5.	permitir	150.5.5.0/26	any	UDP	any	any	any
6.	permitir	any	150.5.5.0/26	UDP	any	any	any
7.	**prohibir**	**any**	**any**	**IP**	**any**	**any**	**any**

1.1.11. Hay 4 hosts (H1, H2, H3 y H4) conectados en una misma red con un router que hace de Gateway hacia Internet. Suponer que se hace un ping entre H1 y H4, determinar cuántos datagramas IP viajaran en la red desde que se ejecuta el ping hasta recibir la primera respuesta.

1.2. - Preguntas ARQ

1.2.1. Un protocolo ARQ de transmisión continua con control de flujo basado en una ventana deslizante tiene un tiempo de propagación de 1 ms y un tiempo de trama de 0.5 ms (la duración de los ack es despreciable). Determinar la ventana óptima.

1.2.2. Calcular el número medio de PDUs que se transmiten al segundo en un sistema que usa un protocolo S&W con tiempo de propagación de 10 ms, velocidad de transmisión de 100 kbit/s, longitud de la PDU de 1000 bytes, temporizador To de 150 ms y número medio de transmisiones Nt = 1.05.

1.2.3. Deducir la ventana de transmisión optima de un protocolo GBN con PDUs de 1000 bits, confirmaciones de 200 bits, tiempo de propagación de 10 ms y velocidad de transmisión de 100 kbit/s.

1.2.4. Determinar el número medio de transmisiones de una PDU de 450 bytes y probabilidad de pérdida por bit *Pb* de 10^{-5}.

1.2.5. Deducir la eficiencia de un sistema que usa retransmisión selectiva con PDUs de 800 bytes. La probabilidad que un bit llegue con un error es de 10^{-5}.

1.2.6. De un sistema de transmisión que usa ARQ, deducir:

a) La eficiencia de GBN si no hay pérdidas.
b) La ventana óptima si se usara GBN con tiempo de propagación de 10 ms y tiempo de transmisión de una PDU de 20 ms.
c) La ventana óptima si se usara Retransmisión Selectiva con tiempo de propagación de 10 ms y tiempo de transmisión de una PDU de 20 ms.
d) Si con S&W la eficiencia máxima se consigue cuando el tiempo de propagación es mucho más grande que el tiempo de transmisión de una PDU

1.2.7. Sabiendo que la velocidad de transmisión entre dos puntos distantes 100 km es de 1500 kbit/s, la velocidad de propagación es de 2×10^8 m/s y las PDU de datos son de 1500 bytes, deducir:

a) El número medio de transmisiones con una pérdida por bit de 5×10^{-6}.
b) El tiempo de ciclo.
c) La eficiencia si el sistema usara retransmisión selectiva y el número medio de transmisiones fuera de 1.05.
d) La ventana óptima.

1.2.8. Sabiendo que la velocidad de transmisión entre dos puntos distantes 250 km es de 500 kbit/s, la velocidad de propagación es de 2×10^8 m/s y las PDUs son de 100 bytes (considerar ack = 0 bytes), deducir:

a) La eficiencia si se usa S&W.
b) La eficiencia si se usa GBN.
c) La eficiencia si se usa SR.
d) El número medio de transmisiones si la eficiencia usando SR es 0.83.
e) El temporizador.
f) La ventana óptima si se usa GBN.
g) La ventana óptima si se usa SR.
h) El número medio de transmisiones si la probabilidad de pérdida en un bit es de 10^{-4}.

1.2.9. Calcular la velocidad de transmisión entre dos puntos distantes 200 km sabiendo que aplican un S&W con eficiencia 0.8, la velocidad de propagación es de 2×10^8 m/s y las PDU de datos son de 1000 bytes.

1.2.10. Dos puntos implementan un protocolo ARQ para transferir datos. Los datos conocidos son: tiempo de propagación de 100 μs, velocidad de transmisión de 2 Mbit/s, longitud PDU y ack de 1200 bits. Deducir:

a) La eficiencia si se usa GBN.
b) El temporizador.
c) La ventana óptima si se usa transmisión continúa.
d) La eficiencia del SR si hay una probabilidad de pérdida de bit de 2×10^{-5}.

1.2.11. Sabiendo que la velocidad de transmisión entre dos puntos distantes 50 km es de 8 Mbit/s, la velocidad de propagación es de 2×10^8 m/s, las PDUs son de 1000 bytes y los ack de 40 bytes, deducir:

a) El temporizador.
b) La eficiencia si se usara SR con probabilidad de pérdida en un bit de 10^{-5}.
c) La ventana óptima.
d) La eficiencia si se usara GBN sin pérdidas.

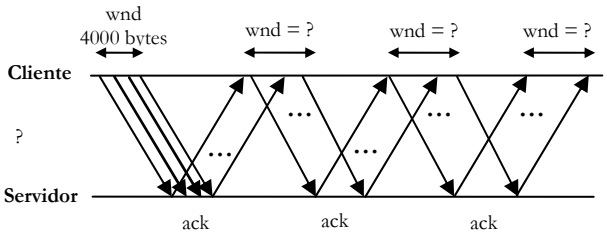
1.2.12. Sabiendo que la velocidad de transmisión entre dos puntos distantes 100 km es de 10 Mbit/s, la velocidad de propagación es de 2×10^8 m/s, las PDUs son de 1000 bytes y los ack de 40 bytes, deducir:

a) El temporizador.
b) La eficiencia si se usara SR sin pérdidas.
c) La eficiencia si se usara GBN con probabilidad de pérdida en un bit de 10^{-5} y temporizador To de 2.5 ms.
d) La ventana óptima.

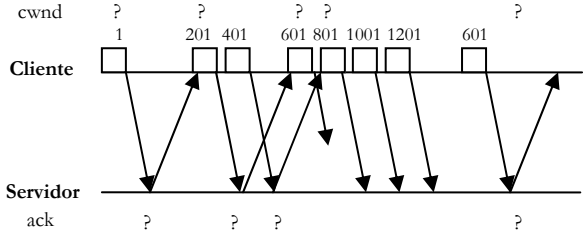
1.3. - Preguntas TCP

1.3.1. Sabiendo que awnd = 600 bytes, cwnd = 200 bytes, MSS = 100 bytes y ssthresh = 400 bytes, deducir la secuencia de valores de la ventana de transmisión al recibir 6 acks sin errores.

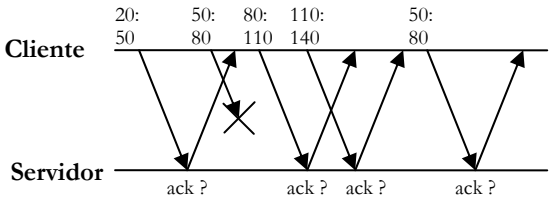
1.3.2. Un cliente y un servidor tienen una conexión TCP abierta. Se sabe que al principio de la figura wnd = 4000 bytes y ssthresh = 8000 bytes. El MSS es de 1000 bytes. Deducir la secuencia del wnd del cliente sabiendo que awnd del servidor es de 9000 bytes, no se pierde ningún ack y el cliente siempre tiene el buffer de transmisión lleno.



1.3.3. Un cliente y un servidor acaban de establecer una conexión TCP. El MSS es de 200 bytes. Deducir la secuencia de la cwnd del cliente y del ack del servidor.

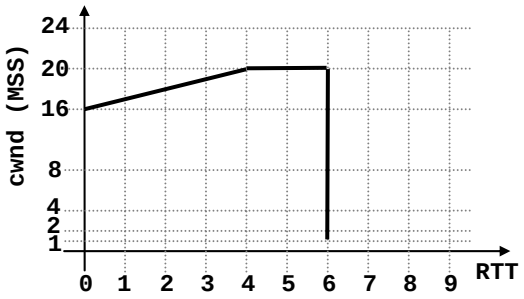


1.3.4. Un cliente y un servidor tienen una conexión TCP sack con Slow Start, Congestion Avoidance y Fast Retransmission activa. Deducir la secuencia de ack del servidor.



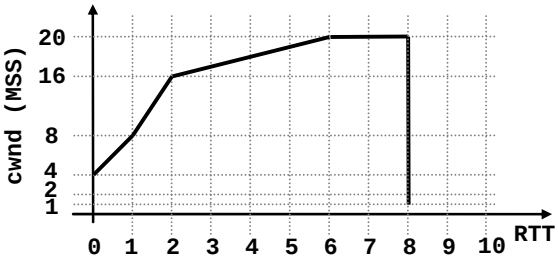
1.3.5. Un cliente y un servidor tienen una conexión TCP abierta. Se sabe que el MSS es de 1500 bytes y el RTT es de 10 ms. En la figura se cuentan los ciclos RTT a partir de un momento cualquiera indicado como 0. Deducir:

a) El valor de cwnd al tiempo 8.
b) El valor de ssthresh al tiempo 6.
c) Que mecanismo del TCP se ha usado del tiempo 0 al tiempo 4.
d) El valor de RTO después del tiempo 6.



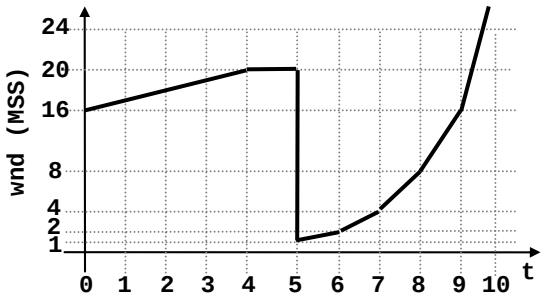
1.3.6. Un cliente y un servidor tienen una conexión TCP abierta. Se sabe que el MSS es de 250 bytes, el RTT es de 5 ms y el RTO de 10 ms. A partir de figura de la derecha, deducir:

a) El valor de ssthresh del tiempo 0 al tiempo 7.
b) El valor del temporizador RTO al tiempo 8.
c) Que mecanismo del TCP se usa del tiempo 2 al tiempo 6.
d) Que mecanismo del TCP se usa a partir del tiempo 8.



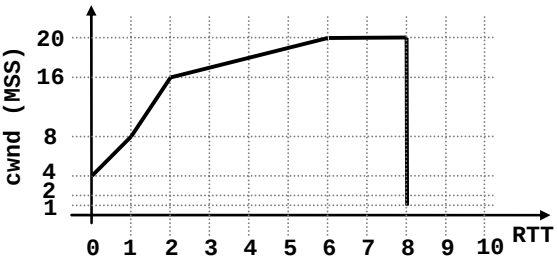
1.3.7. Un cliente y un servidor tienen una conexión TCP abierta. Se sabe que el MSS es de 500 bytes, el RTT es de 40 ms, el RTO de 50 ms y la awnd es de 30 MSS. A partir de figura, deducir:

a) Que mecanismo del TCP se ha aplicado del tiempo 0 al 4.
b) El valor de wnd en el tiempo 4.
c) El valor de RTO en el tiempo 5.
d) Si la gráfica es correcta a partir del tiempo 5 en adelante.



1.3.8. Un cliente y un servidor tienen una conexión TCP abierta. Se sabe que el MSS es de 400 bytes, el RTT es de 10 ms y el RTO de 20 ms. A partir de figura, deducir:

a) El valor de ssthresh del tiempo 0 al tiempo 7 RTT.
b) Que mecanismo del TCP se usa del tiempo 2 al tiempo 6 RTT.
c) El valor de RTO al tiempo 8 RTT.
d) El valor de ssthresh a partir del tiempo 8 RTT.



1.3.9. Hay una conexión TCP abierta entre un cliente y un servidor y se activa un tcpdump en el servidor. Deducir:

```
08:27:18.927644 80.102.155.131.1160 > 64.154.81.168.80: . 2905:3279(374) ack 1 win 8192
08:27:18.923760 64.154.81.168.80 > 80.102.155.131.1160: . ack ???? win 5808
08:27:19.827561 80.102.155.131.1160 > 64.154.81.168.80: . 3279:3653(374) ack 1 win 8192
```

a) El número de ack que se necesita para confirmar la recepción de los datos recibidos en lugar de ????.
b) Quien entre el cliente y el servidor está enviando datos y quien confirmaciones.
c) El valor de awnd que está anunciando el extremo que envía los datos.

1.3.10. De acuerdo con la siguiente captura de una conexión TCP de tipo transferencia masiva, deducir si hay pérdidas y que segmentos se han perdido.

```
11:50:29.02   8.10.15.131.1104  >  104.70.80.180.21: . 82227:82803(576) ack 209 win 7890
11:50:29.03   104.70.80.180.21  >  8.10.15.131.1104: . ack 82803 win 27890
11:50:29.03   8.10.15.131.1104  >  104.70.80.180.21: . 82803:83379(576) ack 209 win 7890
11:50:29.03   8.10.15.131.1104  >  104.70.80.180.21: . 83379:83955(576) ack 209 win 7890
11:50:29.03   8.10.15.131.1104  >  104.70.80.180.21: . 83955:84531(576) ack 209 win 7890
11:50:29.03   8.10.15.131.1104  >  104.70.80.180.21: . 84531:85107(576) ack 209 win 7890
11:50:29.04   104.70.80.180.21  >  8.10.15.131.1104: . ack 82803 win 27890
11:50:29.04   104.70.80.180.21  >  8.10.15.131.1104: . ack 82803 win 27890
11:50:29.05   8.10.15.131.1104  >  104.70.80.180.21: . 82803:83379(576) ack 209 win 7890
11:50:30.06   104.70.80.180.21  >  8.10.15.131.1104: . ack 83955 win 27890
11:50:29.06   8.10.15.131.1104  >  104.70.80.180.21: . 83955:84531(576) ack 209 win 7890
11:50:30.07   104.70.80.180.21  >  8.10.15.131.1104: . ack 85107 win 27890
```

1.3.11. Hay una conexión TCP abierta entre un cliente y un servidor y se activa el tcpdump en el servidor. Deducir:

```
1.  ...
2.  15:54:02.090726 IP 64.154.81.168.80 > 80.102.155.131.1160: P 72805:74285(1480) ack 1 win 64240
3.  15:54:02.090867 IP 64.154.81.168.80 > 80.102.155.131.1160: . 74285:75765(1480) ack 1 win 64240
4.  15:54:02.313596 IP 80.102.155.131.1160 > 64.154.81.168.80: ack 72805 win 7400
5.  15:54:02.313663 IP 64.154.81.168.80 > 80.102.155.131.1160: . 75765:77245(1480) ack 1 win 64240
6.  15:54:02.313727 IP 64.154.81.168.80 > 80.102.155.131.1160: . 77245:78725(1480) ack 1 win 64240
7.  15:54:02.541251 IP 80.102.155.131.1160 > 64.154.81.168.80: ack 74285 win 4380
8.  15:54:02.717161 IP 80.102.155.131.1160 > 64.154.81.168.80: ack 75765 win 4380
9.  15:54:02.717309 IP 64.154.81.168.80 > 80.102.155.131.1160: . 78725:80205(1480) ack 1 win 64240
```

a) Que significa la P de la línea 2.
b) Si el cliente ha enviado segmentos de datos.
c) Si hay pérdidas y donde.
d) La ventana wnd del servidor cuando éste recibe el ack de la línea 4.
e) Cual entre awnd y cwnd está limitando wnd del servidor.

1.3.12. De acuerdo con la siguiente captura de una conexión TCP de tipo transferencia masiva, deducir:

```
1.   3.3.5.5.1104  >  10.7.80.1.80: S 9863486324:9863486324(0) win 7890 <MSS 1460>
2.   10.7.80.1.80  >  3.3.5.5.1104: S 78681332:78681332(0) ack 9863486325 win 27890 <MSS 1460>
3.   3.3.5.5.1104  >  10.7.80.1.80: . ack 1 win 7890
4.   3.3.5.5.1104  >  10.7.80.1.80: P 1:16(15) ack 1 win 7890
5.   10.7.80.1.80  >  3.3.5.5.1104: . 1:1461(1460) ack 16 win 27890
6.   3.3.5.5.1104  >  10.7.80.1.80: . ack 1461 win 7890
7.   10.7.80.1.80  >  3.3.5.5.1104: . 1461:2921(1460) ack 16 win 27890
8.   10.7.80.1.80  >  3.3.5.5.1104: . 2921:4381(1460) ack 16 win 27890
9.   3.3.5.5.1104  >  10.7.80.1.80: . ack 2921 win 7890
10.  10.7.80.1.80  >  3.3.5.5.1104: . 4381:5501(1120) ack 16 win 27890
11.  3.3.5.5.1104  >  10.7.80.1.80: . ack 4381 win 7890
12.  3.3.5.5.1104  >  10.7.80.1.80: . 16:592(576) ack 5501 win 7890
13.  10.7.80.1.80  >  3.3.5.5.1104: F 5501:5501(0) ack 592 win 27890
14.  3.3.5.5.1104  >  10.7.80.1.80: F 592:592(0) ack 5502 win 7890
15.  10.7.80.1.80  >  3.3.5.5.1104: . ack 593 win 27890
```

a) Si hay pérdidas.
b) El total de bytes de datos transmitidos por el cliente.
c) El valor de la ventana anunciada del servidor al cliente durante la conexión.
d) El valor del MSS.
e) El estado del cliente en el punto 1.
f) La ventana cwnd del cliente en el punto 3.
g) La ventana cwnd del servidor en el punto 7.
h) Si en el punto 15 la conexión TCP se ha cerrado del todo.

1.3.13. De acuerdo con la siguiente captura de una conexión TCP de tipo transferencia masiva, deducir:

```
1.  ...
2.  192.168.249.128.1025 > 147.83.34.125.19: . ack 69885 win 4380
3.  147.83.34.125.19 > 192.168.249.128.1025: . 69885:71345(1460) ack 1 win 64240
4.  147.83.34.125.19 > 192.168.249.128.1025: P 72805:74265(1460) ack 1 win 64240
5.  192.168.249.128.1025 > 147.83.34.125.19: . ack 71345 win 0
6.  192.168.249.128.1025 > 147.83.34.125.19: . ack 71345 win 4380
7.  147.83.34.125.19 > 192.168.249.128.1025: . 74265:75725(1460) ack 1 win 64240
8.  147.83.34.125.19 > 192.168.249.128.1025: . 75725:77185(1460) ack 1 win 64240
9.  192.168.249.128.1025 > 147.83.34.125.19: . ack 71345 win 4380
10. 192.168.249.128.1025 > 147.83.34.125.19: . ack 71345 win 4380
11. 147.83.34.125.19 > 192.168.249.128.1025: . 71345:72805(1460) ack 1 win 64240
12. 192.168.249.128.1025 > 147.83.34.125.19: . ack 77185 win 4380
```

a) Si el volcado se ha capturado en el cliente o en el servidor.
b) Si ha habido pérdidas y que mecanismo ha actuado en la recuperación.

1.4. - Preguntas LAN

1.4.1. Se dispone de una red formada por 1 router de 2 puertos, un puerto conectado a un servidor y el otro a un 1 conmutador de 4 puertos. A los 3 puertos libres del conmutador hay conectados 3 hubs de 6 puertos. Deducir:
a) El número de dominios de colisión.
b) El número de LANs que se pueden configurar si el conmutador no soporta trunking.
c) El número de VLANs que se pueden configurar si el conmutador soporta trunking.
d) El número de hosts que se pueden conectar a los hubs.

1.4.2. En caso de colisión entre tramas Ethernet, una estación hace varias operaciones. Deducir:
a) Si se genera un tiempo aleatorio backoff.
b) Si tiene prioridad sobre las otras estaciones que transmiten por primera vez.
c) Cuantas colisiones de la misma trama pueden ocurrir.
d) Si se duplica el tiempo de time-out.

1.4.3. Deducir:
a) Qué tipo de control de flujo usa un conmutador Ethernet en FDX.
b) Cómo hace el protocolo MAC de WLAN para verificar si ha habido colisiones.
c) A que sirven los paquetes RTS/CTS.
d) Cuantas direcciones físicas usa una estación WLAN para enviar una trama a un AP con destino otra estación de la misma WLAN.

1.5. - Preguntas nivel físico

1.5.1. Sabiendo que un canal de transmisión usa codificación NRZ y tiene un ancho de banda de 100 kHz, deducir:
a) Si una velocidad de modulación de 150 kbaud crea distorsión grave (ISI).
b) La capacidad del canal si la relación señal ruido es de 20 dB.
c) La velocidad de transmisión si el tiempo de bit es de 10 μs.

1.5.2. En un enlace de 40 km con atenuación de 0.4dB/km, un transmisor transite una señal de 1 W a un receptor con sensibilidad de 10 mW. Deducir cuantos amplificadores con sensibilidad de 10 mW y ganancia de 20 dB se necesitan.

1.5.3. Sabiendo que un sistema de transmisión con ancho de banda *BW* de 100 kHz, deducir:
a) Si hay distorsión con una codificación Manchester y una velocidad de transmisión de 200 kbit/s.
b) La capacidad del canal con una SNR = 25.
c) Si con símbolos de 8 μs hay distorsión.
d) La velocidad de transmisión con una codifica digital de 8 símbolos y una velocidad de modulación máxima sin distorsión.

1.6. - Soluciones

1.1.1. Host H -----> Router R ------> Servidor S
MTU de H = 576 bytes, MTU de R = 200 bytes, por lo tanto R necesita fragmentar.
De los 200 bytes, 20 bytes son de cabecera IP, por lo tanto quedan 180 bytes
Se verifica que 180 no es múltiplo de 8: 180 / 8 = 22.5, se coge el múltiplo menor 22 * 8 = 176 bytes
De los 576 bytes, 20 bytes son de cabecera IP, por lo tanto hay que fragmentar 556 bytes
Primer fragmento de 176 + 20 de cabecera = 196 bytes, quedan 556 – 176 = 380 bytes
Segundo fragmento de 196 bytes, quedan 280 – 176 = 204 bytes
Tercer fragmento de 196 bytes, quedan 204 – 176 = 28 bytes
Ultimo fragmento de 28 + 20 = 48 bytes

1.1.2. MTU de una red = 320 bytes, llega un datagrama de 1500 bytes, se necesita fragmentar.
De los 320 bytes, 20 bytes son de cabecera IP, por lo tanto quedan 300 bytes
Se verifica que 300 no es múltiplo de 8: 300 / 8 = 37.5, se coge el múltiplo menor 37 * 8 = 296 bytes
De los 1500 bytes, 20 bytes son de cabecera IP, por lo tanto hay que fragmentar 1480 bytes
Primer fragmento de 296 + 20 de cabecera = 316 bytes, quedan 1480 – 296 = 1184 bytes
Segundo fragmento de 316 bytes, quedan 1184 – 296 = 888 bytes
Tercer fragmento de 316 bytes, quedan 888 – 296 = 592 bytes
Cuarto fragmento de 316 bytes, quedan 592 – 296 = 296 bytes
Ultimo fragmento de 296 + 20 = 316 bytes

1.1.3. MTU de una red = 460 bytes, llega un datagrama de 1500 bytes, se necesita fragmentar.
De los 460 bytes, 20 bytes son de cabecera IP, por lo tanto quedan 440 bytes
Se verifica que 440 es múltiplo de 8: 440 / 8 = 55
De los 1500 bytes, 20 bytes son de cabecera IP, por lo tanto hay que fragmentar 1480 bytes
Primer fragmento de 440 + 20 de cabecera = 460 bytes, quedan 1480 – 440 = 1040 bytes
Segundo fragmento de 460 bytes, quedan 1040 – 440 = 600 bytes
Tercer fragmento de 460 bytes, quedan 600 – 440 = 160 bytes
Ultimo fragmento de 160 + 20 = 180 bytes

1.1.4. MTU de una red = 250 bytes, llega un datagrama de 1500 bytes, se necesita fragmentar.
De los 250 bytes, 20 bytes son de cabecera IP, por lo tanto quedan 230 bytes
Se verifica que 230 no es múltiplo de 8: 230 / 8 = 28.75, se coge el múltiplo menor 28 * 8 = 224 bytes
De los 1500 bytes, 20 bytes son de cabecera IP, por lo tanto hay que fragmentar 1480 bytes
Primer fragmento de 224 + 20 de cabecera = 244 bytes, quedan 1480 – 224 = 1256 bytes
Segundo fragmento de 244 bytes, quedan 1256 – 224 = 1032 bytes
Tercer fragmento de 244 bytes, quedan 1032 – 224 = 808 bytes
Cuarto fragmento de 244 bytes, quedan 808 – 224 = 584 bytes
Quinto fragmento de 244 bytes, quedan 584 – 224 = 360 bytes
Sexto fragmento de 244 bytes, quedan 360 – 224 = 136 bytes
Ultimo fragmento de 136 + 20 = 156 bytes

1.1.5. MTU de una red = 576 bytes y llega un datagrama de 1500 bytes, se necesita fragmentar.
De los 576 bytes, 20 bytes son de cabecera IP, por lo tanto quedan 556 bytes
Se verifica que 556 no es múltiplo de 8: 556 / 8 = 69, se coge el múltiplo menor 69 * 8 = 552 bytes
De los 1500 bytes, 20 bytes son de cabecera IP, por lo tanto hay que fragmentar 1480 bytes
Primer fragmento de 552 + 20 de cabecera = 572 bytes, quedan 1480 – 552 = 928 bytes
Segundo fragmento de 244 bytes, quedan 928 – 552 = 376 bytes
Ultimo fragmento de 376 + 20 = 396 bytes
MTU de la segunda red = 250 bytes y el ultimo datagrama es de 396 bytes, se necesita fragmentar.
De los 250 bytes, 20 bytes son de cabecera IP, por lo tanto quedan 230 bytes
Se verifica que 230 no es múltiplo de 8: 230 / 8 = 28.75, se coge el múltiplo menor 28 * 8 = 224 bytes
De los 396 bytes, 20 bytes son de cabecera IP, por lo tanto hay que fragmentar 376 bytes
Primer fragmento de 224 + 20 de cabecera = 244 bytes, quedan 376 – 224 = 152 bytes
Ultimo fragmento de 152 + 20 = 172 bytes

1.1.6. 6 mensajes ARP
ARP request de H1 a R1, ARP reply de R1 a H1
ARP request de R1 a R2, ARP reply de R2 a R1
ARP request de R2 a H2, ARP reply de H2 a R2

1.1.7.

a) R1 aplica PAT; IP origen 101.0.9.25, IP destino 5.4.3.2
b) R2 usa el túnel hasta R1; IP origen 101.0.9.33, IP destino 101.0.9.25 (IP internas, origen 10.0.2.X, destino 5.4.3.2)
Luego R1 aplica PAT; IP origen 101.0.9.25, IP destino 5.4.3.2
c) R1 usa el túnel hasta R2; IP origen 101.0.9.25, IP destino 101.0.9.33 (IP internas, origen 10.0.1.X, destino 10.0.2.Y)

1.1.8.

a) Tabla de encaminamiento de R4

red	gw	hops
N1	R2	3
N2	R2	2
N3	R3	2
N4	-	1
N5	-	1

b) Si falla N2, R2 envía el siguiente mensaje a R3 pasados 30 segundos desde el último mensaje de actualización si tiene Split horizon y Poison reverse activos. R2 puede haber aprendido la red N5 bien de R4 o bien de R3. Si en la tabla de R2, R3 aparece como Gateway de N5, entonces R2 no enviaría su conocimiento de N5 (por eso es entre paréntesis).

red	hops
N1	16
N2	16
N4	1
(N5)	1

c) Mensaje de R1 a R2 cada 30 segundos con Split horizon activo.

red	hops
N1	1

d) Mensaje de R2 a R4 cada 30 segundos con Split horizon activo. . R2 puede haber aprendido la red N5 bien de R4 o bien de R3. Si en la tabla de R2, R4 aparece como Gateway de N5, entonces R2 no enviaría su conocimiento de N5 (por eso es entre paréntesis)

red	hops
N1	2
N2	1
N3	1
(N5)	2

1.1.9.

a) R1 aplica NAT dinámico: IP origen 201.0.1.100
b) R1 aplica IP en IP: IP origen 201.0.1.2, IP destino 201.0.1.6
c) IP privada origen 10.0.2.20, IP privada destino 10.0.1.10
d) R2 aplica NAT dinámico: IP origen 201.0.1.100, IP destino 1.2.3.4

1.1.10.

a) El cliente 10.1.1.10 puede bajarse una página web de un servidor en Internet porque las reglas 3 (petición al servidor) y 4 (respuesta servidor) lo permiten.
b) Ninguna regla de la ACL permite que el cliente 147.7.7.7 en Internet no puede conectarse al servidor 10.1.1.254.
c) La regla 5 deja pasar la solicitud de resolución de nombres en Internet (protocolo UDP) y la regla 6 deja pasar la respuesta.
d) El cliente 10.1.1.10 puede hacer un ping al servidor 150.5.5.5 porque estos datagramas no pasan por la interfaz donde se aplica la ACL.
e) Ningún host de Internet puede hacer un ping (protocolo ICMP o IP) a la red 10.1.1.0/24.

1.1.11. 2 datagramas IP, el ICMP echo request y el ICMP echo reply del ping

1.2.1. Datos: ARQ de transmisión continua, Tt = 0.5 ms, Ta = 0, Tp = 1 ms

Tiempo de ciclo

$Tc = Tt + Ta + 2*Tp = 2.5$ ms

Ventana óptima

$Wopt = ceil(Tc / Tt) = ceil(2.5 / 0.5) = 5$ PDUs

1.2.2. Datos: S&W, Lt = 1000 bytes, vt = 100 kbit/s, Tp = 10 ms, To = 150 ms, Nt = 1.05
Duración de una PDU
$Tt = Lt / vt = 1000 * 8 / 100\times10^3 = 80$ ms
Tiempo de ciclo
$Tc = Tt + Ta + 2*Tp = 80 + 0 + 2*10$ ms = 100 ms
Número medio Q de PDUs
$Q = 1 / ((Nt - 1) * To + Tc) = 9.30$ PDUs/s

1.2.3. Datos: GBN, Lt = 1000 bits, La = 200 bits, vt = 100 kbit/s, Tp = 10 ms
Duración de una PDU y de un ack
$Tt = Lt / vt = 1000 / 100\times10^3 = 10$ ms
$Ta = La / vt = 200 / 100\times10^3 = 2$ ms
Tiempo de ciclo
$Tc = Tt + Ta + 2*Tp = 10 + 2 + 2*10$ ms = 32 ms
Ventana óptima
$Wopt = ceil(Tc / Tt) = ceil(32 / 10) = ceil(3.2) = 4$ PDUs

1.2.4. Datos: Lt = 450 bytes, $Pb = 10^{-5}$
Número medio de transmisiones
$Nt = 1 / (1 – Pb)^{Lt} = 1 / (1 – 10^{-5})^{450*8} = 1.037$

1.2.5. Datos: SR, Lt = 800 bytes, $Pb = 10^{-5}$
Número medio de transmisiones
$Nt = 1 / (1 – Pb)^{Lt} = 1 / (1 – 10^{-5})^{800*8} = 1.066$
Eficiencia
$E = 1 / Nt = 0.938$

1.2.6.
a) $E_{GBN} = 1$
b) Datos: GBN, Tp = 10 ms, Tt = 20 ms
Tiempo de ciclo
$Tc = Tt + Ta + 2 * Tp = 20 + 0 + 2*10 = 40$ ms
Ventana óptima
$Wopt = ceil(Tc / Tt) = ceil(40 / 20) = ceil(2) = 2$ PDUs
c) Datos: GBN, Tp = 10 ms, Tt = 20 ms
Mismo resultado que b), Wopt = 2 PDUs
d) La eficiencia con S&W es E = Tt / (Tt + Ta + 2*Tp). Cuando más grande es Tp, más grande el denominador, menor la eficiencia.

1.2.7. Datos: D = 100 km, vt = 1500 kbit/s, $vp = 2\times10^8$ m/s, Lt = 1500 bytes
a) Número medio de transmisiones con $Pb = 5\times10^{-5}$
$Nt = 1 / (1 – Pb)^{Lt} = 1 / (1 – 5\times10^{-5})^{1500*8} = 1.064$
b) Duración de una PDU
$Tt = Lt / vt = 1500 * 8 / 1500\times10^3 = 8$ ms
Tiempo de propagación
$Tp = D / vp = 100\times10^3 / 2\times10^8 = 0.5$ ms
Tiempo de ciclo
$Tc = Tt + Ta + 2*Tp = 8 + 0 + 2*0.5 = 9$ ms
c) Eficiencia si SR con Nt = 1.05
$E = 1 / Nt = 0.952$
d) Ventana óptima
$Wopt = ceil(Tc / Tt) = ceil(9 / 8) = ceil(1.125) = 2$ PDUs

1.2.8. Datos: D = 250 km, vt = 500 kbit/s, $vp = 2\times10^8$ m/s, Lt = 100 bytes, La = 0
a) Duración de una PDU
$Tt = Lt / vt = 100 * 8 / 500\times10^3 = 1.6$ ms
Tiempo de propagación
$Tp = D / vp = 250\times10^3 / 2\times10^8 = 1.25$ ms
Tiempo de ciclo
$Tc = Tt + Ta + 2*Tp = 1.6 + 0 + 2*1.25 = 4.1$ ms
Eficiencia con S&W
$E = Tt / Tc = 0.39$
b) La eficiencia con GBN es 1
c) La eficiencia con SR es 1

d) Número medio de transmisiones con $E_{SR} = 0.83$
   $Nt = 1 / E_{SR} = 1.2$
e) To > Tc = 4.1 ms, por ejemplo To = 4.5 ms
f) Ventana óptima
   Wopt = ceil(Tc / Tt) = ceil(4.1 / 1.6) = ceil(2.5625) = 3 PDUs
g) Lo mismo que f), Wopt = 3 PDUs
h) Número medio de transmisiones con $Pb = 10^{-4}$
   $Nt = 1 / (1 – Pb)^{Lt} = 1 / (1 – 10^{-4})^{100*8} = 1.08$

1.2.9. Datos: S&W, D = 200 km, E = 0.8, $vp = 2\times10^8$ m/s, Lt = 1000 bytes
Tiempo de propagación
$Tp = D / vp = 200\times10^3 / 2\times10^8 = 1$ ms
Duración de una PDU
Sabiendo que E = Tt / (Tt + Ta + 2*Tp), se encuentra que
Tt = 2*Tp * E / (1 - E) = 8 ms
Velocidad de transmisión
$vt = Lt / Tt) = 1000*8 / 8\times10^{-3} = 1$ Mbit/s

1.2.10. Datos: Tp = 100 μs, vt = 2 Mbit/s, Lt = La = 1200 bits
a) La eficiencia con GBN es 1
b) Duración de una PDU y ack
   $Tt = Lt / vt = 1200 / 2\times10^6 = 600$ μs
   Ta = Tt = 600 μs
   Tiempo de ciclo
   Tc = Tt + Ta + 2*Tp = 600 + 600 + 2*100 = 1.4 ms
   Temporizador
   To > Tc = 1.4 ms, por ejemplo To = 1.6 ms
c) Ventana óptima
   Wopt = ceil(Tc / Tt) = ceil(1400 / 600) = ceil(2.33) = 3 PDUs
d) Número medio de transmisiones con $Pb = 2\times10^{-5}$
   $Nt = 1 / (1 – Pb)^{Lt} = 1 / (1 – 2\times10^{-5})^{1200+1200} = 1.05$
   Eficiencia SR
   $E_{SR} = 1 / Nt = 0.95$

1.2.11. Datos: D = 50 km, vt = 8 Mbit/s, $vp = 2\times10^8$ m/s, Lt = 1000 bytes, La = 40 bytes
a) Duración de una PDU y ack
   $Tt = Lt / vt = 1000 * 8 / 8\times10^6 = 1$ ms
   $Ta = La / vt = 40 * 8 / 8\times10^6 = 0.04$ ms
   Tiempo de propagación
   $Tp = D / vp = 50\times10^3 / 2\times10^8 = 0.25$ ms
   Tiempo de ciclo
   Tc = Tt + Ta + 2*Tp = 1 + 0.04 +2*0.25 = 1.54 ms
   Temporizador
   To > Tc = 1.54 ms, por ejemplo To = 1.8 ms
b) Número medio de transmisiones con SR y $Pb = 10^{-5}$
   $Nt = 1 / (1 – Pb)^{Lt} = 1 / (1 – 10^{-5})^{(1000+40)*8} = 1.087$
   Eficiencia SR
   $E_{SR} = 1 / Nt = 0.92$
c) Ventana óptima
   Wopt = ceil(Tc / Tt) = ceil(1.54 / 1) = ceil(1.54) = 2 PDUs
d) La eficiencia con GBN es 1

1.2.12. Datos: D = 100 km, vt = 10 Mbit/s, $vp = 2\times10^8$ m/s, Lt = 1000 bytes, La = 40 bytes
a) Duración de una PDU y ack
   $Tt = Lt / vt = 1000 * 8 / 10\times10^6 = 0.8$ ms
   $Ta = La / vt = 40 * 8 / 10\times10^6 = 0.032$ ms
   Tiempo de propagación
   $Tp = D / vp = 100\times10^3 / 2\times10^8 = 0.5$ ms
   Tiempo de ciclo
   Tc = Tt + Ta + 2*Tp = 0.8 + 0.032 +2*0.5 = 1.832 ms
   Temporizador
   To > Tc = 1.832 ms, por ejemplo To = 2 ms
b) La eficiencia con SR es 1
c) Número medio de transmisiones con GBN, $Pb = 10^{-5}$ y To = 2.5 ms

$Nt = 1 / (1 - Pb)^{Lt} = 1 / (1 - 10^{-5})^{(1000+40)*8} = 1.087$

Eficiencia GBN

$E_{GBN} = Tt / ((Nt - 1) * To + Tt) = 0.79$

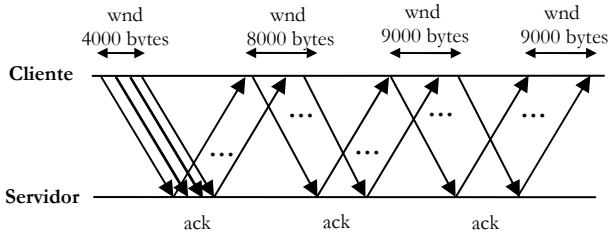
d) Ventana óptima

Wopt = ceil(Tc / Tt) = ceil(1.832 / 0.8) = ceil(2.29) = 3 PDUs

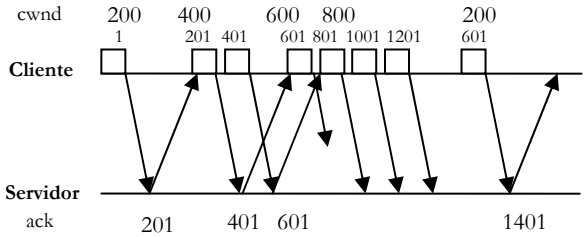
1.3.1. Datos: awnd = 600 bytes, cwnd = 200 bytes, MSS = 100 bytes, ssthresh = 400 bytes

Primer ack, wnd ≤ ssthresh, cwnd = 200 + 100 = 300 bytes, wnd = min(awnd, cwnd) = 300 bytes
Segundo ack, wnd ≤ ssthresh, cwnd = 300 + 100 = 400 bytes, wnd = min(awnd, cwnd) = 400 bytes
Tercer ack, wnd ≤ ssthresh, cwnd = 400 + 100 = 500 bytes, wnd = min(awnd, cwnd) = 500 bytes
Cuarto ack, wnd > ssthresh, cwnd = 500 + 100*100/500 = 520 bytes, wnd = min(awnd, cwnd) = 520 bytes
Quinto ack, wnd > ssthresh, cwnd = 520 + 100*100/520 = 540 bytes, wnd = min(awnd, cwnd) = 540 bytes
Sexto ack, wnd > ssthresh, cwnd = 540 + 100*100/540 = 560 bytes, wnd = min(awnd, cwnd) = 560 bytes

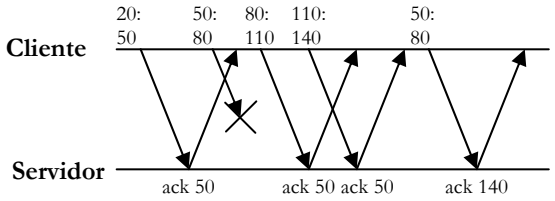
1.3.2. Datos: MSS = 1000 bytes, inicialmente wnd = 4000 bytes, ssthresh = 8000 bytes, awnd = 9000 bytes.



1.3.3. Datos: MSS = 200 bytes



1.3.4. Datos: TCP sack con Slow Start, Congestion Avoidance y Fast Retransmission



1.3.5. Datos: MSS = 1500 bytes, RTT = 10 ms

a) cwnd = 4 MSS = 6000 bytes
b) ssthresh = 10 MSS = 15000 bytes
c) Como la subida es lineal en el tiempo, se habrá usado Congestion Avoidance
d) RTO = 2 * RTO = 20 ms

1.3.6. Datos: MSS = 250 bytes, RTT = 5 ms, RTO = 10 ms.

a) ssthresh = 16 MSS = 4000 byes
b) RTO = 2 * RTO = 20 ms
c) Como la subida es lineal en el tiempo, se habrá usado Congestion Avoidance
d) Ha habido una perdida y se ha vuelto a empezar con cwnd = 1 MSS. Como el ssthresh vale ahora 10 MSS, hasta este valor se usará Slow Start.

1.3.7. Datos: MSS = 500 bytes, RTT = 40 ms, RTO = 50 ms, awnd = 30 MSS

a) Como la subida es lineal en el tiempo, se habrá usado Congestion Avoidance
b) wnd = 20 MSS, siendo wnd = min(awnd, cwnd) = min(30 MSS, cwnd)
cwnd = wnd = 20 MSS = 10000 bytes
c) RTO = 2 * RTO = 100 ms

d) Al tiempo 5 hay una perdida, el nuevo valor de ssthresh es wnd / 2 = 10 MSS.
A partir de cwnd > ssthresh, la ventana debería incrementarse como Congestion Avoidance mientras en la figura se incrementa como si se estuviera aplicando Slow Start.

1.3.8. Datos: MSS = 400 bytes, RTT = 10 ms, RTO = 20 ms.
a) ssthresh = 16 MSS = 6400 byes
b) Como la subida es lineal en el tiempo, se habrá usado Congestion Avoidance
c) RTO = 2 * RTO = 40 ms
d) Ha habido una perdida, ssthresh = wnd / 2 = 10 MSS = 4000 bytes

1.3.9.
a) Debe ser el ack 3279.
b) El extremo que envía datos es el cliente 1160 mientras el servidor 80 envía acks.
c) El cliente está anunciado una awnd de 8192 bytes.

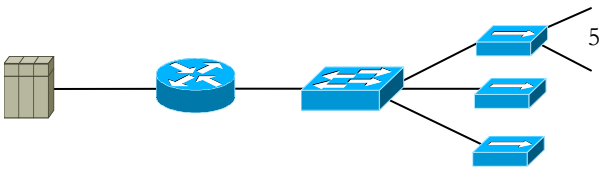
1.3.10. Hay pérdidas y se han perdidos los segmentos 82803 y 83955.

1.3.11.
a) P indica el flag Push, indica al destino que debe leer el buffer rápidamente.
b) En todas las líneas se puede ver que el servidor 80 envía siempre ack 1. Como el valor de este ack no se ha modificado desde el principio, eso quiere decir que el servidor no ha tenido que confirmar ningún dato trasmitido por el cliente y por lo tanto el cliente nunca ha trasmitido datos.
c) No hay pérdidas.
d) Al recibir el ack 72805, el servidor envía en seguida dos segmentos más (se ve que ha sido en seguida por los tiempos). Si entonces el servidor ha enviado hasta el byte 78725 y tiene confirmados hasta el 72805, hay en vuelo exactamente 78725-72805 = 5920 bytes. Por lo tanto la ventana de trasmisión es igual o superior a 5920 bytes.
e) La awnd limita la wnd. De hecho, en las líneas 7 y 8 el cliente anuncia una awnd de 4380 bytes. Con esta ventana awnd el servidor bajará su ventana wnd de los por lo menos 5920 bytes que tenía en las líneas anteriores a los 4380 bytes.

1.3.12.
a) No hay pérdidas.
b) El cliente ha trasmitido 591 bytes.
c) La awnd del servidor es 27890 bytes.
d) MSS = 1460 bytes.
e) SYN_SENT
f) La ventana cwnd del cliente en el punto 3 es de 1 MSS = 1480 bytes
g) La ventana cwnd del servidor en el punto 7 es de 2 MSS = 2920 bytes
h) La conexión está cerrada en el cliente y en el servidor porque hay un flag F 5501 con su ack 5502 y un flag F 592 con su ack 593.

1.3.13.
a) Muy probablemente la captura se ha hecho en el cliente. El cliente tiene una dirección IP privada y el servidor una IP pública. Si se hubiera capturado en el servidor, la dirección privada del cliente no se habría podido ver.
b) Se ha perdido el segmento 71345 y muy probablemente ha actuado el Fast Retransmission porque el servidor vuelve a trasmitir el segmente 71345 al recibir 4 ack duplicados.

1.4.1. La figura muestra la red
a) El switch separa dominios de colisión y el router separa redes e implícitamente también dominios de colisión. Por lo tanto hay 2 redes de las cuales una tiene 4 dominios de colisión. En total hay 5 dominios.
b) Si el switch no tiene capacidad de VLAN, solo se pueden configurar dos LANs.
c) Se pueden configurar 3 VLANs
d) Se pueden conectar 15 hosts a los hubs



1.4.2.
a) Si hay una colision entre tramas Ethernet, ambas estaciones generan un tiempo aleatorio llamado backoff.
b) Al acabar el tiempo de backoff, una estación actuará como cualquier otra estación y por lo tanto no tiene alguna prioridad.
c) Al máximo una trama puede colisionar 16 veces, luego se descarta.
d) No existe el time-out en Ethernet.

1.4.3.

a) Un switch en FDX usa tramas de pausa para hacer control de flujo hacia aquellos dominios que están creando congestión.
b) En WLAN solo se puede comprobar el éxito de una transmisión a través de confirmaciones.
c) Para evitar el problema del terminal escondido, una WLAN en modo infraestructura puede usar el protocolo RTS/CTS. Con este protocolo una estación para poder transmitir una trama debe antes enviar una petición RTS al Access Point (AP) que luego contesta con un paquete CTS con el permiso de transmisión.
d) Se usan 3 direcciones físicas, la MAC de la estación origen, la MAC de la estación destino y la MAC del AP.

1.5.1. Datos: NRZ, BWc = 100 kHz

a) Se cumple el Criterio de Nyquist, siendo vm = 150 kbaud ≤ 2 * BWc = 200 kHz, por lo tanto no hay ISI
b) Capacidad del canal con SNR = 20 dB, teorema de Shannon
$C = BWc * \log_2(1 + SNR) = 100\times10^3 * \log2(1 + 20\ dB) = 10^5 * \log2(1 + 100) = 6.66\times10^5 = 666$ kbit/s
c) Si Tb = 10 μs
vt = 1 / Tb = 100 kbit/s

1.5.2. Datos: D = 40 km, A = 0.4 dB/km, Ps = 1 W, Psens = 10 mW, Pi = 10 mW, G = 20 dB

Atenuación total en 40 km
A = 0.4 dB/km * 40 km = 16 dB
Conversión de dB a lineal
A = 16 dB = 10 dB + 3 dB + 3 dB = 10 * 2 * 2 = 40
Potencia en recepción
Pr = Ps / A = 1 W / 40 = 25 mW
Esta potencia es más alta que la sensibilidad del receptor, no se necesitan amplificadores

1.5.3. Datos: BWc = 100 kHz

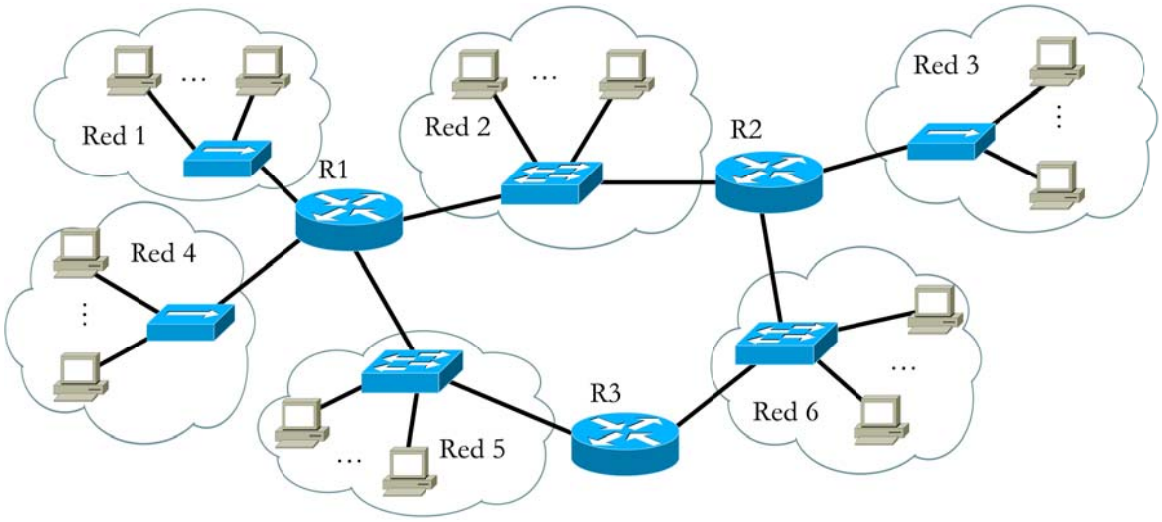
a) Con Manchester y vt = 200 kbit/s
vm = 2 * vt = 400 kbaud
No se cumple el Criterio de Nyquist, siendo vm = 400 kbaud > 2 * BWc = 200 kHz
b) Capacidad del canal con SNR = 25 dB, teorema de Shannon
$C = BWc * \log_2(1 + SNR) = 100\times10^3 * \log2(1 + 25\ dB) = 10^5 * \log2(1 + 316) = 8.31\times10^5 = 831$ kbit/s
c) Con Ts = 8 μs
vm = 1 / Ts = 125 kbaud
Se cumple el Criterio de Nyquist, siendo vm = 125 kbaud ≤ 2 * BWc = 200 kHz
d) Con 8 símbolos se pueden agrupar $n = \log_2 8 = 3$ bits/símbolo
Velocidad de modulación máxima sin distorsión
vm = 2 BWc = 200 kbaud
Velocidad de transmisión
vt = n * vm = 3 bits/símbolo * 200 kbaud = 600 kbit/s

Capítulo 2.
Problemas cortos por tema.

2.1. - Direccionamiento IP

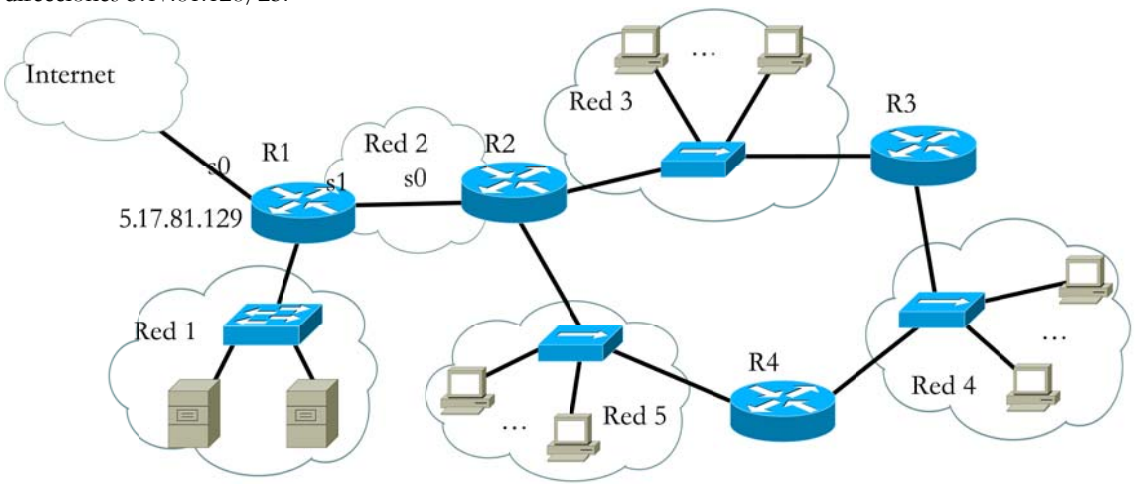
Problema 2.1.1.

Dada la red de la figura, asignar direcciones a las redes a partir del rango 10.0.0.0/24 y sabiendo que cada red tiene como máximo 20 usuarios.



Problema 2.1.2

Se ha montado la red de la figura y se ha conectado a Internet a través de un ISP. El ISP ha proporcionado el rango de direcciones 5.17.81.128/25.



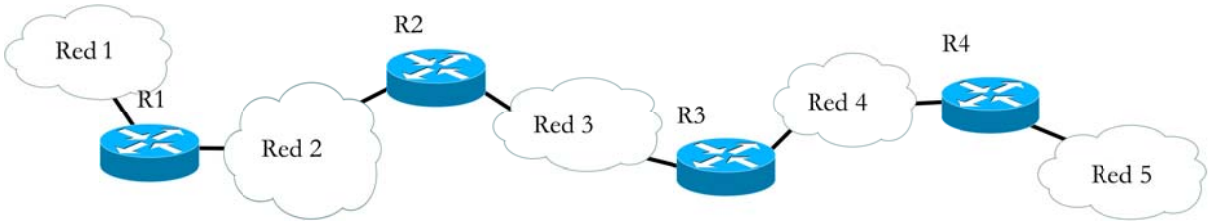
Se pide

a) Asignar direcciones a las redes a partir del rango proporcionado, sabiendo que el router R1 usa la IP 5.17.81.129 para mantener la conexión a Internet y sabiendo que cada red como máximo tendrá estos usuarios:
   - Red 1: 2 servidores
   - Red 2: ningún usuario
   - Red 3: 5 usuarios
   - Red 4: 10 usuarios
   - Red 5: 10 usuarios

b) Suponer ahora que se quieren poner hasta un máximo de 20 usuarios en las redes 4 y 5. Determinar el nuevo direccionamiento.

Problema 2.1.3.

Se ha montado la red privada de la figura.



Se pide

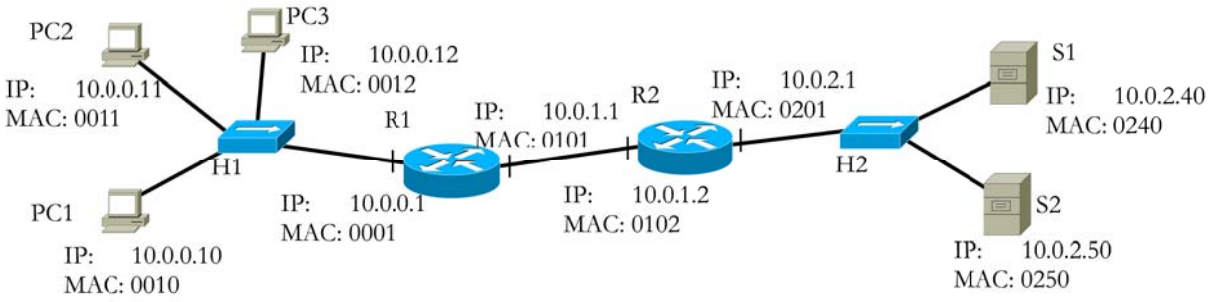
a) Encontrar un direccionamiento valido sabiendo que cada red como máximo tendrá estos usuarios:
   - Red 1: 20 usuarios
   - Red 2: 40 usuarios
   - Red 3: 60 usuarios
   - Red 4: 10 usuarios
   - Red 5: 10 usuarios

b) Suponer ahora que se van a extender las redes 2 y 3 conectando respectivamente un máximo de 200 y 500 usuarios. Recalcular las direcciones IP para todas las redes.

2.2. - ARP

Problema 2.2.1.

Considerar la red de la figura.



a) Se hace un ping del PC1 al S2. Sabiendo que todas las tablas ARP de los hosts y de los routers están vacías y que la dirección MAC de broadcast es :FFFF, indicar toda la información que se envía para que el ping complete por lo menos dos recorridos de ida y vuelta. Usar una tabla del tipo:

Eth		ARP					IP		ICMP
@src	@dst	Query / Response	MAC sender	IP sender	MAC receiver	IP receiver	@src	@dst	Echo RQ/RP

Indicar como quedarían las tablas ARP de los hosts PC1 y S2 y de los routers R1 y R2 usando una tabla del tipo

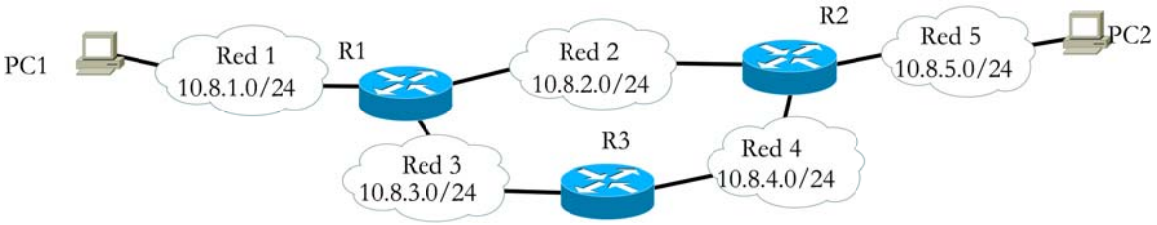
Tabla ARP PC1

IP	MAC

b) Se para el ping anterior pero no se borran las tablas ARP y se hace un ping de PC2 a S1. Indicar la información que se intercambian los hosts y los routers completando las tablas indicadas en el punto a.

Problema 2.2.2.

Se ha montado la red de la figura.



y se han configurado las tablas de encaminamiento indicadas a continuación.

PC1	
red	**gw**
red 1	directa
defecto	R1

R1	
red	**gw**
red 1	directa
red 2	directa
red 3	directa
defecto	R3

R2	
red	**gw**
red 2	directa
red 4	directa
red 5	directa
defecto	R1

R3	
red	**gw**
red 3	directa
red 4	directa
red 5	R1
defecto	R2

PC2	
red	**gw**
red 5	directa
defecto	R2

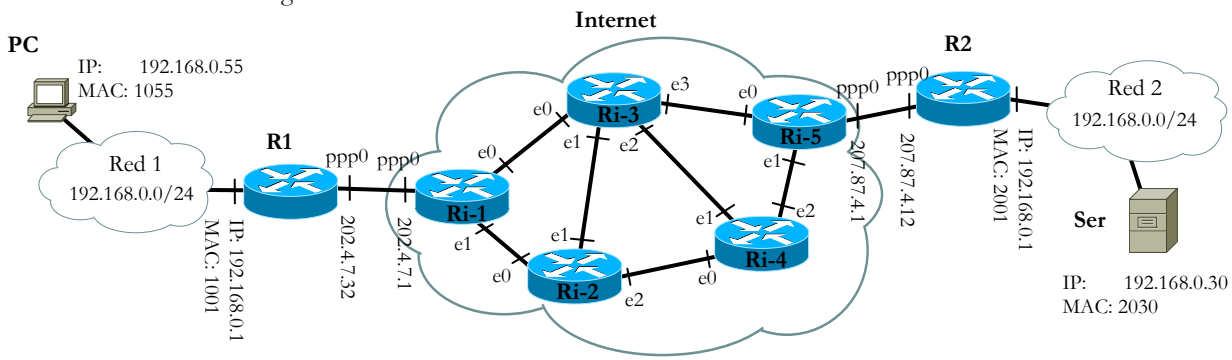
a) Se hace un ping del PC1 al PC2. Inventar las direcciones IP que hacen falta y suponer que las direcciones MAC de las dispositivos sean los últimos dos octetos de la dirección IP (por ejemplo la dirección MAC de 10.8.1.70 es :0170) y que todas las tablas ARP están vacías. La dirección MAC de broadcast se puede indicar como :FFFF. Completar una tabla del tipo del problema anterior poniendo la información que se intercambian hosts y routers para que el ping complete por lo menos un recorrido de ida y vuelta.

b) Si se considera que el ping no ha tenido éxito, comentar la o las razones del problema y deducir las modificaciones necesarias.

c) Una vez resuelto el problema se vuelve a hacer un ping de PC1 a PC2. Usar la tabla del punto a) para indicar la información intercambiada entre hosts y routers para que se complete el recorrido de ida y vuelta de un ping.

Problema 2.2.3.

Se ha montado la red de la figura



Las tarjetas Ethernet de los routers de Internet tienes las siguientes direcciones IP y MAC

Ri-1		
Int	**IP**	**MAC**
e0	8.0.1.1	8100
e1	8.0.2.1	8101

Ri-2		
Int	**IP**	**MAC**
e0	8.0.2.2	8200
e1	8.0.3.1	8201
e2	8.0.4.1	8202

Ri-3		
Int	**IP**	**MAC**
e0	8.0.1.2	8300
e1	8.0.3.2	8301
e2	8.0.5.1	8302
e3	8.0.6.1	8303

Ri-4		
Int	**IP**	**MAC**
e0	8.0.4.2	8400
e1	8.0.5.2	8401
e2	8.0.7.1	8402

Ri-5		
Int	**IP**	**MAC**
e0	8.0.6.2	8500
e1	8.0.7.2	8501

Se hace un ping de PC al Servidor Ser.
Sabiendo que:

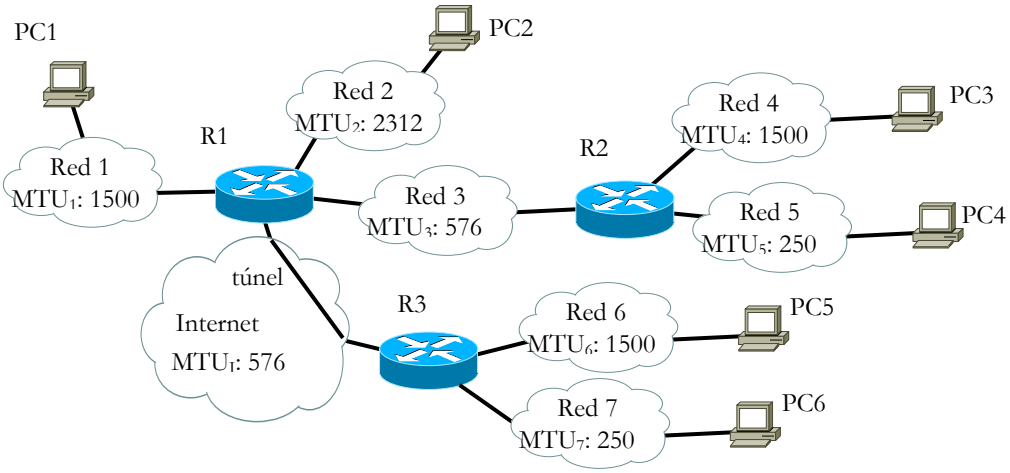
- los paquetes en Internet eligen siempre el camino más cortos (es decir el menor número de saltos)
- en una conexión PPP no existe el concepto de dirección MAC y por lo tanto no hace falta hacer ARP.
- las tablas ARP de PC, Ser, R1 y R2 están vacías
- las tablas de ARP de los routers de Internet ya contienen las MAC de todos los vecinos
- el router R1 aplica un NAT en la interfaz ppp0 para que los datagramas de la red 1 puedan encaminarse por Internet con dirección 202.4.7.25
- el router R2 aplica un NAT en la interfaz ppp0 para que los datagramas de la red 2 puedan encaminarse por Internet con dirección 207.84.4.10

Se pide completar una tabla del tipo mostrada en el primer problema poniendo la información que se intercambian hosts y routers para que el ping complete por lo menos un recorrido de ida y vuelta.

2.3. - Fragmentación

Problema 2.3.1.

Considerar la red de la figura.



a) Suponer que PC1 envía un datagrama de 1500 bytes a PC2 con el flag DF desactivo. Deducir que operación hará el router R1 y que información va a enviar y hacia quien. Si es necesario, hacer uso de la tabla a continuación.

Fragmento	Flag DF	Flag MF	Offset	Total length

b) Suponer que PC1 envía otro datagrama de 1500 bytes a PC2 pero con el flag DF activo. Deducir que operación hará el router R1 y que información va a enviar y hacia quien. Si es necesario, haz uso de la tabla del punto a).

c) Ahora PC2 envía un datagrama de 2312 bytes a PC1 con el flag DF desactivo. Indicar que información recibirá PC1. ¿Y si PC2 enviara otro datagrama con el flag DF activo?

d) PC1 envía un datagrama de 1500 bytes a PC3 con el flag DF desactivo. Deducir los fragmentos que R1 enviará a R2 y los que R2 enviará a PC3 completando unas tablas como las indicadas en el punto a).

e) Como en el punto d) pero el datagrama va directo a PC4.

Sabiendo que los routers R1 y R3 están configurados para hacer tunneling con *IP within IP* y que el router R1 fragmenta los datagramas IP y los reensambla el router R3 al final del túnel, deducir

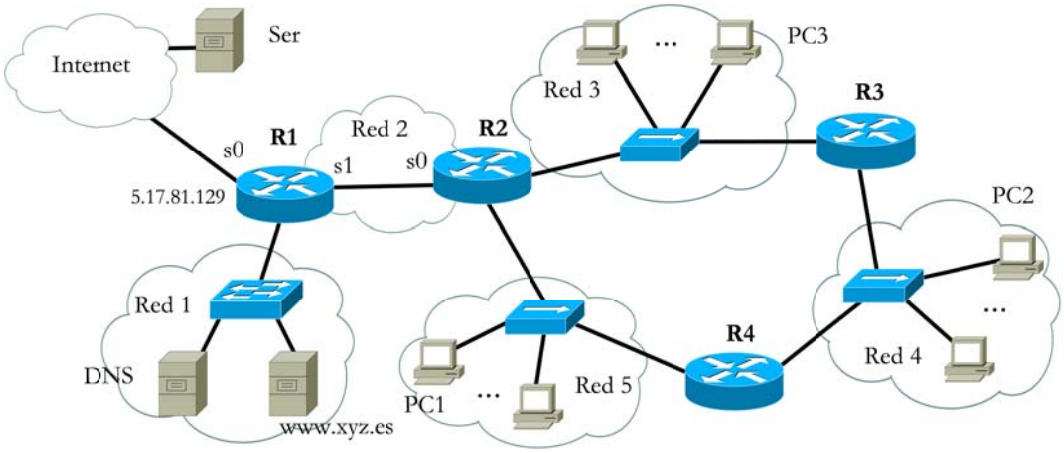
f) los fragmentos que envía R1 en el tunel y los que envía R3 a PC5 si PC1 enviara un datagrama de 1500 bytes.

g) como en el punto f) pero el datagrama va hacia PC6.

2.4. - DHCP y DNS

Problema 2.4.1.

Considerar la red de la figura.



a) Suponiendo que el router R2 sea capaz de proporcionar direcciones IP a través del protocolo DHCP, indicar que mensajes se enviarán para que los hosts PC1 y PC3 obtengan una dirección IP.

b) ¿Puede PC2 obtener una dirección IP como PC1 y PC3? Justificar la respuesta y decir que mecanismos y/o dispositivos habría que usar o añadir para conseguirlo.

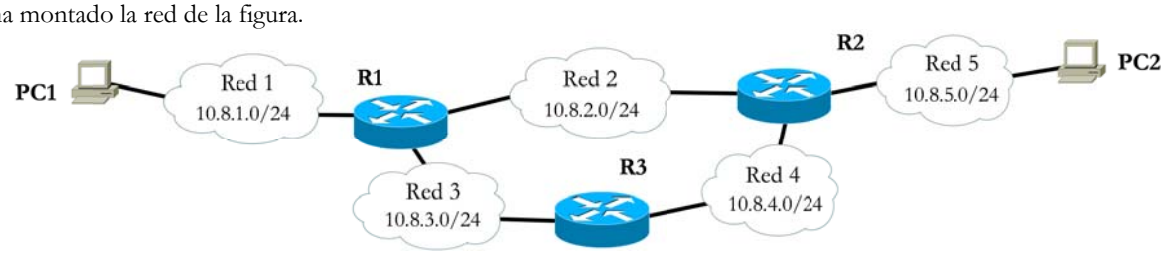
c) PC3 quiere consultar la web de la empresa XYZ. Sabiendo que PC3 tiene configurado el servidor de la empresa DNS para la resolución de los nombres, indicar que mensajes se enviarán para estos casos
   (i) PC3 tiene en su caché la resolución del nombre.
   (ii) PC3 no tiene la resolución del nombre, mientras el servidor DNS tiene resuelto el nombre.

d) PC3 quiere consultar el servidor Ser. Sabiendo que PC3 tiene configurado el servidor de la empresa DNS para la resolución de los nombres, indicar que mensajes se enviarán para estos casos
   (i) PC3 tiene en su caché la resolución del nombre.
   (ii) PC3 no tiene la resolución del nombre, mientras el servidor DNS tiene resuelto el nombre.
   (iii) Ni PC3, ni el servidor DNS de la empresa tienen la resolución del nombre.

2.5. - RIP

Problema 2.5.1.

Se ha montado la red de la figura.



Se han configurado las tablas de encaminamiento en los dos PCs como mostrado a continuación

PC1	
red	**gw**
red 1	directa
defecto	R1

PC2	
red	**gw**
red 5	directa
defecto	R2

y se ha activado el RIPv1 sin *split horizon* en los routers.

a) Suponiendo que hayan transcurrido 30 segundos desde la activación del RIPv1, indicar los mensajes que se han intercambian los routers (suponiendo que lo han hecho todos a la vez) y como quedan las tablas de encaminamiento de los routers completando las tablas a continuación.

Mensajes RIPv1

R1->R2	
red	**hop**

R1->R3	
red	**Hop**

R2->R1	
red	**hop**

R2->R3	
red	**hop**

R3->R1	
red	**hop**

R3->R2	
red	**hop**

Tablas de encaminamiento

R1		
red	**gw**	**hop**

R2		
red	**gw**	**hop**

R3		
red	**gw**	**hop**

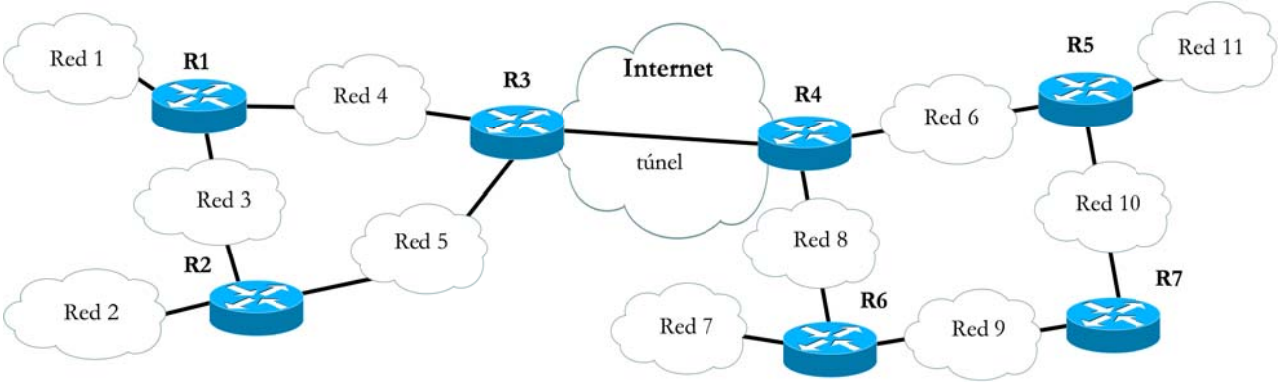
b) Suponiendo que han transcurrido otros 30 segundos, indicar cómo quedan ahora las tablas de encaminamiento.

c) ¿Cómo cambiaría el punto a) si se hubiera activado el split horizon?

d) Suponiendo ahora que se activa el RIPv2 con split horizon, repetir el punto a). Indicar bien cual serian ahora los mensajes intercambiados entre los routers.

Problema 2.5.2.

Se ha montado la red de la figura y se ha activado el RIP con *split horizon*, *poison revers* y *triggered update* en los routers.



a) Escribir la tabla de encaminamiento de los routers R1, R3, R5 y R7. Usar una tabla del tipo mostrada a continuación.

R1		
Red	**gw**	**hop**

R3		
red	**gw**	**hop**

R5		
red	**gw**	**hop**

R7		
red	**gw**	**hop**

b) Escribir el mensaje que cada 30 segundos el router R2 envía a R3, el que envía R6 a R7 y el que envía R4 a R3. Usar una tabla del tipo mostrada a continuación.

R2 -> R3	
red	**hop**

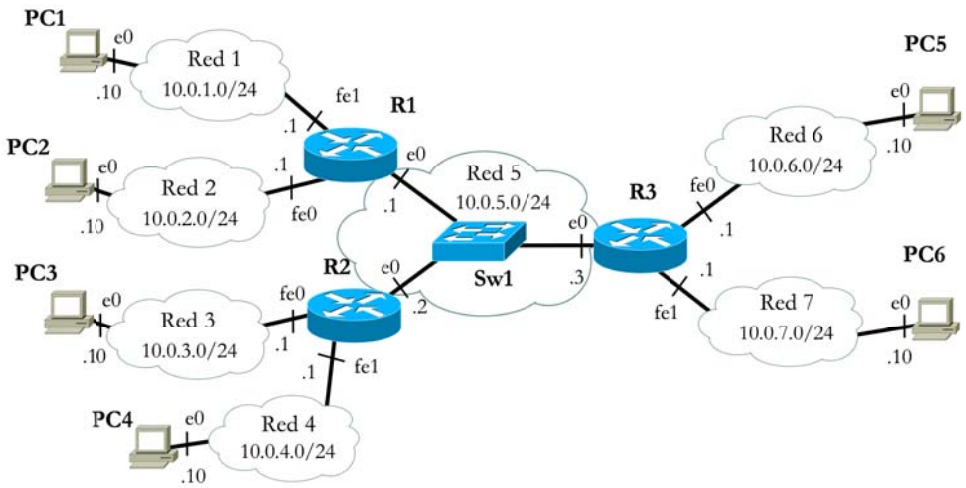
R6 -> R7	
red	**hop**

R4 -> R3	
red	**hop**

c) Suponer ahora que cae la red 6. Escribir los mensajes que enviarían los router R4 y R5 indicando, además del contenido de los mensajes, también hacia quien los envían. Haz uso de tablas del tipo mostradas en el punto b).

Problema 2.5.3.

Disponemos de la red de la figura. Los números del tipo .X indican la parte hostID de la dirección IP de la interfaz, la parte netID es fácilmente deducible por la dirección de red. Los routers usan RIPv2.



a) Escribir la tabla de encaminamiento de R1 (donde protocolo indica si la entrada es "S" estática, "R" por RIP o "C" directamente conectada). Usar una tabla del tipo mostrada a continuación.

Protocolo	Red/mascara	Gateway	Interfaz	Métrica

b) Indica que mensajes de encaminamiento enviaría el router R1 a R3 si se usa
   (i) split horizon
   (ii) no usa split horizon
   Completar por cada punto una tabla del tipo mostrada a continuación.

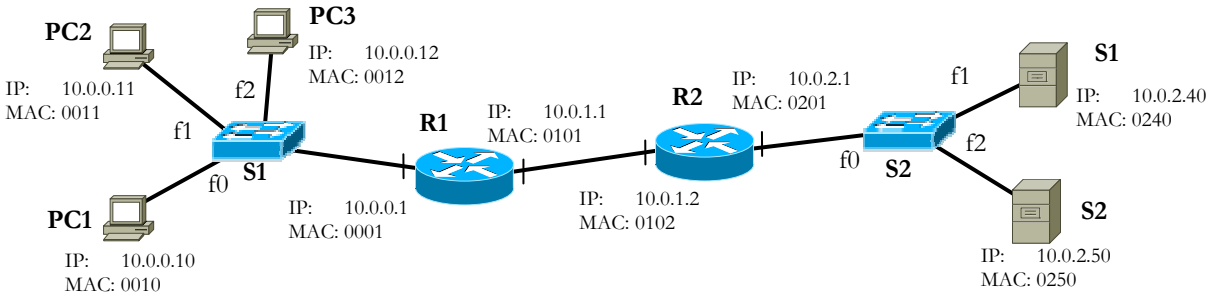
Red	Mascara	Métrica

c) Suponer ahora que el enlace entre R3 y la red 6 cae. Indicar que informaciones se intercambiarían R1 y R3 si
   (i) no se usa split horizon, poison reverse y triggered update
   (ii) se usa split horizon pero no poison reverse ni triggered update
   (iii) se usa split horizon, poison reverse y triggered update
   Completa por cada punto una tabla del tipo mostrada en el punto b).

2.6. - Switch

Problema 2.6.1.

Considerar la red de la figura.



a) Se hace un ping del PC1 al S2. Sabiendo que todas las tablas ARP de los hosts y de los routers están vacías y que la dirección MAC de broadcast es :FFFF, indicar toda la información que se envía para que el ping complete por lo menos dos recorridos de ida y vuelta. Usar una tabla del tipo:

Eth		**ARP**					**IP**		**ICMP**
@src	@dst	Query / Response	MAC sender	IP sender	MAC receiver	IP receiver	@src	@dst	Echo RQ/RP

Indicar como quedarían las tablas ARP de los hosts PC1 y S2 y de los routers R1 y R2 usando una tabla del tipo

Tabla ARP PC1

IP	MAC

b) Sabiendo que las tablas ARP no se han borrado después de ejecutar el punto a. se vuelve a hacer un ping del PC1 al S2. Indicar la información que se intercambian los hosts y los routers completando una tabla del tipo indicado en el punto a). Indicar también cual sería la tabla MAC del switch usando el formato

Tabla MAC switch

Puerto	MAC

c) Se para el ping anterior pero no se borran las tablas ARP y se hace un ping de PC2 a S1. Indicar la información que se intercambian los hosts y los routers completando una tabla del tipo indicado en el punto a). Indicar también cual sería la tabla MAC del switch usando el formato

Tabla MAC switch

Puerto	MAC

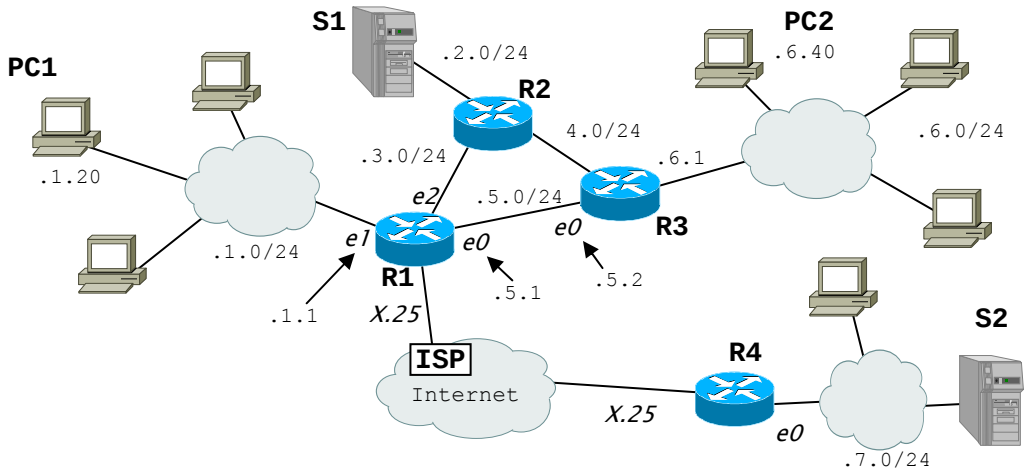
2.7. - Soluciones

Capítulo 3.
Problemas largos.

3.1. - Redes IP, protocolos ARQ y TCP/UDP

Problema 3.1.1.

Se dispone de la red de la figura. Toda la red es Ethernet excepto la conexión a Internet que usa X.25. Las IP de las redes tienen forma 10.0.X.0/24 con X = 1,2,…, 7.



a) Los routers R1, R2 y R3 tienen RIPv1 activo. Escribir la tabla de encaminamiento de R1 donde protocolo indica si la entrada es S estática, R por RIP o C directamente conectada. Usar una tabla del tipo:

Protocolo	Red/Mascara	Gateway	Interfaz	Métrica

b) Los routers R1 y R4 están configurados para hacer tunneling. La MTU de las redes ethernet es 1500 bytes y la del enlace X.25 es de 576 bytes. Suponer que PC1 envía un datagrama IP de 1500 bytes al servidor S2 con el flag DF desactivado. El router R1 fragmenta los datagramas IP y los reensambla el router R4. Deducir los flags DF y MF, los campos offset y total length de los fragmentos IP que envía R1. Usar una tabla del tipo:

Fragmento	Flag DF	Flag MF	Offset	Total length

c) Si se hace un ping del PC1 con IP 10.0.1.20 al PC2 con IP 10.0.6.40, indicar que paquetes se envían. Suponer que las tablas ARP están vacías excepto R1 que ya conoce la MAC de la interfaz e0 de R3 y viceversa. Las direcciones MAC de las maquinas se indican con el los últimos dos octetos de la dirección IP (por ejemplo la dirección MAC del host 10.0.1.20 es :0120). Indicar la dirección MAC de broadcast como :FFFF. Usar una tabla del tipo:

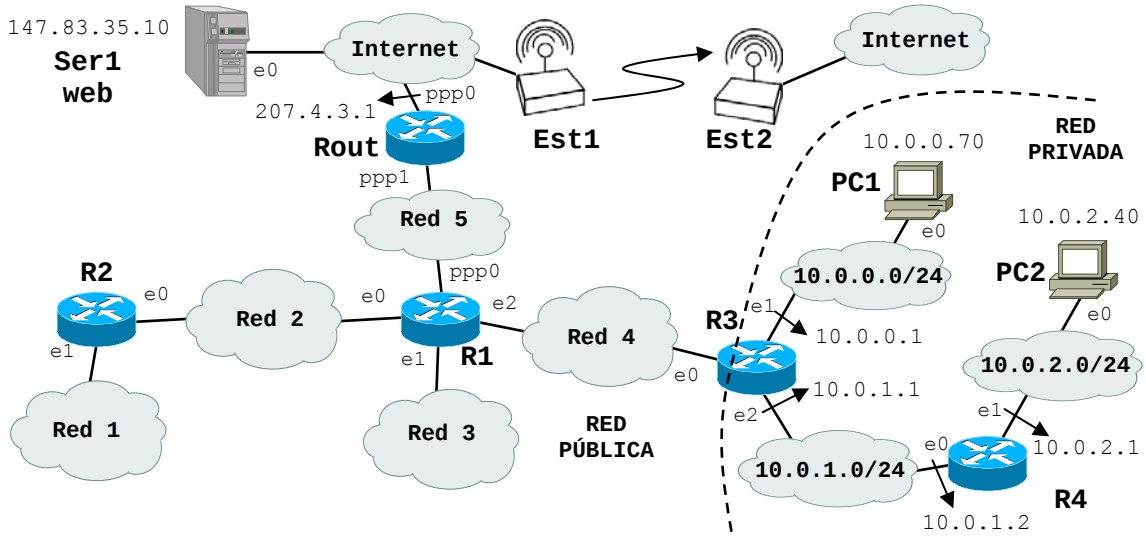
Eth		ARP					IP		ICMP
@src	@dst	Query / Response	MAC sender	IP sender	MAC receiver	IP receiver	@src	@dst	Echo RQ/RP

Problema 3.1.2.

Se dispone de la red de la figura compuesta por una parte privada y una parte pública. Para la red pública se usan direcciones IP tomadas del rango 207.4.3.0/24 proporcionado por el ISP. El número de usuarios de cada una de las 5 redes que forman la red pública es el siguiente:

- Red 1: 25 usuarios, Red 2: 10 usuarios, Red 3: 20 usuarios, Red 4: 10 usuarios, Red 5 ningún usuario

El router de conexión a Internet Rout tiene asignada la dirección IP 207.4.3.1 tomada del rango 207.4.3.0/24.



a) Diseñar un esquema de direccionamiento para la red pública. Se puede elegir entre mascaras fijas o variables. Indicar claramente de cada subred la máscara, la dirección de red, la dirección de broadcast, el número de direcciones IP disponibles y cuantas quedan libres después de asignar las IP a los usuarios y a los routers.

b) Se hace un ping del PC1 al PC2. Suponer que las direcciones MAC de las maquinas se indican con los últimos dos octetos de la dirección IP (por ejemplo la dirección MAC de 10.0.1.70 es :0170) y que las tablas ARP de PC1 y R3 están vacías, mientras las de R4 y PC2 contienen las siguientes entradas.

Tabla ARP R4

@IP	@MAC
10.0.2.40	:0240

Tabla ARP PC2

@IP	@MAC
10.0.2.1	:0201

Indicar la dirección MAC de broadcast como :FFFF. Indicar la información que se envía completando una tabla del tipo del Problema 3.1.1, Pregunta c).

c) Indicar a cual router hay que aplicar un NAT dinámico por puertos (4000-4100) para que el usuario del PC1 pueda conectarse al servidor web de Internet Ser1. Sabiendo que la aplicación cliente usa el puerto 1064, indicar cual sería la conversión IP/puertos en el router completando una tabla del tipo:

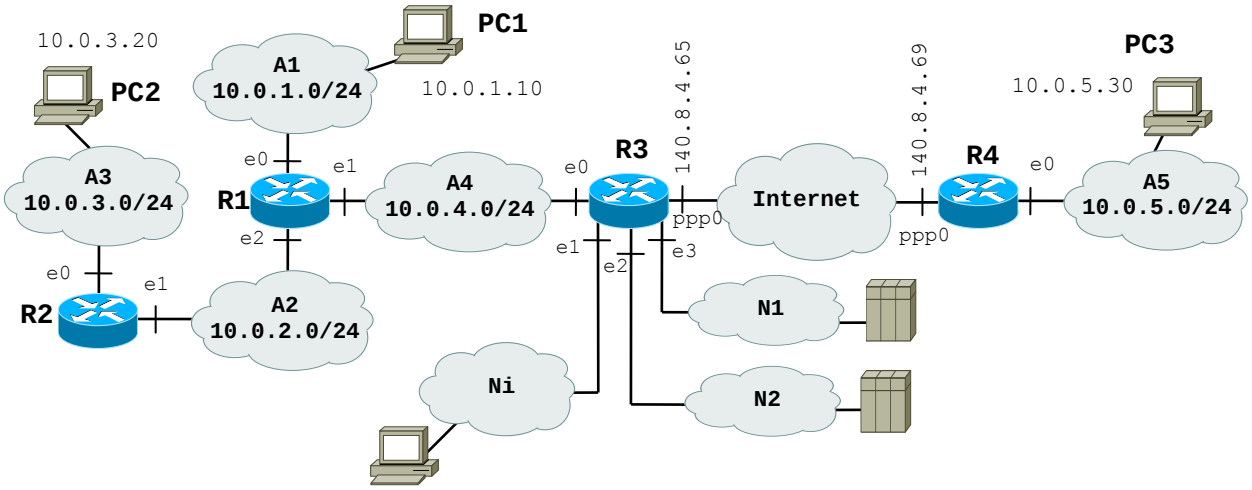
			IP		Puerto		Web
Dirección		Interfaz	Origen	Destino	Origen	Destino	Petición/Servicio
Ida	Entrada						
	Salida						
Vuelta	Entrada						
	Salida						

d) Para interconectar dos partes lejanas de Internet se usa una conexión inalámbrica entre las estaciones Est1 y Est2. Estas dos estaciones usan un protocolo ARQ de retransmisión selectiva a 10 Mbit/s. La distancia entre las estaciones es de 1000 km y la velocidad de propagación de 2×10^8 m/s. La longitud de las PDUs es de 1500 bytes mientras los acks son de 20 bytes. Hay que determinar:

(i) la ventana óptima Wopt de este sistema
(ii) diseñar el tiempo de time-out calculado como el 50% más de la ventana óptima
(iii) determinar cuál debería ser la probabilidad de error en el bit Pb para tener una eficiencia del sistema superior al 95%.

Problema 3.1.3.

Se dispone de la red de la figura compuesta por una parte privada y una parte pública. La parte privada usa un túnel en Internet entre los routers R3 y R4 para conectar dos partes distintas. Las direcciones de los extremos del túnel son 140.8.4.65/30 y 140.8.4.69/30. La parte pública consiste de dos redes para servidores públicos N1 y N2 y de varias redes de hosts públicos Ni; al máximo hay **5 servidores** en las redes N1 y N2, mientras no hay un límite al número de hosts para las redes Ni. Para la parte pública se usan direcciones IP tomadas del rango 140.8.4.0/26.



a) Diseñar un esquema de direccionamiento para la red pública. En particular se pide en este orden:
   (i) Determinar la **máscara** fija que mejor se ajuste a los requisitos de las redes de servidores públicos N1 y N2 (se recuerda que al máximo hay 5 servidores para cada red).
   (ii) Determinar **el número total de subredes** creadas con la máscara anterior.
   (iii) Determinar cuántas **subredes de hosts públicos** se han creado con la máscara anterior.
   (iv) Determinar **el número total de direcciones IP** que se pueden asignar a las subredes de los hosts públicos.
   (v) Ahora se quiere que las redes de hosts sean solo dos (N3 y N4), determinar **las máscaras** que mejor se ajusten para tener un número máximo de direcciones IP (nota que las dos redes pueden tener mascara distinta).

b) Toda la red (privada y pública) usa RIPv2. Escribir la tabla de encaminamiento del router R2 con el formato indicado. Indicar en la columna adquisición una ruta directa con C, determinada por RIP con R y una estática con S. En la columna Red/mascara se recomienda usar los nombres de las redes y no sus direcciones IP (por ejemplo A1/24 en lugar de 10.0.1.0/24). En la columna Gateway indicar la dirección del router como router-interfaz (por ejemplo R3-e2 para la interfaz e2 del router R3). En la columna Interfaz indicar la interfaz de salida del router R4.

Adquisición	Red/mascara	Gateway	Interfaz	Métrica

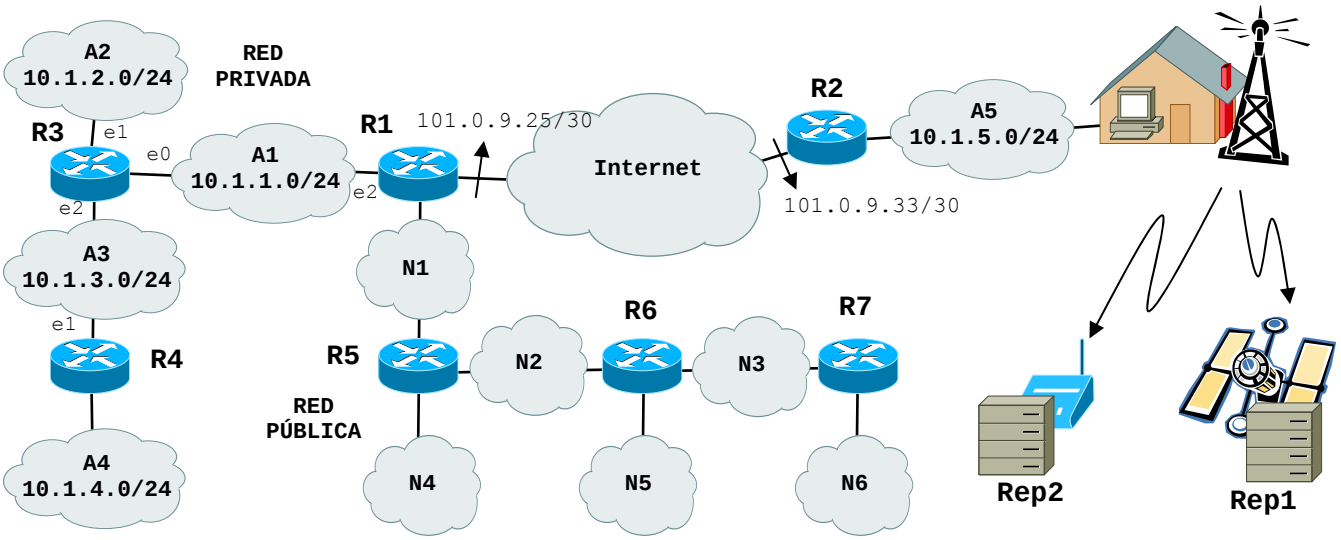
c) Se hace un ping del PC2 al PC1. Inventar las direcciones IP de los routers. Suponer que las direcciones MAC de los hosts/routers se indican con los últimos dos octetos de la dirección IP (por ejemplo la dirección MAC de 10.0.1.70 es :0170) y que todas las tablas ARP están vacías. Indicar la dirección MAC de broadcast como :FFFF. Indicar la información que se envía completando una tabla como la del Problema 3.1.1, Pregunta c):

Eth		ARP					IP		ICMP
@src	@dst	Query / Response	MAC sender	IP sender	MAC receiver	IP receiver	@src	@dst	Echo RQ/RP

d) Suponer que PC1 de la red A1 accede a PC3 de la red A5. Escribir las direcciones origen y destino de los datagramas IP cuando estos pasan por
   (i) La interfaz e0 de R3
   (ii) La interfaz ppp0 de R3
   (iii) La interfaz ppp0 de R4
   (iv) La interfaz e0 de R4

Problema 3.1.4.

Una empresa dispone de la red de la figura compuesta por una parte privada y una parte pública. La parte pública consiste de 6 redes: N1, N2, N3, N4, N5 y N6. La parte privada se compone de 5 redes: A1, A2, A3, A4 y A5. La red A5 está situada en la casa del propietario de la empresa y se conecta a las otras con una VPN a través de un túnel en Internet entre los routers R1 y R2. Las direcciones de los extremos del túnel son 101.0.9.25/30 y 101.0.9.33/30, respectivamente. El propietario también tiene acceso inalámbrico a dos repositorios de datos Rep1 y Rep2.



a) Para la red pública, el ISP ofrece dos rangos de direcciones públicas: el 202.4.4.128/25 y el 212.6.6.0/24. Diseñar un esquema de direccionamiento para las 6 redes públicas sabiendo que:
   - cada red pública tendrá al máximo **10** hosts y
   - se quiere contratar un **único** rango de direcciones, el que mejor se ajusta a los requisitos de la empresa.

b) Se quiere activar el RIP en toda la red (privada y pública) para que los routers configuren automáticamente las tablas de encaminamiento. Se pide:
   (i) Deducir si hay que usar el RIPv2 o ya es suficiente el RIPv1.
   (ii) Escribir la tabla de encaminamiento de R3 usando el formato indicado en el Problema 3.1.3, Pregunta b).

c) Suponer ahora que hay un fallo en la red A3 y esta se desconecta del router R3. Sabiendo que están activos Split-horizon, Poison Reverse y Triggered Update, deducir el mensaje RIP que envía R3 a R1 usando el formato indicado.

Red	Mascara	Métrica

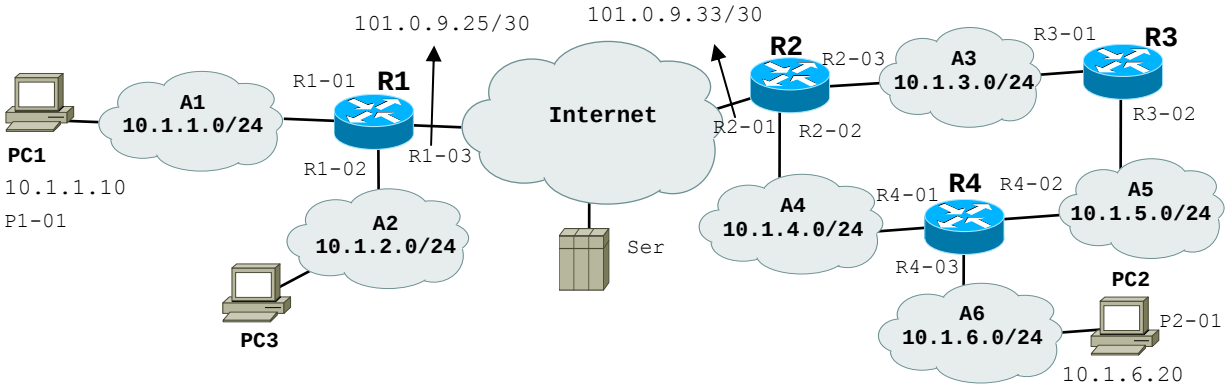
d) El propietario quiere saber que hacen los router R2 y R1 con los datagramas que su host de casa envía a la red de la empresa. Sabiendo que el túnel entre R2 y R1 usa una tecnología con una MTU de 400 bytes y que la MTU de todas las redes Ai es de 1500 bytes, determinar:
   (i) el tamaño que deben tener los datagramas del host de casa para que el router R2 no necesite fragmentar
   (ii) indicar que mecanismo se podría usar en el host para determinar este valor

e) Para intercambiar datos con los dos repositorios, el host de la casa usa unos protocolos ARQ. En particular
   - Entre **Rep1** y el **host** se usa un protocolo **Go-back-N**, la distancia es de 36000 km, la longitud de las PDUs de 1500 bytes, la velocidad de transmisión de 50 kbit/s, el temporizador de 1 s y la probabilidad de error en un bit de 10^{-5}.
   - Entre **Rep2** y el **host** se usa un protocolo **Stop&Wait**, la longitud de las PDUs es de 500 bytes, la velocidad de transmisión de 6 Mbit/s y la probabilidad de error de este sistema es nula.

   Sabiendo que la velocidad de propagación en los dos casos es de 2×10^{-8} m/s, se pide:
   (i) Calcular la eficiencia del sistema Rep1-host.
   (ii) Calcular la distancia que debería haber entre Rep2-host para que este segundo sistema tenga la misma eficiencia del primero.

Problema 3.1.5.

Una empresa dispone de la red privada de la figura. Una VPN conecta las dos partes a través de un túnel en Internet entre los routers R1 y R2. Las direcciones de los extremos del túnel son 101.0.9.25/30 y 101.0.9.33/30, respectivamente. Los routers R1 y R2 tienen activado un PAT para poder traducir las direcciones privadas a públicas.



a) PC1 hace un ping a PC2. Completar una tabla como la del Problema 3.1.1, Pregunta c) indicando todos los mensajes que se intercambian los routers y los hosts para que el ping complete un recorrido de ida y vuelta. Tener en cuenta lo siguiente:
- Todas las tablas ARP están vacías.
- Hay un túnel entre R1 y R2. Entre estos no se necesita descubrir las direcciones físicas de las interfaces.
- Los routers usan RIPv2 así que las rutas son las de números de saltos mínimos.
- Inventarse las direcciones IP que faltan.
- Las direcciones físicas están indicadas en la figura como P1-01, R1-01, R4-03, etc. Usar FF-FF para la dirección física de broadcast.

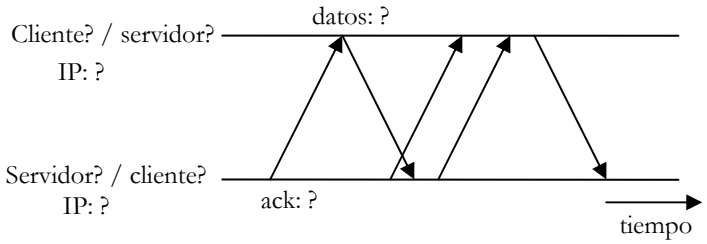
b) PC3 de la figura anterior ha abierto una conexión con el servidor Ser disponible en Internet. Se ha capturado la siguiente traza:

```
17:01:15.9887  10.1.2.20.3413 > 147.3.4.7.22  S 736252:736252(0) win 8192 <mss 1024>
17:01:16.1901  147.3.4.7.22 > 10.1.2.20.3413  S 2514272:2514272(0) ack 736253 win 4096 <mss 1024>
17:01:16:1906  10.1.2.20.3413 > 147.3.4.7.22  ack 1 win 8192
17:01:22:0918  10.1.2.20.3413 > 147.3.4.7.22  P 1:1025(1024) ack 1 win 8192
17:01:22:2901  147.3.4.7.22 > 10.1.2.20.3413  ack 1025 win 4096
17:01:22:2905  10.1.2.20.3413 > 147.3.4.7.22  . 1025:2049(1024) ack 1 win 8192
17:01:22:2951  10.1.2.20.3413 > 147.3.4.7.22  . 2049:3073(1024) ack 1 win 8192
17:01:22:5001  147.3.4.7.22 > 10.1.2.20.3413  ack 2049 win 4096
17:01:22:5060  147.3.4.7.22 > 10.1.2.20.3413  ack 3073 win 4096
17:01:22:5070  10.1.2.20.3413 > 147.3.4.7.22  . 3073:4097(1024) ack 1 win 8192
17:01:22:5081  10.1.2.20.3413 > 147.3.4.7.22  . 4097:5121(1024) ack 1 win 8192
17:01:22:5088  10.1.2.20.3413 > 147.3.4.7.22  . 5121:6145(1024) ack 1 win 8192
17:01:22:5096  10.1.2.20.3413 > 147.3.4.7.22  . 6145:7169(1024) ack 1 win 8192
17:01:22:6991  147.3.4.7.22 > 10.1.2.20.3413  ack 4097 win 4096
17:01:22:7012  147.3.4.7.22 > 10.1.2.20.3413  ack 5121 win 4096
17:01:22:7033  147.3.4.7.22 > 10.1.2.20.3413  ack 6145 win 4096
17:01:22:7063  10.1.2.20.3413 > 147.3.4.7.22  . 7169:8193(1024) ack 1 win 8192
17:01:22:7065  147.3.4.7.22 > 10.1.2.20.3413  ack 7169 win 4096
17:01:22:7088  10.1.2.20.3413 > 147.3.4.7.22  . 8193:9217(1024) ack 1 win 8192
17:01:22:7095  10.1.2.20.3413 > 147.3.4.7.22  . 9217:10241(1024) ack 1 win 8192
17:01:22:7106  10.1.2.20.3413 > 147.3.4.7.22  . 10241:11265(1024) ack 1 win 8192
17:01:22:9245  147.3.4.7.22 > 10.1.2.20.3413  ack 8193 win 4096
17:01:22:9251  147.3.4.7.22 > 10.1.2.20.3413  ack 9217 win 4096
17:01:22:9267  147.3.4.7.22 > 10.1.2.20.3413  ack 10241 win 4096
17:01:22:9279  147.3.4.7.22 > 10.1.2.20.3413  ack 11265 win 4096
17:01:22:9280  10.1.2.20.3413 > 147.3.4.7.22  . 11265:12289(1024) ack 1 win 8192
17:01:22:9288  10.1.2.20.3413 > 147.3.4.7.22  . 12289:13313(1024) ack 1 win 8192
17:01:22:9295  10.1.2.20.3413 > 147.3.4.7.22  . 13313:14337(1024) ack 1 win 8192
17:01:22:9301  10.1.2.20.3413 > 147.3.4.7.22  . 14337:15361(1024) ack 1 win 8192
17:01:23:1199  147.3.4.7.22 > 10.1.2.20.3413  ack 12289 win 4096
...
```

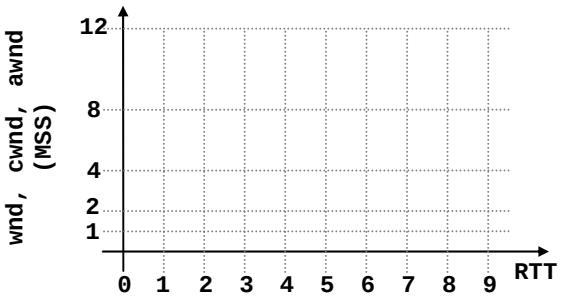
Sabiendo que el tiempo de propagación entre cliente y servidor es de 10 ms, se pide deducir:
(i) la dirección IP y el puerto del cliente y del servidor,
(ii) el tamaño de los buffers de recepción de cliente y servidor,
(iii) el MSS de los datos.

c) Deducir si la traza se ha capturado en el servidor o en el cliente. Motivar la respuesta. Conociendo la configuración de la red de la figura, deducir si hubiera cambiado algo en las direcciones IP del cliente o del servidor si la captura se hubiera hecho en el otro extremo.

d) Transcribir el intercambio de mensajes entre cliente y servidor en un diagrama de tiempo como el ilustrado en la figura a continuación.



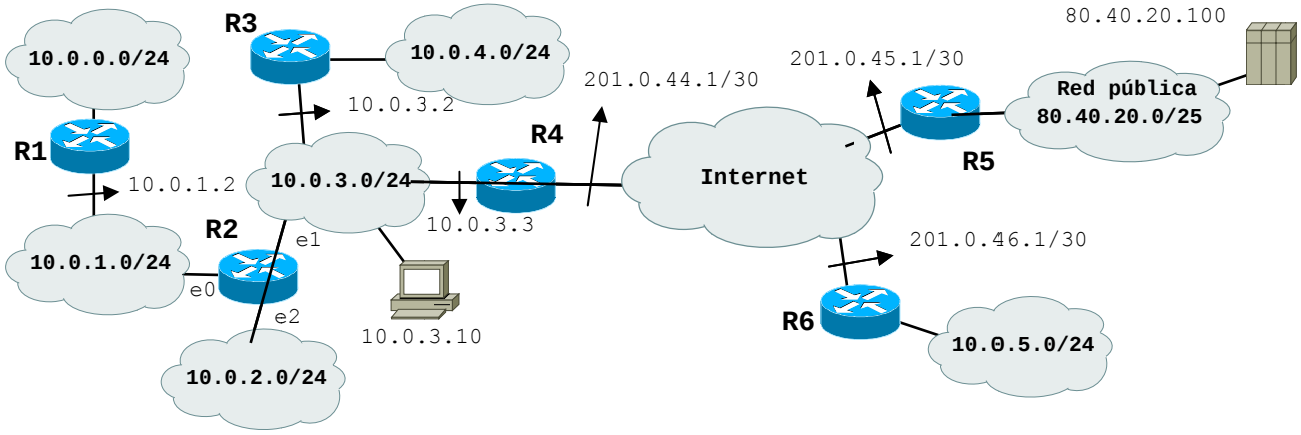
e) Dibujar la evolución de la ventana de transmisión, de congestión y anunciada en un grafico en función de los round-trip time (RTT) como el ilustrado a continuación.



f) Determinar la velocidad efectiva de la transmisión una vez alcanzado un régimen estacionario. Suponer la velocidad de los enlaces infinitamente grande.

Problema 3.1.6.

Una empresa dispone de la red de la figura. Una VPN conecta la sede central de la izquierda con las dos sedes remotas de la derecha a través de dos túneles en Internet entre los routers R4 y R5 y entre R4 y R6. Las direcciones de los extremos del túnel son 201.0.44.1/30, 201.0.45.1/30 y 201.0.46.1/30. La sede remota que corresponde al router R5 tiene asignado un rango de direcciones publicas 80.40.20.0/25.



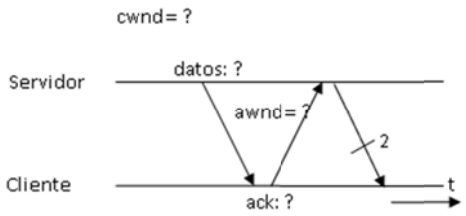
a) Sabiendo que en la red pública de la sede remota se quieren configurar 5 redes diferentes con estos requisitos:
- 3 redes, cada una con un mínimo de 25 direcciones IP
- 2 redes, cada una con un mínimo de 10 direcciones IP

Determinar un direccionamiento valido.

b) Sabiendo que se ha activado RIPv2 en todos los routers, determinar la tabla de encaminamiento del router R2. En la tabla indicar las columnas IP destino, mascara, Gateway, interfaz y métrica. La red pública indicarla simplemente como 80.40.20.0/25.

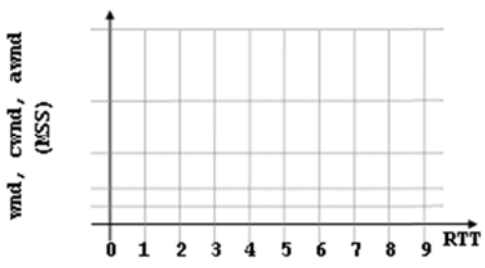
c) El PC 10.0.3.10 se conecta al servidor 80.40.20.100 para bajarse una página web. La conexión se establece con estos parámetros:
- el tiempo de propagación entre cliente y servidor es de 50 ms,
- el tamaño del buffer de recepción del PC es de 8192 bytes, el tamaño de los otros buffers se aproxima a infinito,
- el MSS es de 512 bytes

Se pide dibujar el intercambio de información entre cliente y servidor *a partir del primer segmento de datos enviado por el servidor* y *hasta 600 ms* en un diagrama de tiempo como el ilustrado en la figura.



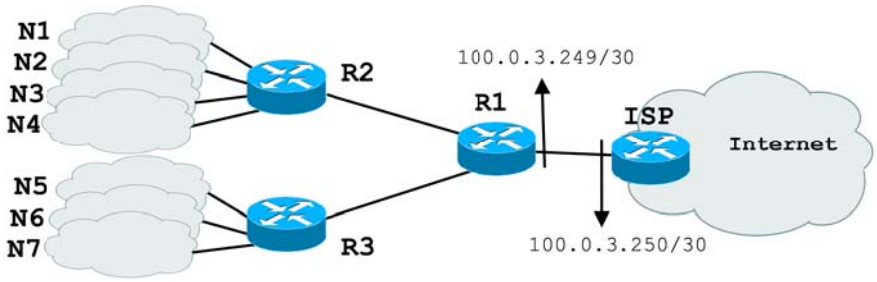
d) Determinar la velocidad efectiva de la transmisión una vez alcanzado un régimen estacionario. Suponer la velocidad de los enlaces infinitamente grande.

e) Suponer que, una vez alcanzado el régimen estacionario, hay una perdida. Dibujar la evolución de la ventana de transmisión, de congestión, anunciada y el umbral ssthresh en un gráfico en función de los round-trip time (RTT) como el ilustrado en la figura. Considerar el RTO igual a dos veces el RTT.



Problema 3.1.7.

Una empresa obtiene de un ISP el rango de direcciones públicas 100.0.0.0/22. De este rango, la dirección de red 100.0.3.248/30 se reserva para la conexión entre R1 y el ISP.



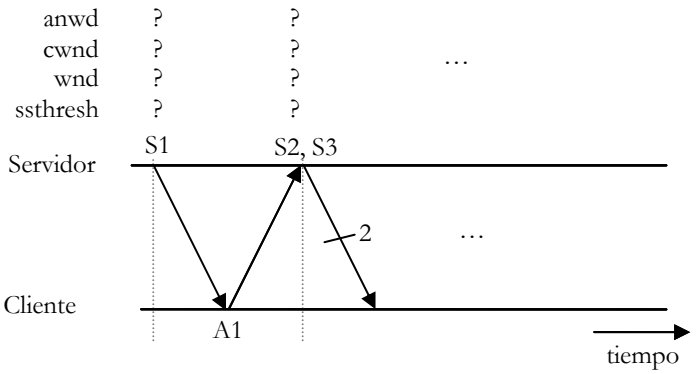
a) Con las direcciones restantes, la empresa quiere configurar 7 redes con hosts públicos y 2 redes de interconexión entre routers (R1-R2 y R1-R3). Los requerimientos de estas redes son los siguientes:
- 2 redes (N1 y N2) tienen 180 hosts cada una.
- 2 redes (N3 y N4) tienen 20 hosts cada una.
- 3 redes (N5, N6 y N7) tienen 90 hosts cada una.
- 2 redes de interconexión R1-R2 y R1-R3.

Encontrar un direccionamiento valido para esta empresa.

b) Dos puntos de conexión distantes 400 km se comunican a través de un protocolo ARQ a 1 Mbit/s. Las PDUs son de 220 bytes mientras las confirmaciones de 20 bytes. Sabiendo que la velocidad de propagación es de $2 \cdot 10^8$ m/s, determinar
   (i) La eficiencia del sistema si se usara Stop&Wait, Go-back-N o Retrasmisión selectiva.
   (ii) El valor de la ventana óptima.
   (iii) El valor del temporizador.

c) Suponer ahora que se ha elegido el Go-back-N como protocolo ARQ y que el sistema tiene una probabilidad de error en un bit de $3 \cdot 10^{-5}$. Suponiendo que el valor del temporizador es el mínimo posible, determinar
   (i) La eficiencia.
   (ii) A qué distancia deberían estar los dos puntos para asegurar una eficiencia de 0.9.

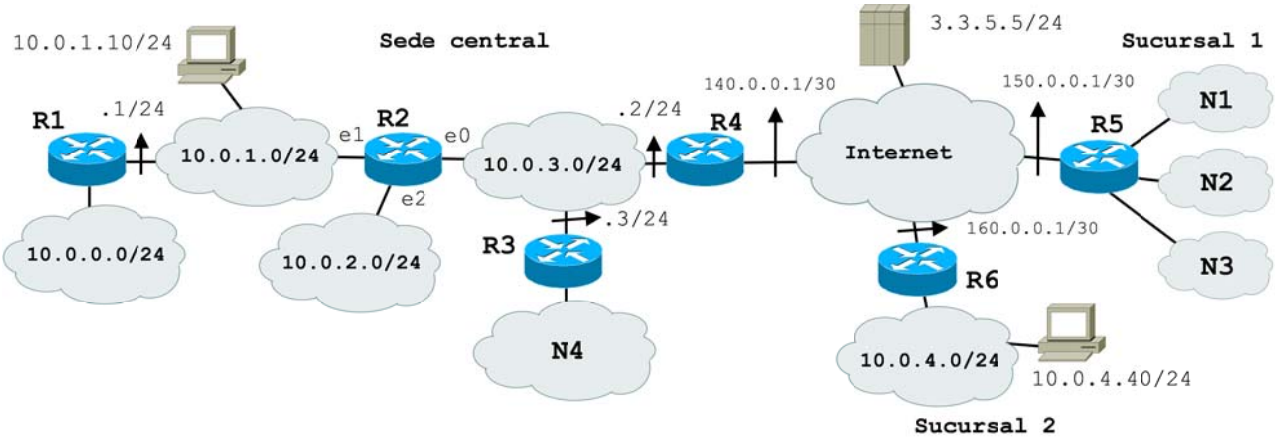
d) Suponer que un cliente se conecta a un servidor para bajarse una página web de 32120 bytes (22 MSS de 1460 bytes). El TCP solo implementa Slow Start y Congestion Avoidance. Suponer que el buffer de recepción del cliente es de 11680 bytes y el tiempo de propagación entre cliente y servidor es de 100 ms.
   (i) Suponiendo que no hay pérdidas, dibujar un diagrama de tiempo (como en la figura) donde se vea la evolución de las ventanas de congestión (cwnd), anunciada (awnd) y de transmisión (wnd) y el umbral ssthresh. Por simplicidad, numerar los segmentos como S1, S2, etc, y las confirmaciones como A1, A2, etc.



   (ii) Suponer ahora que el segmento S6 se pierde. Dibujar un diagrama de tiempo, como en el caso a), donde se vea la evolución de las ventanas de congestión (cwnd), anunciada (awnd) y de transmisión (wnd) y el umbral ssthresh. Suponer un temporizador RTO de 250 ms.

Problema 3.1.8.

La red de una empresa consiste de 3 partes: una sede central y dos sucursales. Se ha configurado una VPN que mantiene dos túneles, uno entre R4 y R5 y el otro entre R4 y R6. Las direcciones públicas de estos túneles son 140.0.0.1/30, 150.0.0.1/30 y 160.0.0.1/30. Para dar salida a Internet a todos los hosts privados de la red, R4 aplica NAT dinámico con rango 140.0.0.9-140.0.0.14.



a) La empresa obtiene de un ISP el rango de direcciones públicas 140.10.0.0/25 con la que quiere configurar 4 redes de hosts públicos. Los requerimientos de estas redes son los siguientes:
   - Red N1 tiene 20 hosts, Red N2 tiene 8 hosts, Red N3 tiene 10 hosts, Red N4 tiene 50 hosts.

   Encontrar un direccionamiento valido para esta empresa.

b) Sabiendo que se ha activado el RIPv2 en toda la red, escribir la tabla de encaminamiento de R2. Indicar las redes públicas con N1, N2, N3 y N4. Ayudarse con una tabla del tipo

Adquisición	Red/mascara	Gateway	Interfaz	Métrica
S, R o C				

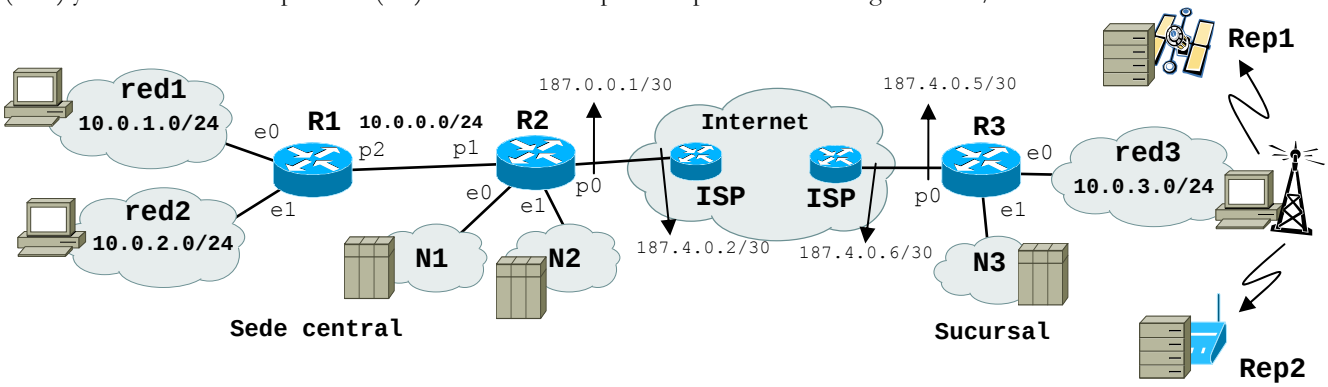
c) Una vez que la red ha alcanzado una situación estable, encontrar:
   (i) El mensaje RIPv2 que R2 envía por su interfaz e0 suponiendo split horizon activo.
   (ii) El mensaje RIPv2 que R2 envía por su interfaz e0 si cae la red 10.0.1.0/24 suponiendo split horizon y poison reverse activos.
   (iii) Mismo caso que (ii) pero también está activo triggered update.

d) Encontrar las direcciones orígenes y destinos de los siguientes datagramas cuando estos pasan por Internet (si pasan más de una vez, indicar los valores de cada vez):
   (i) El host 10.0.1.10 hace ping a 10.0.4.40.
   (ii) El host 10.0.1.10 hace ping a 3.3.5.5.
   (iii) El host 10.0.4.40 hace ping a 3.3.5.5.

e) A través de una conexión TCP, el host 10.0.1.10 empieza a bajarse un fichero de 2 Mbytes del servidor 3.3.5.5. Sabiendo que la velocidad de transmisión es muy grande (suponer infinito), que el tiempo de ciclo del TCP (RTT) es de 100 ms y que las ventanas anunciadas por el cliente y por el servidor se mantienen constantes a 8192 bytes y 27680 bytes, respectivamente, calcular la velocidad efectiva de la transferencia en régimen estacionario (es decir cuando la ventana de transmisión se mantiene constante).

Problema 3.1.9.

La red de una empresa consiste de 2 partes: una sede central y una sucursal. La red de la sede central consiste de dos redes de hosts privados (red1 y red2) y dos de servidores públicos (N1 y N2). La red de la sucursal tiene una red de hosts privados (red3) y otra de servidores públicos (N3). Las direcciones privadas pertenecen al rango 10.0.0.0/8.



a) La empresa obtiene de un ISP el rango de direcciones públicas 187.4.0.0/25. Este rango se utiliza para
- dar conexión a Internet a través de los dos routers de salida R2 y R3 (redes 187.4.0.0/30 y 187.4.0.4/30),
- configurar 3 redes de 10 servidores públicos cada una,
- dar acceso a Internet reservando por lo menos 50 direcciones IP para NAT.

Encontrar un direccionamiento valido para esta empresa.

b) Se pide configurar una lista de acceso en el router R3 sobre el tráfico de salida de la interfaz e0. Las reglas deben permitir lo siguiente
- Los servidores de la red3 son accesibles solamente desde clientes de la red privada 10.0.0.0/8.
- Los clientes de la red3 pueden acceder a cualquier servidor de la red privada 10.0.0.0/8 y de la N3. Sin embargo solo pueden conectarse a los servidores web del resto de Internet.

Escribir dicha lista de acceso. Usar el siguiente formato indicando bien los límites de los puertos a través de operadores como = (igual), ≥ (mayor igual), ≤ (menor igual) y ≠ (diferente). El estado puede ser *toda* conexión o conexión ya *establecida*

```
permitir/prohibir    protocolo    origen (IP y puerto/s)    destino (IP y puerto/s)    estado
```

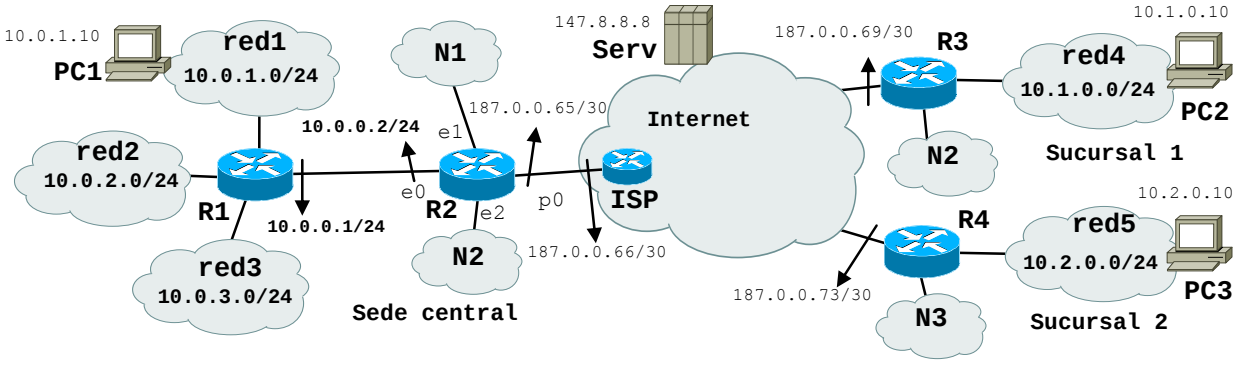
c) Para intercambiar datos con los dos repositorios, el host de la red3 usa unos protocolos ARQ. En particular:
- Entre Rep1 y el host se usa un protocolo Go-back-N, la distancia es de 4000 km, la longitud de las PDUs de 1500 bytes, la velocidad de transmisión de 500 kbit/s, el temporizador de 100 ms y la probabilidad de error en un bit de 5×10^{-6}.
- Entre Rep2 y el host hay una distancia despreciable y se usa un protocolo Stop&Wait, la longitud de las PDUs es de 500 bytes, la velocidad de transmisión de 5 Mbit/s y el temporizador de 1 ms.

Sabiendo que la velocidad de propagación en los dos casos es de 2×10^8 m/s, se pide:
(i) Calcular la eficiencia del sistema Rep1-host.
(ii) Calcular la máximo probabilidad de error en un bit que debería haber entre Rep2-host para que este segundo sistema tenga la misma eficiencia del primero. Se puede usar la formula simplificada Nt = 1 / (1 - L×Pb).

d) Un servidor de la N1 envía datos a un cliente de la red3 usando TCP. Al establecer la conexión, los extremos han acordado un MSS de 1000 bytes. La ventana que el servidor anuncia al cliente es de 5000 bytes y la que anuncia el cliente de 7000 bytes. El RTT es de 50 ms y el RTO de 150 ms.
(i) Dibujar el intercambio de datos y ack entre servidor y cliente hasta pasados 300 ms (no se pide incluir el 3WH).
(ii) Suponiendo que no hay pérdidas, determinar la velocidad efectiva de este sistema una vez alcanzado el régimen estacionario.

Problema 3.1.10.

La red de una empresa consiste de 3 partes conectadas a través de una **VPN**: una **sede central** y **dos sucursales**. La red de la sede central consiste de tres redes de hosts privados (**red1**, **red2** y **red3**) y dos de servidores públicos (**N1** y **N2**). La red de las sucursales son similares y cada una tiene una red de hosts privados (**red4** y **red5**) y otra de servidores públicos (**N3** y **N4**). Las direcciones privadas pertenecen al rango 10.0.0.0/8. La VPN consiste de dos túneles: **tun0** que conecta virtualmente R2 con R3 con direcciones 10.8.0.1/30 y 10.8.0.2/30 y **tun1** que conecta R2 con R4 con direcciones 10.8.1.1/30 y 10.8.1.2/30. Para proporcionar acceso a Internet a toda la red privada de la empresa, **R2** soporta **PAT** (NAT por puertos).



a) La empresa obtiene de un ISP el rango de direcciones públicas 187.0.0.0/26 para las cuatros redes de servidores públicos. Encontrar un direccionamiento valido para esta empresa considerando que:
- En N1 hay 25 servidores
- En N2 hay 10 servidores
- En N3 y N4 hay 5 servidores en cada una

b) Se activa el RIPv2 en todos los routers de la empresa. Se pide determinar la tabla de encaminamiento del router R2. Usar el formato siguiente:

```
Adquisición    IP/mascara      Gateway      Interfaz      Métrica
```

Indicando en adquisición si la entrada en la tabla se refiere a una ruta S (estática), C (conectada directamente) o R (aprendida por RIP). Indicar las redes de servidores como N1, N2, N3 y N4

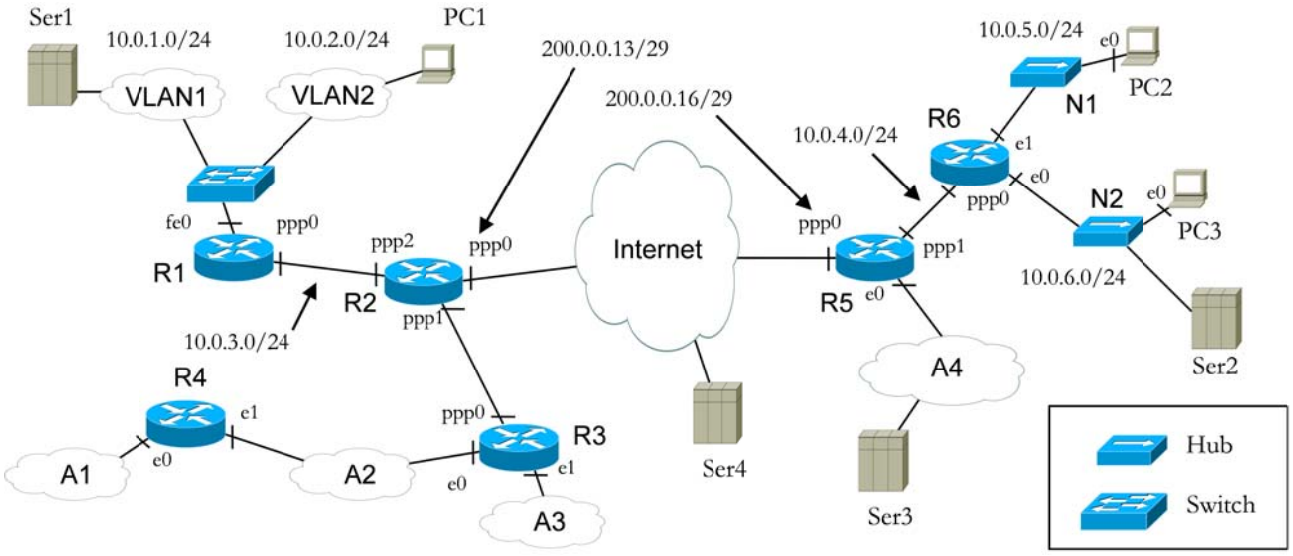
c) Se pide determinar las direcciones origen y destino de los datagramas IP cuando estos pasan por Internet en los siguientes casos, indicando claramente que mecanismo se está empleando.
(i) PC1 hace un ping a PC2
(ii) PC1 hace un ping a Serv
(iii) PC2 hace un ping a Serv
(iv) PC2 hace un ping a PC3

d) PC1 se conecta con Serv para bajarse un fichero (los datos van de Serv a PC1). Al establecer la conexión, los extremos han acordado un MSS de 552 bytes. Los buffers de recepción de los dos extremos son de 65136 bytes para PC1 y 35328 bytes para Serv. El tiempo de propagación se supone constante e igual a 50 ms. La velocidad de transmisión de la red de la empresa es de 100 Mbit/s mientras en Internet se consiguen 20 Mbit/s. Se pide
(i) Suponiendo que no hay pérdidas, dibujar la grafica ventana de transmisión wnd – tiempo hasta pasados 1 s, indicando claramente los calores de la ventana anunciada awnd y de congestión cwnd.
(ii) Determinar la velocidad efectiva de este sistema una vez alcanzado el régimen estacionario.

3.2. - Redes IP

Problema 3.2.1.

La figura corresponde a una empresa compuesta por una sede central y una sucursal conectada por medio de Internet. A los interfaces PPP de los routers R2 y R5, el ISP les asigna las direcciones públicas indicadas en la figura (200.0.0.13 y 200.0.0.16 respectivamente). Los dos routers tienen capacidad para realizar *tunneling* y NAT. De las subredes que forman la red, en algunas se asignarán direcciones IP privadas (direcciones 10.0.X.X) y en otras, direcciones IP públicas. En la figura se muestra la asignación de direcciones y máscaras IP de la parte privada. En la sede central se utiliza un *switch* para generar y gestionar 2 VLANs, en las que se asignan direcciones IP privadas. También son redes privadas las N1 y N2 de la sucursal y las conexiones PPP entre R1 y R2 y entre R5 y R6. Las subredes sin asignación de direcciones y máscaras son subredes públicas, estas son la subred A1, A2, A3, A4 y la conexión PPP entre el router R2 y el R3.



a) Se quiere adquirir un grupo de direcciones IP públicas para las subredes. Definir un esquema de direcciones públicas apropiado al esquema de la figura, a partir del rango 131.1.8.0/24. Para la asignación de las direcciones ten en cuenta las siguientes condiciones: en la red A1 se van a conectar 5 PCs, en la red A2 20 PCs, en la red A3 30 PCs y en la red A4 tantos PCs como sea posible. En el enlace PPP entre R2 y R3 se necesitan sólo 2 direcciones (los extremos de enlace PPP). Además se quiere que los valores numéricos de las direcciones sigan el orden (de menor a mayor): A1, A2, A3, PPP, A4 (por ejemplo 131.1.8.2 tiene un valor numérico inferior a 131.1.8.10).

b) Desde el host PC2 se hace un ping al servidor Ser2. PC2 tiene @IP 10.0.5.100 y Ser2 tiene @IP 10.0.6.10. Suponer que las tablas de ARP de los elementos involucrados están vacías y que durante el tiempo de trabajo, no hay otras tramas circulando que las derivadas del comando antes mencionado. Describir la secuencia de tramas Ethernet, datagramas IP, paquetes ARP y paquetes ICMP que aparecerán en la red desde el momento en que da comienzo la ejecución del comando hasta que llega la primera respuesta del destinatario del ping. Indicar las direcciones físicas de las interfaces usando el formato nombre-interfaz (por ejemplo PC2-e0 para indicar la dirección MAC de la interfaz e0 de PC2). Para la dirección de broadcast usar el formato FF-FF. Asignar las direcciones IP que se consideran necesarias.

Eth		ARP					IP		ICMP
@src	@dst	Query / Response	MAC sender	IP sender	MAC receiver	IP receiver	@src	@dst	Echo RQ/RP

c) Sabiendo que todos los routers operan con RIPv2 con split horizon, poison reverse y triggered uptade, ¿cuál sería la tabla de encaminamiento del router R3? Indicar en la columna adquisición con C una ruta directa, con R determinada por el RIP y con S una ruta estática. En la columna Gateway indicar la dirección del router como nombre-interfaz (por ejemplo, R4-e1 para la interfaz e1 del router R4).

Adquisición	Red / máscara	Gateway	Interfaz	Métrica

d) Indicar que haría el router R3 si se cayera el enlace entre R2 y R3. Indicar el/los mensaje/s que enviaría R3, después de cuánto tiempo y a quien. Comenta las suposiciones que hagas.

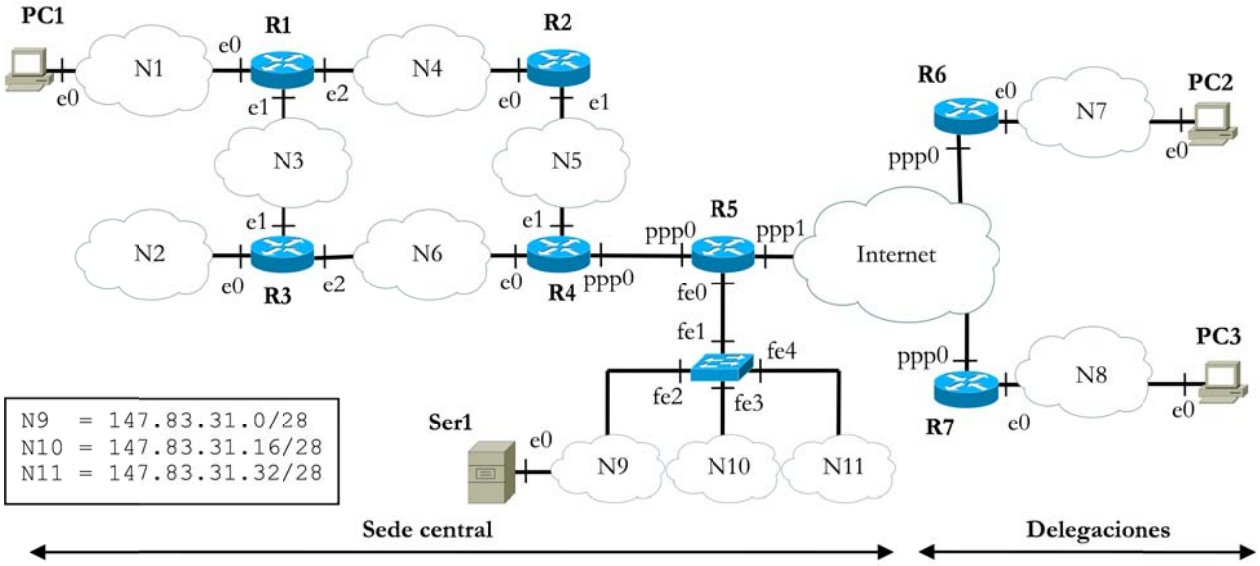
Red	Máscara	Métrica

e) Escribir la cabecera de un paquete IP (solo direcciones IP origen y destino) en el router de salida R2 cuando se accede desde PC1 con IP 10.0.2.55 a un servidor Ser4 de Internet con IP 220.20.10.135 (asumir que las ARP caches están llenas).

f) Escribir la cabecera de un paquete IP (solo direcciones IP origen y destino) en el router de salida R2 cuando se accede desde PC1 al servidor Ser2 de la sucursal (asumir que las ARP caches están llenas)

Problema 3.2.2.

Una empresa acaba de instalar la red de la figura compuesta por una sede central y dos delegaciones que están conectadas por medio de Internet. En la sede central tenemos cinco routers (R1 a R5) que forman las redes departamentales internas *privadas* (N1 a N6) y un switch que conecta las redes VLAN de los servidores *públicos* (N9 a N11). Cada delegación se compone de un router y una red privada (N7 y N8).



Las direcciones públicas de las interfaces de los routers conectados a Internet son la 140.0.0.1/30 para la ppp1 de R5, la 150.0.0.1/30 para la ppp0 de R6 y la 160.0.0.1/30 para la ppp0 de R7. Los terminales de las redes privadas (sede central y delegaciones) acceden a Internet pasando por el respectivo router de salida (R5, R6 o R7) que aplica NAT por puertos. Cada delegación usa un túnel para acceder a la red privada de la sede central; en los dos extremos del túnel se usan las direcciones públicas de los respectivos routers. Eso implica que hay dos túneles, uno que conecta el router R6 al R5 y el otro el router R7 al R5 y que para ir de una delegación al otra hay que pasar necesariamente por el router R5.

a) Las redes públicas usan las direcciones de red ilustradas en la figura. A las redes privadas de la sede central y de las delegaciones se le asigna el rango de direcciones 10.8.28.0/22. Cada subred privada tiene como máximo 50 usuarios (excepto claramente la subred formada por la conexión serie entre el router R4 y R5). Definir un esquema de direccionamiento apropiado a la configuración de la figura, asignando las subredes necesarias. Indicar para cada red (N1..N8) la dirección y máscara asignada en la forma IP/máscara.

b) Suponiendo que N8 pasa a tener 100 usuarios, definir un nuevo esquema de direccionamiento. Por simplicidad, se sugiere aprovechar parte de la solución del punto a)

c) A partir del de direccionamiento encontrado, asignar direcciones IP a las interfaces ppp0 y fe0 del router R5.

d) Toda la red usa RIPv2. Indica el mensaje que R3 envía a R4 después de 30 segundos desde la activación del RIPv2 suponiendo que R3 aún no ha recibido ningún mensaje de los otros routers. Indicar tanto el caso que el RIPv2 usara *split horizon* como el caso sin *split horizon*.

R3 -> R4 con split horizon

red	mascara	métrica

R3 -> R4 sin split horizon

red	mascara	Métrica

e) Escribir la tabla de encaminamiento del router R4 con el formato indicado. Indica en la columna adquisición una ruta directa con C, determinada por RIP con R y estática con S. En la columna Gateway indica la dirección del

router como router-interfaz (por ejemplo R3-e2 para referirte a la dirección IP de la interfaz e2 del router R3). En la columna Interfaz indicar la interfaz de salida del router R4.

Adquisición	Red/mascara	Gateway	Interfaz	Métrica

f) Supón que la MTU de todas las redes es de 1500 bytes excepto la MTU de la red N8 que es de 512 bytes. PC2 envía un datagrama de longitud máxima a PC3 con el flag DF desactivo. Suponiendo que no hay fragmentación en Internet, deduce que operación hará el router R7, que información va a enviar y hacia quien. Usa la siguiente tabla:

Número fragmento	Flag DF	Flag MF	Offset	Longitud total

g) Ahora PC3 contesta a PC2 enviando un datagrama de longitud máxima pero con el flag DF activo. Deducir que operación hare el router R7, que información va a enviar y hacia quien. Si necesario, hacer uso de la tabla del punto f).

h) Definir una lista de acceso para efectuar filtrado en la interfaz fe0 del router R5 para que direcciones externas a la empresa solo puedan acceder a los servicios TCP de los servidores públicos y que no haya restricciones para las direcciones privadas. El formato de cada entrada en la lista de acceso debe ser el siguiente:

access-list **denegar / permitir** **protocolo (IP, TCP, etc.)** **IP_{origen}/mask** **=,!=,<,> $puerto_{origen}$** **IP_{origen}/mask** **=,!=,<,> $puerto_{destino}$**

Se puede usar la palabra **todo** en los campos protocolo, IP o puertos para indicar que concierne todos los protocolos, las IP o los puertos. Los símbolos "=, !=, >, <" en el campo puerto indican respectivamente "igual, diferente, mayor y menor" de un determinado puerto.

Ejemplo: **access-list denegar TCP 10.0.0.4/24 >=1024 todo =21**

significa que se deniega información de tipo TCP con origen 10.0.0.4/24 y puerto mayor igual de 1024 y destino cualquier IP con puerto igual a 21.

i) Escribir la cabecera de un paquete IP (solo dirección origen y destino) en el router de salida R7 cuando:
   (i) PC3 accede al servidor Ser1 de la red N9 con IP 147.83.31.12.
   (ii) PC3 accede a PC1 de la red N1.

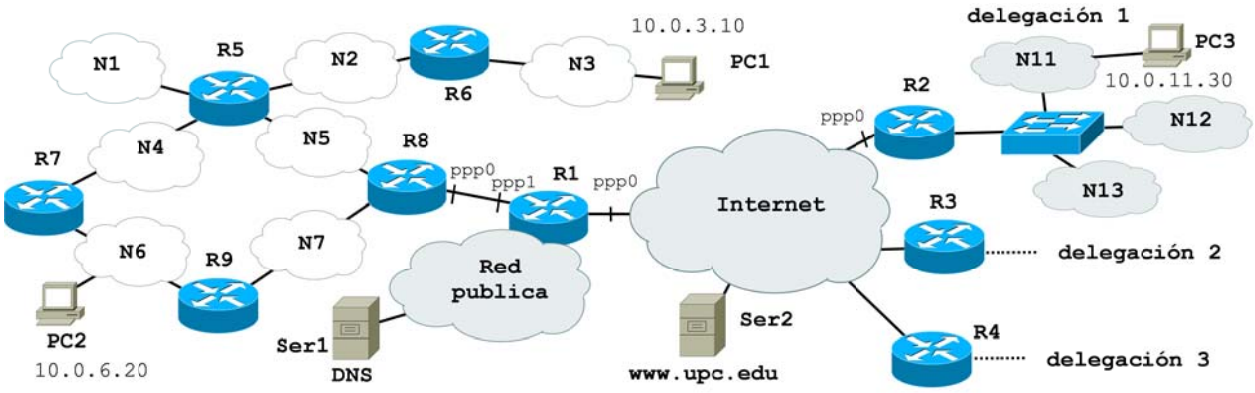
Problema 3.2.3.

Una empresa dispone de la red de la figura compuesta por una sede central y tres delegaciones conectadas por medio de Internet. En la sede central tenemos

- Siete redes departamentales internas privadas (de N1 a N7). Estas redes tienen direcciones privadas del tipo 10.0.X.0/24 donde X es el número de la red (por ejemplo la N1 tiene la 10.0.1.0/24).
- una red de los servidores públicos (red pública).
- un router/firewall que conecta las redes privadas y públicas con Internet.

Cada delegación Y está compuesta por

- un router que se conecta a la sede central con una VPN a través de un túnel en Internet.
- un switch que conecta tres VLANs (de NY1 a NY3) que componen la red privada. Las direcciones privadas siguen el mismo esquema de la sede central, por ejemplo la red N31 de la delegación 3 tiene la 10.0.31.0/24.



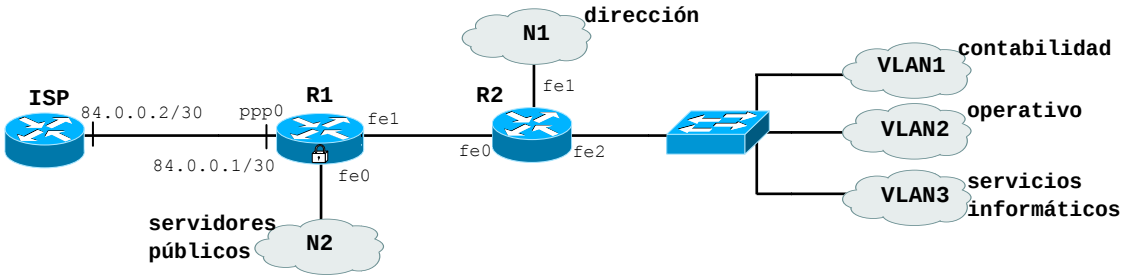
a) A partir del rango 202.0.1.128/25 diseñar un esquema de direccionamiento para la parte pública sabiendo que esta se compone de 7 redes:
   - Dos redes de interconexión entre routers
   - Tres redes con 5 hosts cada una
   - Una red con 28 hosts
   - Una red con 50 hosts

b) Sabiendo que las direcciones IP públicas de los routers R1-R4 son 201.0.1.1, 201.0.2.1, 201.0.3.1 y 201.0.4.1 respectivamente y que el router R1 usa NAT dinámico con rango 202.0.1.10-202.0.1.19, mientras R2, R3 y R4 usan PAT, deducir:
   (i) Si PC1 hace un ping a PC3, las direcciones IP que tendrán los datagramas en las redes N5, en Internet y en N11.
   (ii) Si PC1 hace un ping al Ser2, las direcciones IP que tendrán los datagramas en las redes N5 y en Internet.
   (iii) Si PC3 hace un ping al Ser2, las direcciones IP que tendrán los datagramas en las redes N11 y en Internet.

c) Asignar direcciones IP a las interfaces internas (las que están conectadas con los switches) de los routers R2, R3 y R4.

Problema 3.2.4.

La sede central de una empresa tiene la siguiente configuración



Se pide:

a) Un direccionamiento valido para esta empresa sabiendo que: 1) el router R1 separa la red de servidores públicos N2 del resto que son redes privadas; 2) que el ISP proporciona un rango de direcciones publicas a partir de 200.0.0.0/24; 3) la empresa quiere mantener los 5 servidores públicos (http, DNS, mail, ssh, fax) siempre visibles desde Internet y quiere adquirir el número mínimo de direcciones públicas; 4) en la red privada hay 2 hosts en dirección, 10 en contabilidad, 10 en operativo y 5 en servicios informáticos. Motivar los razonamientos y elecciones.

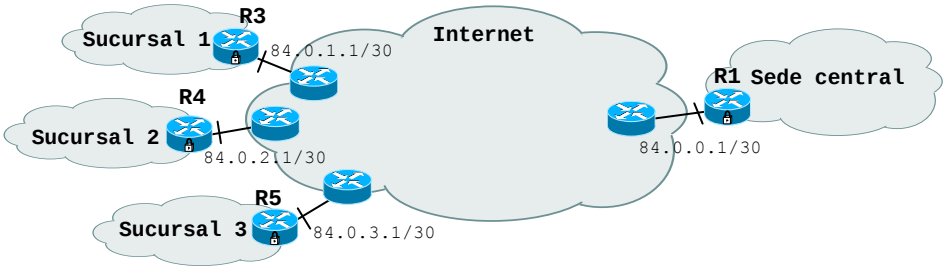
b) Dar conexión a Internet a dirección, contabilidad y operativo. Motivar los razonamientos y elecciones.

c) Configurar las interfaces de los routers R1 y R2 e indica sus tablas de encaminamiento especificando los valores de "**`destino, máscara, gateway, interfaz y métrica`**". Suponer que se ha activado RIPv2 y las tablas han convergido.

d) Configurar el router R1 para que haga de firewall. En particular: 1) que cualquier cliente de Internet pueda acceder a los servidores públicos pero no a la red privada; 2) que los hosts de la red privada puedan acceder a los servidores públicos y a los servidores de Internet. Para las reglas ACL usar el siguiente formato:

```
IPdest/mascara   puertodest   IPorig/mascara   puertoorig   protocolo   estado   acepta/rechaza
```

Suponer ahora que esta sede central pertenece a una empresa que tiene además 3 sucursales.



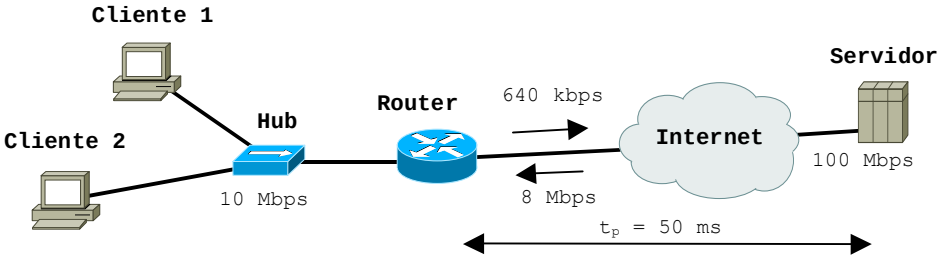
Se pide:

e) Proponer qué túneles deberían configurarse si se desea que haya el menor número posible de túneles en la VPN de la empresa.

f) Configurar las direcciones IP de los túneles.

3.3. - Protocolos ARQ y TCP/UDP

Problema 3.3.1.



Los PCs Cliente 1 y Cliente 2 están conectados a Internet a través de un hub 10baseT y un router ADSL. La línea ADSL tiene una velocidad de 8 Mbps de bajada y de 640 kbps de subida. Un servidor repositorio de ficheros está conectado a una línea de acceso de 100 Mbps. Se sabe que el tiempo de propagación entre router y servidor es de 50 ms, y que el retardo en la red de los clientes es despreciable. Cuando se establece una conexión TCP, el *Maximum Segment Size* (MSS) usado es de 512 bytes en los dos sentidos.

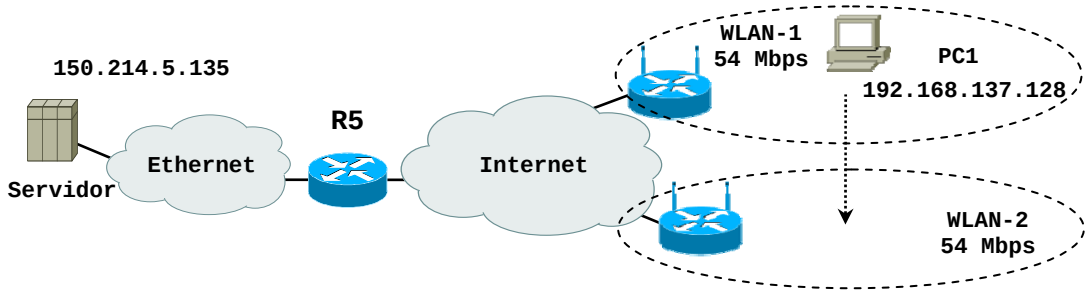
a) El Cliente 1 establece una conexión TCP con el servidor para bajarse un fichero. Dibujar un diagrama de tiempos con dos ejes: Cliente-1 y Servidor donde se muestre el intercambio de segmentos TCP y confirmaciones entre Cliente 1 y Servidor desde que se envía el primer segmento hasta pasados 800 ms. Mostrar claramente los tiempos de envío y recepción y la evolución de la ventana de congestión (cwnd) del servidor.

b) Suponiendo que la ventana anunciada (awnd) por el Cliente 1 es siempre de 65536 bytes y que no se pierde ningún dato, determinar (i) la velocidad efectiva de la conexión TCP, (ii) la máxima ventana de transmisión, (iii) cuantos segmentos componen una ventana máxima, y (iv) el tiempo que se tarda para alcanzarla. Comenta las suposiciones que hagas.

c) Suponer ahora que el Cliente 2 también establece una conexión TCP con el Servidor. En este caso pero el Cliente 2 envía un fichero al Servidor para guardarlo en su repositorio. Suponiendo que no hay pérdidas y que la ventana anunciada por el Servidor es de 16384 bytes, determinar la velocidad efectiva de la conexión TCP entre Cliente 2 y Servidor. Calcular también cual sería la ventana de transmisión óptima en segmentos (mínima ventana que permite conseguir esta velocidad). Razonar la respuesta.

d) Suponer ahora que se pierde el segmento enviado inmediatamente después de que el Cliente 2 alcance la ventana óptima calculada anteriormente. TCP no usa *fast-retransmision/fast-recovery*. El temporizador RTO es de 200 ms. Haz un gráfico que muestre la evolución de la ventana de transmisión (eje *y*: ventana de transmisión, eje *x*: tiempo) desde la transmisión del primer segmento hasta alcanzar nuevamente la ventana máxima después de la pérdida. Calcular la duración de este intervalo de tiempo en segundos. Mostrar claramente en el gráfico las fases de *slow-start* y *congestion-avoidance* y el valor del umbral sstresh.

Problema 3.3.2.



El PC1 está conectado a Internet a través de una red WLAN de 54 Mbps. Un servidor de video está conectado a una red Ethernet de 10 Mbps. La velocidad de transmisión en internet es más grande que la de las dos redes locales. Todos los dispositivos tienen una eficiencia del 100% y los buffers del router y del access point son infinitos. PC1 establece una conexión TCP (la opción *window scale* está desactiva) con el servidor y se determina que el tiempo de propagación extremo a extremo es de 50 ms. Se pide lo siguiente:

a) A partir de la siguiente captura y sabiendo que no hay pérdidas, determinar: (i) el MSS de la conexión servidor-PC1, (ii) el tamaño de la ventana de transmisión una vez terminado el transitorio, (iii) la velocidad efectiva y (iv) cuanto tiempo se tarda aproximadamente en completar la descarga del video.

```
...
150.214.5.135.80 > 192.168.137.128.39599: P 726852531:726853991(1460) ack 1637 win 5240
192.168.137.128.39599 > 150.214.5.135.80: . ack 726853991 win 64240
150.214.5.135.80 > 192.168.137.128.39599: . 726853991:726855451(1460) ack 1637 win 5240
192.168.137.128.39599 > 150.214.5.135.80: . ack 726855451 win 64240
150.214.5.135.80 > 192.168.137.128.39599: . 726855451:726856911(1460) ack 1637 win 5240
192.168.137.128.39599 > 150.214.5.135.80: . ack 726856911 win 64240
150.214.5.135.80 > 192.168.137.128.39599: F 726856911:726857231(320) ack 1637 win 5240
192.168.137.128.39599 > 150.214.5.135.80: F 1637: 1637(0) ack 726857231 win 64240
150.214.5.135.80 > 192.168.137.128.39599: . ack 1638 win 5240
```

b) Identificar si el volcado se ha capturado en el servidor o en el PC1.

c) A partir de las condiciones del punto a), si en la red Ethernet hubieran otros 4 servidores transmitiendo a la vez hacia otros clientes, determinar la velocidad efectiva de la conexión servidor-PC1 y la duración aproximada de la descarga.

d) A partir de las condiciones del punto a), si el *window scale* fuera activo con un factor de multiplicación de la ventana anunciada de 4, determinar la velocidad efectiva y la duración aproximada de la descarga.

e) Suponer ahora que PC1 se mueve de la WLAN-1 a la WLAN-2. Durante esta transición, se pierden algunos segmentos. Sabiendo que PC1 hace el cambio de red cuando estaba en la mitad de la descarga y a su máxima velocidad, haz un gráfico que muestre la evolución de la ventana de transmisión (eje *y*: ventana de transmisión, eje *x*: tiempo) desde la transmisión del primer segmento en la nueva red hasta 1.5 segundos. Muestra claramente en el gráfico las fases de *slow-start* y *congestion-avoidance* y el valor del umbral *sstresh*. Suponer que TCP no usa *fast-retransmission/fast-recovery* y el temporizador RTO es de 200 ms.

f) Hacer un gráfico como el punto anterior pero ahora suponer que, en la WLAN-2, se pierde un segmento cada vez que la ventana de congestión llega a 23360 bytes.

Problema 3.3.3.

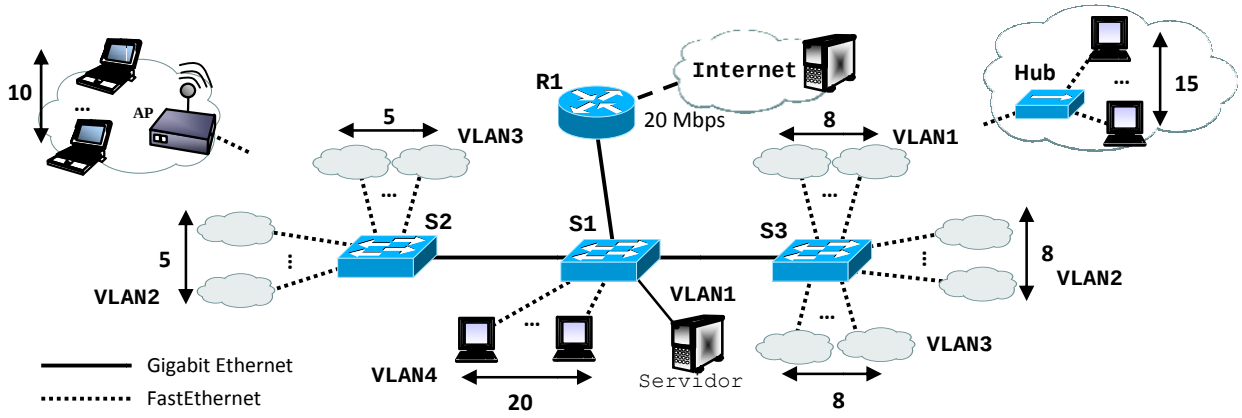
a) Entre dos puntos se establece una conexión ARQ de tipo Go-back-N a 20 Mbps con PDUs de 1500 bytes y ack de 40 bytes de longitud respectivamente. El ping da 100 ms como retardo medio entre estos dos puntos. El sistema garantiza una probabilidad de error en un bit de 10^{-6}. Se fija un temporizador de 110 ms. Se pide
   (i) Calcular la eficiencia E de este sistema.
   (ii) Calcular la velocidad efectiva vef.
   (iii) Determinar la ventana óptima Wopt.
   (iv) Si las PDUs fueran más pequeñas (por ejemplo 100 bytes), ¿mejoraría la eficiencia?

b) Ahora se decide reemplazar la conexión Go-back-N entre estos dos puntos con una conexión TCP con MSS de 1460 bytes. El ping sigue dando 100 ms. Se pide
   (i) Determinar si con un window scale desactivado y sin errores, la velocidad efectiva vef con TCP una vez alcanzado un régimen estable es mejor o peor del sistema anterior con Go-back-N.
   (ii) Si se aceptara un window scale de 8 (es decir la ventana anunciada se desplaza de 3 bits de manera que su valor se multiplicaría por 23), calcular cual sería en este caso la velocidad efectiva vef.
   (iii) Suponiendo que se fija un window scale de 2 y que el sistema con TCP tiene perdida cada vez que la ventana llega a 64 MSS, dibujar cual sería la evolución de la ventana de transmisión wnd en el tiempo (grafico wnd vs. RTT) indicado claramente los valores de la ventana de congestión cwnd, anunciada awnd y el umbral ssthresh. Notar que la ventana de transmisión debería presentar un aspecto periódico. Suponer un temporizador RTO igual al tiempo de ida y vuelta RTT.
   (iv) Determinar aproximadamente cual sería la velocidad efectiva vef en este último caso. Se sugiere hacer uso del dibujo anterior.

c) Entre estos dos puntos se cierra la conexión TCP y se activa una aplicación de telefonía sobre IP que usa UDP como protocolo de transporte. La aplicación genera datagramas UDP con 256 bytes de datos periódicamente con un tiempo entre paquetes de 100ms. Se pide
   (i) Determinar la velocidad efectiva vef .
   (ii) Suponiendo que un 10% de los paquetes se pierden, determinar la velocidad efectiva vef en este caso.

3.4. - Redes LAN

Problema 3.4.1.



La red de la figura está formada por 480 estaciones y un servidor interno. Se han configurado 4 VLANs. Todos los enlaces son FastEthernet excepto los enlaces S1-S2, S1-S3, S1-R1 y S1-Servidor que son Gigabit Ethernet y el enlace del router a Internet que es de 20Mbps. La eficiencia de los Switch es del 100%, de los Hubs del 80% y de los Access-Points (APs) del 66.7% (dos tercios). Cada VLAN conectada al switch S3 consiste de 8 hubs, cada uno conectado con 15 estaciones. Cada VLAN conectada al switch S2 consiste de 5 APs, cada uno conectado con 10 estaciones wireless. Los APs y las estaciones wireless usan 802.11g (54 Mbps). Supón que todas las estaciones usan un tipo de aplicación que usa conexiones TCP y siempre tienen información lista para transmitir al servidor (las respuestas del servidor son despreciables). Las estaciones que no están activas no transmiten. Contesta para los escenarios que se dan a continuación: (i) Los enlaces donde se creará un cuello de botella, (ii) Cual será el o los mecanismos que regulan la velocidad efectiva de las estaciones, (iii) La velocidad efectiva que conseguirán las estaciones activas. Razonar y motivar las respuestas comentando las suposiciones hechas (no se aceptarán respuestas numéricas sin explicaciones).

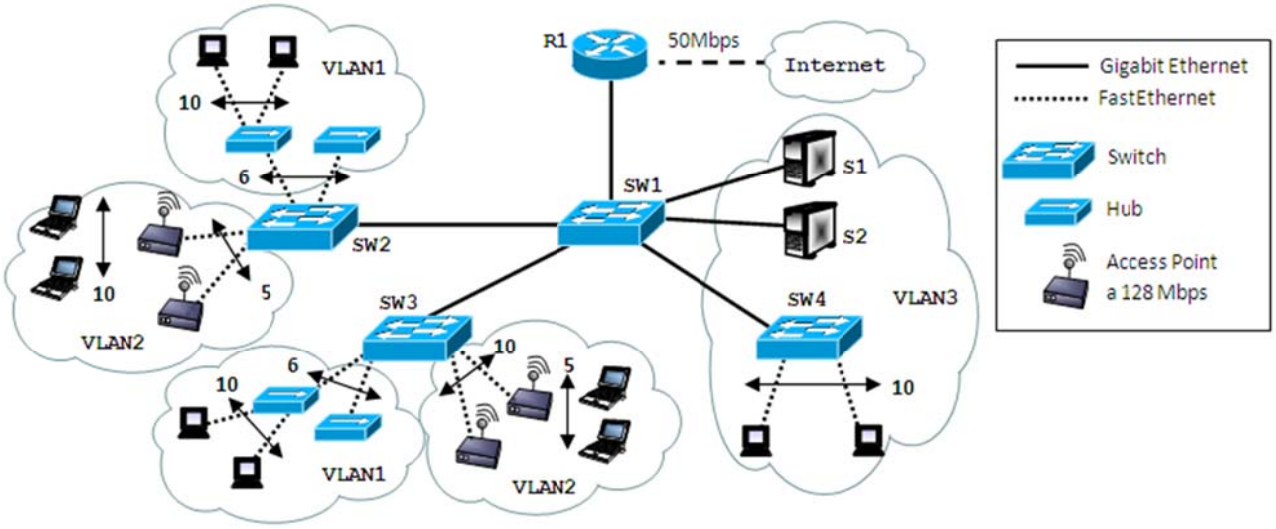
a) Solo están activas las estaciones de la VLAN1.

b) Solo están activas las estaciones de las VLAN2 y VLAN3.

c) Solo están activas las estaciones de las VLAN1 y VLAN4.

d) Las estaciones de las VLAN1, VLAN2 y VLAN3 acceden a un servidor de Internet.

Problema 3.4.2.



La red de la figura está formada por 230 estaciones y dos servidores S1 y S2. Se han configurado 3 VLANs donde el número de Access Points (APs), hubs y estaciones por hub o AP está indicado en la figura. Los enlaces cableados son GigabitEthernet o FastEthernet según si son dibujados como líneas enteras o punteadas. Los APs usan una conexión

wireless a 128 Mbps. El enlace del router a Internet es de 50Mbps. La eficiencia de los Switch es del 100%, de los Hubs del 80% y de los APs del 50%. Contesta para los escenarios que se dan a continuación suponiendo que solo transmiten información las estaciones que están activas despreciando el efecto de las respuestas. Se pide determinar para cada escenario:
(i) Los enlaces donde se creará el cuello de botella principal.
(ii) Cual será el o los mecanismos que regulan la velocidad efectiva de las estaciones.
(iii) La velocidad efectiva que conseguirán las estaciones activas.
Razona y motiva las respuestas comentando las suposiciones hechas considerando que no se aceptarán respuestas numéricas sin explicaciones.

a) Solo están activas las estaciones de la VLAN1 que transmiten datos al servidor S1.

b) Solo están activas las estaciones de las VLAN1 y VLAN2 que transmiten datos al servidor S1.

c) Solo están activas las estaciones de las VLAN3 que transmiten datos de igual manera a los servidores S1 y S2.

d) Mismo caso que el anterior pero ahora los servidores S1 y S2 tambien transmiten a las estaciones.

e) Las estaciones de las VLAN1 y VLAN2 transmiten a un servidor de Internet.

3.5. - Soluciones

Problema 3.1.1.

Problema 3.1.2.

a)
Número de @IP necesarias

Red	Usuarios	Interfaces routers	Red + broadcast	Total @IP
red 1	25	e1 de R2	2	28
red 2	10	e0 de R2 + e0 de R1	2	14
red 3	20	e1 de R1	2	23
red 4	10	e2 de R1 + e0 de R3	2	14
red 5	0	ppp0 de R1 + ppp1 de Rout	2	4

Red 1 es la que más @IPs necesita 28. La mínima potencia de dos superior a 28 es 2^5=32
Por lo tanto se necesitan por lo menos 5 bits para el hostID

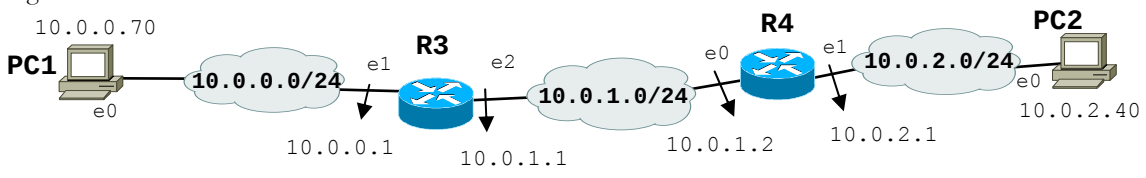
netID 24 bits	**subnetID** 3 bits	**hostID** 5 bits	**Dirección de red**
207. 4. 3.	0 0 0	0 0 0 0 0	207.4.3.0
207. 4. 3.	0 0 1	0 0 0 0 0	207.4.3.32
207. 4. 3.	0 1 0	0 0 0 0 0	207.4.3.64
207. 4. 3.	0 1 1	0 0 0 0 0	207.4.3.96
207. 4. 3.	1 0 0	0 0 0 0 0	207.4.3.128
207. 4. 3.	1 0 1	0 0 0 0 0	207.4.3.160
207. 4. 3.	1 1 0	0 0 0 0 0	207.4.3.192
207. 4. 3.	1 1 1	0 0 0 0 0	207.4.3.224

Las máscaras de las redes son de 24 bits de netID + 3 bits de subnetID = 27 bits
/27 o 255.255.255.224

Dirección de red	Dirección de broadcast	Asignada a	@IP disponibles	@IP libres
207.4.3.0/27	207.4.3.31	ppp0 de Rout (207.4.3.1)	32	29
207.4.3.32/27	207.4.3.63	red 1	32	4
207.4.3.64/27	207.4.3.95	red 2	32	18
207.4.3.96/27	207.4.3.127	red 3	32	9
207.4.3.128/27	207.4.3.159	red 4	32	18
207.4.3.160/27	207.4.3.191	red 5	32	28
207.4.3.192/27	207.4.3.223	libre	32	todas
207.4.3.224/27	207.4.3.255	libre	32	todas

La red 207.4.3.0/27 no se puede asignar a una red interna porque la dirección 207.4.3.1 se está usando para conectar el router de salida Rout con Internet.

b)
PC1 ping a PC2



N	Cabecera trama		ARP					IP		ICMP
	origen	destino	Q/R	MAC sender	IP sender	MAC receiver	IP receiver	origen	destino	Echo RQ/RP
1	:0070	:FFFF	Q	:0070	10.0.0.70	?	10.0.0.1	-	-	-
2	:0001	:0070	R	:0001	10.0.0.1	:0070	10.0.0.70	-	-	-
3	:0070	:0001	-	-	-	-	-	10.0.0.70	10.0.2.40	RQ
4	:0101	:FFFF	Q	:0101	10.0.1.1	?	10.0.1.2	-	-	-
5	:0102	:0101	R	:0102	10.0.1.2	:0101	10.0.1.1	-	-	-
6	:0101	:0102	-	-	-	-	-	10.0.0.70	10.0.2.40	RQ
7	:0201	:0240	-	-	-	-	-	10.0.0.70	10.0.2.40	RQ
8	:0240	:0201	-	-	-	-	-	10.0.2.40	10.0.0.70	RP
9	:0102	:0101	-	-	-	-	-	10.0.2.40	10.0.0.70	RP
10	:0001	:0070	-	-	-	-	-	10.0.2.40	10.0.0.70	RP

1. PC1 de la red 10.0.0.0/24 debe hacer un ping a PC2 de la red 10.0.2.0/24. Siendo dos redes distintas, PC1 necesita pasar por el router R3 que le hace de gateway con la interfaz e1 con IP 10.0.0.1. Para poder enviar el ping a R3, PC1 necesita conocer la MAC de esta interfaz. Envía entonces un ARP request en broadcast en la red 10.0.0.0/24 para descubrir la MAC del 10.0.0.1.
2. R3 contesta a PC1 con un ARP reply informándole que la MAC de su interfaz e1 es :0001. Al finalizar los pasos 1 y 2, PC1 y R3 tienen una nueva entrada en sus respectivas tablas ARP

Tabla ARP PC1

@IP	@MAC
10.0.0.1 (e1 de R3)	:0001

Tabla ARP R3

@IP	@MAC
10.0.0.70 (PC1)	:0070

3. PC1 ahora conoce la MAC de la interfaz e1 de R3 y le puede enviar el ping para PC2. Este es un datagrama ICMP request con dirección IP fuente PC1 y destino PC2, mientras a nivel de trama la dirección física es la interfaz de PC1 y la interfaz e1 de R3.
4. Cuando R3 recibe el ping, mira en su tabla de encaminamiento como llegar a la dirección IP destino, es decir PC2. Ve que tiene que enviarlo por su interfaz e2 y llegar a la interfaz e0 del router R4. En la tabla ARP, R3 no tiene la MAC de la interfaz e0 de R4 así que debe descubrirla; envía un ARP request en broadcast por la red 10.0.1.0/24 saliendo por su interfaz e2.
5. R4 envía el ARP reply a R3 informándole sobre la MAC de su interfaz e0. Al finalizar este paso, R3 y R4 tienen nuevas entradas en sus tablas ARP.

Tabla ARP R3

@IP	@MAC
10.0.0.70 (PC1)	:0070
10.0.1.2 (e0 de R4)	:0102

Tabla ARP R4

@IP	@MAC
10.0.2.40 (PC2)	:0240
10.0.1.1 (e2 de R3)	:0101

6. Ahora R3 puede enviar el ping de PC1 a R4.
7. R4 recibe el ping, mira su tabla de encaminamiento y ve que puede llegar a PC2 con entrega directa saliendo por su interfaz e1; mira su tabla ARP y ve que ya tiene la MAC de PC2 así que puede pasarle el ping sin necesidad de hacer un ARP.
8. PC2 recibe el ping de PC1 y le contesta con un datagrama ICMP reply. Para contestarle ve en su tabla de encaminamiento que debe pasar por el router R4 que le hace de gateway. La tabla ARP de PC2 ya tiene la MAC de la interfaz e1 de R4 así que él envía el ping reply.
9. R4 recibe el ping reply y ve en su tabla de encaminamiento que para llegar a PC1 debe pasar por R3. Mira su tabla ARP y ve que ya tiene la MAC de la interfaz e2 de R3, así que le pasa el ping reply sin necesidad de hacer un ARP.
10. R3 recibe el ping reply y ve en su tabla de encaminamiento que para llegar a PC1 debe hacer una entrega directa saliendo por su interfaz e1. Su tabla ARP ya contiene la MAC de PC1 así que envía el ping reply sin necesidad de hacer un ARP.

c)

El NAT es mejor aplicarlo al router de salida hacia Internet de la red administrada, es decir el router Rout.

		IP		Puerto		Web
Dirección	Interfaz	Origen	Destino	Origen	Destino	Petición/Servicio

Ida	Entrada	ppp1	10.0.0.70	147.83.35.10	1064	80	Petición
	Salida	ppp0	207.4.3.1	147.83.35.10	4000	80	Petición
Vuelta	Entrada	ppp0	147.83.35.10	207.4.3.1	80	4000	Servicio
	Salida	ppp1	147.83.35.10	10.0.0.70	80	1064	Servicio

d)

Datos de entrada: SR, vt = 10 Mbit/s, D = 1000 km, vp = 2×10^8 m/s, Lt = 1500 bytes, La = 20 bytes, To = 1.5 Wopt, E ≥ 95%

(i) Calculo de la duración de las PDUs y de los acks.

Tt = Lt / vt = 1500 bytes / 10 Mbps = 1500 * 8 / $10x10^6$ = 1.2 ms

Ta = La / vt = 20 bytes / 10 Mbps = 20 * 8 / $10x10^6$= 0.016 ms

Calculo del tiempo de propagación

Tp = D / vp = 1000 km / 2×10^8 m/s = 1000 * 10^3 / $2x10^8$ = 5 ms

Calculo del tiempo de ciclo

Tc = Tt + Ta + 2*Tp = 11.216 ms

Calculo de la ventana óptima

Wop = ceil(Tc / Tt) = ceil(11.216 / 1.2) = ceil(9.35) = 10 PDUs

(ii) To = 1.5 Wopt = 15 PDUs = 15 * Tt = 15 * 1.2 ms = 18 ms

(iii) E ≥ 95% = 0.95

E_{SR} = 1 / Nt = 1.053

Sabiendo que $N_t = \frac{1}{(1-Pb)^{Lt+La}} \cong \frac{1}{1-(Lt+La)\times Pb}$, se encuentra que

$$Pb = \frac{1}{Lt+La}\left(1-\frac{1}{Nt}\right) = \frac{1}{(1500+20)\times 8}(1-0.95) = 4.11\times10^{-6}$$

Entonces para $E \geq 95\%$, se necesita que Pb sea menor que 4.11×10^{-6}.

Problema 3.1.3.

a)

(i) 5 servidores + IP del router R3 + IP de red + broadcast = 8 direcciones IPs.

La mínima potencia de dos superior/igual a 8 es $2^3 = 8$

Se necesitan por lo menos 3 bits para el hostID.

Por lo tanto la máscara es /29 = 255.255.255.248.

netID 26 bits					subnetID 3 bits			hostID 3 bits			Dirección de red	Red
140.	8.	4.	0	0	0	0	0	0	0	0	140.8.4.0	N1
140.	8.	4.	0	0	0	0	1	0	0	0	140.8.4.8	N2
140.	8.	4.	0	0	0	1	0	0	0	0	140.8.4.16	Ni
140.	8.	4.	0	0	0	1	1	0	0	0	140.8.4.24	Ni
140.	8.	4.	0	0	1	0	0	0	0	0	140.8.4.32	Ni
140.	8.	4.	0	0	1	0	1	0	0	0	140.8.4.40	Ni
140.	8.	4.	0	0	1	1	0	0	0	0	140.8.4.48	Ni
140.	8.	4.	0	0	1	1	1	0	0	0	140.8.4.56	Ni

(ii) A partir del rango con mascara /26 y haciendo subnetting con mascara /29 se han creado 23 = 8 subredes.

(iii) 8 subredes – N1 – N2 = 6 subredes para los hosts públicos.

(iv) 8 - 2 (red + broadcast) = 6 direcciones IP para cada subred de los hosts.

Hay 6 subredes disponibles.

=> 6 × 6 = 36 direcciones IP en total

(v) Si solo hay 2 subredes para los hosts, podemos ajustar las máscaras para ocupar todo el rango a disposición.

netID 26 bits	subnetID	hostID	Dirección de red	Red

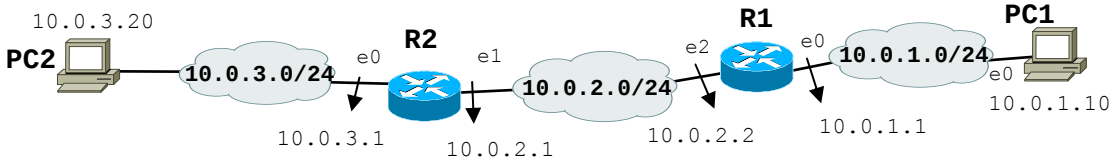
140.	8.	4.	0	0	0	0	0	0	0	0	140.8.4.0 / 29	N1
140.	8.	4.	0	0	0	0	1	0	0	0	140.8.4.8 / 29	N2
140.	8.	4.	0	0	0	1	0	0	0	0	140.8.4.16 / 28	N3
140.	8.	4.	0	0	1	0	0	0	0	0	140.8.4.32 / 27	N4

La red N3 tiene $2^4 = 16$ direcciones IP – 2 (red + broadcast) = 14.
La red N3 tiene $2^5 = 32$ direcciones IP – 2 (red + broadcast) = 30.
En total hay 14+30 = 44 direcciones IP

b)
Tabla de encaminamiento del router R2.

Adquisición	Red/mascara	Gateway	Interfaz	Métrica
C	A3/24	-	e0	1
C	A2/24	-	e1	1
R	A1/24	R1-e2	e1	2
R	A4/24	R1-e2	e1	2
R	A5/24	R1-e2	e1	4
R	N1/29	R1-e2	e1	3
R	N2/29	R1-e2	e1	3
R	N3/28	R1-e2	e1	3
R	N4/27	R1-e2	e1	3
S	0/0	R1-e2	e1	-

c)
PC2 ping a PC1.



N	Cabecera trama		ARP					IP		ICMP
	origen	destino	Q/R	MAC sender	IP sender	MAC receiver	IP receiver	origen	destino	Echo RQ/RP
1	:0320	:FFFF	Q	:0320	10.0.3.20	?	10.0.3.1	-	-	-
2	:0301	:0320	R	:0320	10.0.3.20	:0301	10.0.3.1	-	-	-
3	:0320	:0301	-	-	-	-	-	10.0.3.20	10.0.1.10	RQ
4	:0201	:FFFF	Q	:0201	10.0.2.1	?	10.0.2.2	-	-	-
5	:0202	:0201	R	:0201	10.0.2.1	:0202	10.0.2.2	-	-	-
6	:0201	:0202	-	-	-	-	-	10.0.3.20	10.0.1.10	RQ
7	:0101	:FFFF	Q	:0101	10.0.1.1	?	10.0.1.10	-	-	-
8	:0110	:0101	R	:0101	10.0.1.1	:0110	10.0.1.10	-	-	-
9	:0101	:0110	-	-	-	-	-	10.0.3.20	10.0.1.10	RQ
10	:0110	:0101	-	-	-	-	-	10.0.1.10	10.0.3.20	RP
11	:0202	:0201	-	-	-	-	-	10.0.1.10	10.0.3.20	RP
12	:0301	:0320	-	-	-	-	-	10.0.1.10	10.0.3.20	RP

d)
PC1 accede a PC3-
(i) IP origen = 10.0.1.10, IP destino = 10.0.5.30
(ii) IP origen = 140.8.4.65, IP destino = 140.8.4.69
(iii) IP origen = 140.8.4.65, IP destino = 140.8.4.69
(iv) IP origen = 10.0.1.10, IP destino = 10.0.5.30

Problema 3.1.4.

a)
10 hosts + 2 interfaces routers + dirección de red + dirección de broadcast = 14 IPs
La mínima potencia de dos superior/igual a 14 es $2^4 = 16$
=> se necesitan por lo menos 4 bits para el hostID.

6 redes publicas
La mínima potencia de dos superior/igual a 6 es $2^3 = 8$
=> se necesitan por lo menos 3 bits para el subnetID.

El total es por lo tanto 3 + 4 = 7 bits entre subnetting y hosts, la máscara del rango inicial que más se ajusta a este requisito es la /25 (25+7 = 32); al rango inicial con mascara /24 le sobraría un bit

Haciendo subnetting de 3 bits al rango inicial 202.4.4.128/25, tenemos una máscara /28 = 255.255.255.248

netID 25 bits	subnetID 3 bits	hostID 4 bits	Dirección de red/mascara	Red
202. 4. 4. 1	0 0 0	X X X X	202.4.4.128/28	N1
202. 4. 4. 1	0 0 1	X X X X	202.4.4.144/28	N2
202. 4. 4. 1	0 1 0	X X X X	202.4.4.160/28	N3
202. 4. 4. 1	0 1 1	X X X X	202.4.4.176/28	N4
202. 4. 4. 1	1 0 0	X X X X	202.4.4.192/28	N5
202. 4. 4. 1	1 0 1	X X X X	202.4.4.208/28	N6
202. 4. 4. 1	1 1 0	X X X X	202.4.4.224/28	libre
202. 4. 4. 1	1 1 1	X X X X	202.4.4.240/28	libre

b)
(i) RIPv2 porque ya usamos un rango inicial /25 y además haciendo subnetting, tenemos redes públicas con mascara /28.

(ii) El RIPv2 se activa en toda la red (pública y privada) así que, pasados unos segundos desde la activación y estando en una situación estable, el router R3 tiene una tabla de encaminamiento donde aparecen todas las redes.

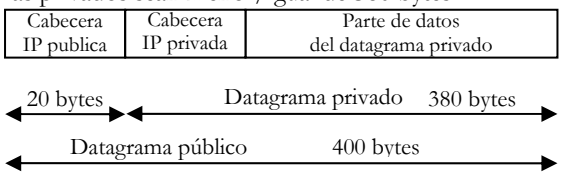
Adquisición	Red/mascara	Gateway	Interfaz	Métrica
C	A1/24	-	e0	1
C	A2/24	-	e1	1
C	A3/24	-	e2	1
R	A4/24	R4-e1	e2	2
R	A5/24	R1-e2	e0	3
R	N1/28	R1-e2	e0	2
R	N2/28	R1-e2	e0	3
R	N3/28	R1-e2	e0	4
R	N4/28	R1-e2	e0	3
R	N5/28	R1-e2	e0	4
R	N6/28	R1-e2	e0	5
S	0/0	R1-e2	e0	-

(iii) Cuando cae la red A3 y el router R3 detecta el fallo, este envía enseguida (Triggered Update activo) al router vecino R2 un mensaje RIP donde aparecen solo las redes que están afectada por este fallo y con métrica 16 (Poison Reverse activo)

Red	Mascara	Métrica
A3	24	16
A4	24	16

c)
(i) Si el túnel entre R2 y R1 usa un MTU de 400 bytes, los datagramas que se intercambian estos routers no pueden tener un tamaño más grande de 400 bytes.
Visto pero que el túnel usa una encapsulación IP en IP, el datagrama tiene una doble cabecera IP, cada una de 20 bytes.

La segunda cabecera (la pública) la pone el router de salida R2 para enviar los datos privados de los hosts de la red A5 a través del túnel de manera que Internet pueda encaminarlos. Para que el datagrama final del túnel sea menor/igual de 400 bytes, necesitamos que los datagramas privados sean menor/igual de 380 bytes.



(ii) El host podría usar el MTU path discovery para descubrir el máximo MTU posible para que no hay fragmentación en los routers.

d)

(i) Datos de entrada: GBN, vt = 50 kbit/s, D = 36000 km, Lt = 1500 bytes, To = 1 s, Pb = 10^{-5}, vp = 2×10^8 m/s

Calculo de la duración de las PDUs

Tt = Lt / vt = 1500 bytes / 50 kbit/s = 1500 * 8 / 50x10^3 = 0.24 ms

Calculo del tiempo de propagación

Tp = D / vp = 36000 km / 2×10^8 m/s = 36000 * 10^3 / 2x10^8 = 0.18 ms

Calculo del número de transmisiones

$$N_t = \frac{1}{(1-Pb)^{Lt}} \cong \frac{1}{1-Lt\times Pb} = \frac{1}{1-1500\times 8\times 10^{-5}} = 1.136$$

$$E_{GNB} = \frac{Tt}{(Nt-1)\times To + Tt} = \frac{0.24}{(1.136-1)\times 1 + 0.24} = 0.638$$

(ii) Datos de entrada: S&W, vt = 6 Mbit/s, Lt = 500 bytes, Pb = 0, vp = 2×10^8 m/s, $E_{GBN} = E_{S\&W} = 0.638$

Calculo de la duración de las PDUs.

Tt = Lt / vt = 500 bytes / 6 Mbit/s = 1500 * 8 / 6x10^6 = 0.668 ms

Calculo del tiempo de propagación

sabiendo que $E_{S\&W} = \frac{Tt}{Tt + 2\times Tp} = E_{GBN} = 0.638$, entonces $Tp = \frac{1}{2}\left(\frac{Tt}{E_{S\&W}} - Tt\right) = 189.5\ \mu s$

Calculo de la distancia

D = Tp * vp = 189.5 × 10^{-6} × 2 × 10^8 = 37.84 km

Problema 3.1.5.

a)

Interfaz física		**ARP**					**IP**		**ICMP**
@src	@dst	Query / Response	MAC sender	IP sender	MAC receiver	IP receiver	@src	@dst	Echo RQ/RP
P1-01	FF-FF	Q	P1-01	10.1.1.10	-	10.1.1.1			
R1-01	P1-01	R	P1-01	10.1.1.10	R1-01	10.1.1.1			
P1-01	R1-01						10.1.1.10	10.1.6.20	RQ
R1-03	R2-01						101.0.9.25	101.0.9.33	RQ
R2-02	FF-FF	Q	R2-02	10.1.4.1	-	10.1.4.2			
R4-01	R2-02	R	R2-02	10.1.4.1	R4-01	10.1.4.2			
R2-02	R4-01						10.1.1.10	10.1.6.20	RQ
R4-03	FF-FF	Q	R4-03	10.1.6.1	-	10.1.6.20			
P2-01	R4-03	R	R4-03	10.1.6.1	P2-01	10.1.6.20			
R4-03	P2-01						10.1.1.10	10.1.6.20	RQ
P2-01	R4-03						10.1.6.20	10.1.1.10	RP
R4-01	R2-02						10.1.6.20	10.1.1.10	RP
R2-01	R1-03						101.0.9.33	101.0.9.25	RP
R1-01	P1-01						10.1.6.20	10.1.1.10	RP

b)

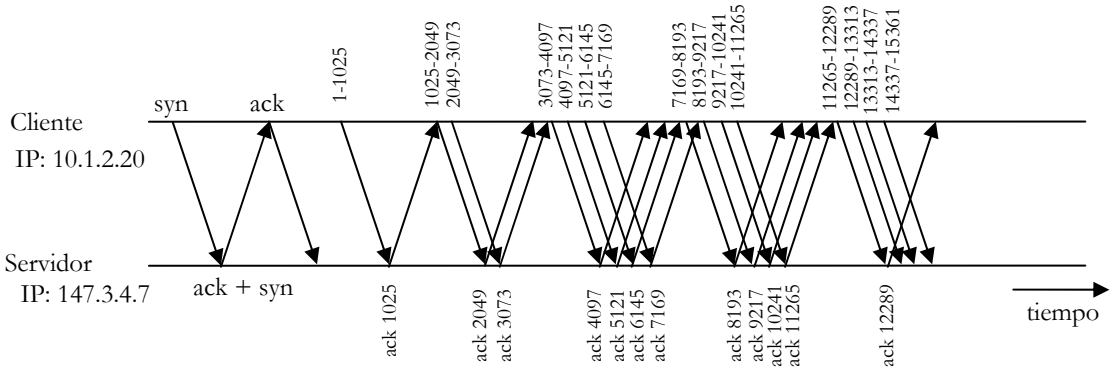
(i) Cliente IP: 10.1.2.20, puerto: 3413; Servidor IP: 147.3.4.7, puerto: 22

(ii) Cliente, buffer de recepción: 8192 bytes; Servidor, buffer de recepción: 4096 bytes

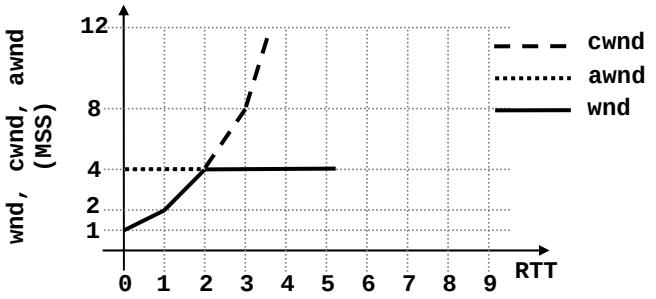
(iii) MSS = 1024 bytes

c)
La traza se ha capturado en el cliente. Si fuera en el servidor, la dirección IP del cliente sería la 101.0.9.25 (el router R1 hace PAT). Además se puede intuir porque la diferencia de tiempos entre los acks del servidor y los datos del cliente son muy pequeños (pocos ms), mientras es de alrededor de 200 ms entre los datos del cliente y los acks del servidor.

d)



e)



f)
Calculo de la velocidad efectiva
vef = min(enlace más lento, wnd/RTT) = 4096 bytes / 20 ms = 4096*8 / 0.002 = 1.638 Mbit/s

Problema 3.1.6.

a)

25 hosts + 1 interfaces routers + dirección de red + dirección de broadcast = 28 IPs
La mínima potencia de dos superior/igual a 28 es $2^5 = 32$
=> se necesitan por lo menos 5 bits para el hostID.

10 hosts + 1 interfaces routers + dirección de red + dirección de broadcast = 13 IPs
La mínima potencia de dos superior/igual a 13 es $2^4 = 16$
=> se necesitan por lo menos 4 bits para el hostID.

5 redes publicas
La mínima potencia de dos superior/igual a 5 es $2^3 = 8$
=> se necesitan por lo menos 3 bits para el subnetID.

Sumando los bits del hostID de las redes que más necesitan (5) con los bits del subnetID necesitamos en total
3 + 5 = 8 bits

Pero la máscara del rango inicial es de 25, solo hay 7 bits disponibles para el subnetID y el hostID. Hay que usar mascaras variables.

netID 25 bits	subnetID	hostID	Dirección de red/mascara	Red
80. 40. 20. 0	0 0	X X X X X	80.40.20.0/27	N1
80. 40. 20. 0	0 1	X X X X X	80.40.20.32/27	N2
80. 40. 20. 0	1 0	X X X X X	80.40.20.64/27	N3

80.	40.	20.	0	1	1	0	X	X	X	X	80.40.20.96/28	N4
80.	40.	20.	0	1	1	1	X	X	X	X	80.40.20.112/28	N5

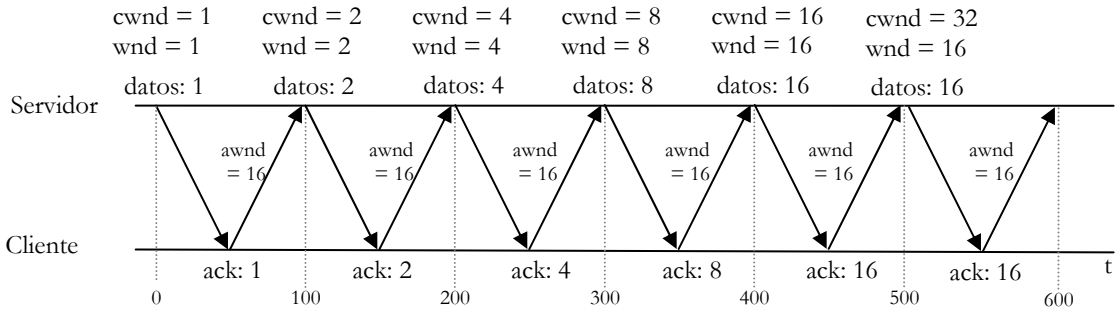
b)

Adquisición	Red/mascara	Gateway	Interfaz	Métrica
C	10.0.1.0/24	-	e0	1
C	10.0.3.0/24	-	e1	1
C	10.0.2.0/24	-	e2	1
R	10.0.0.0/24	10.0.1.2	e0	2
R	10.0.4.0/24	10.0.3.2	e1	2
R	80.40.20.0/25	10.0.3.3.	e2	3
R	10.0.5.0/24	10.0.3.3	e2	3
S	0/0	10.0.3.3	e2	-

c)

Calculo de la ventana anunciada

awnd = buffer RX / MSS = 8192 bytes / 512 bytes = 16 MSS



d)

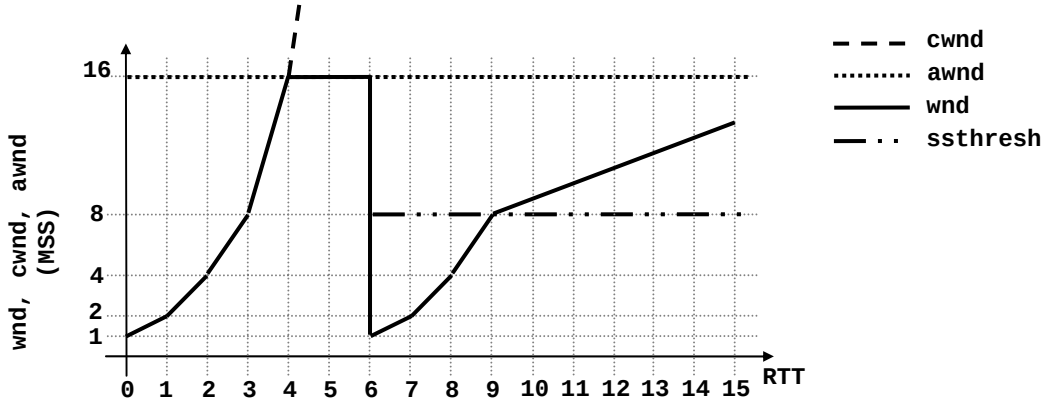
Calculo de la velocidad efectiva

vef = min(enlace más lento, wnd/RTT) = 8192 bytes / 100 ms = 8192*8 / 0.1 = 640 kbit/s

e)

Calculo del umbral cuando hay la perdida

sshtresh = max(wnd / 2, 2) = max(16 / 2, 2) = 8 MSS



Problema 3.1.7.

a)

180 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 183 IPs
La mínima potencia de dos superior/igual a 183 es $2^8 = 256$
=> se necesitan por lo menos 8 bits para el hostID.

20 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 23 IPs
La mínima potencia de dos superior/igual a 23 es $2^5 = 32$

=> se necesitan por lo menos 5 bits para el hostID.

90 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 93 IPs
La mínima potencia de dos superior/igual a 93 es $2^7 = 128$
=> se necesitan por lo menos 7 bits para el hostID.

2 interfaces routers + dirección de red + dirección de broadcast = 4 IPs
La mínima potencia de dos superior/igual a 4 es $2^2 = 4$
=> se necesitan por lo menos 2 bits para el hostID.

9 redes publicas
La mínima potencia de dos superior/igual a 9 es $2^4 = 16$
=> se necesitan por lo menos 4 bits para el subnetID.

Sumando los bits del hostID de las redes que más necesitan (8) con los bits del subnetID necesitamos en total
8 + 4 = 12 bits

Pero la máscara del rango inicial es de 22, solo hay 10 bits disponibles para el subnetID y el hostID. Hay que usar mascaras variables.

netID 22 bits	subnetID	hostID								Dirección de red/mascara	Red
100. 0. 000000	00.	X	X	X	X	X	X	X	X	100.0.0.0/24	N1
100. 0. 000000	01.	X	X	X	X	X	X	X	X	100.0.1.0/24	N2
100. 0. 000000	10.	0	X	X	X	X	X	X	X	100.0.2.0/25	N5
100. 0. 000000	10.	1	X	X	X	X	X	X	X	100.0.2.128/25	N6
100. 0. 000000	11.	0	X	X	X	X	X	X	X	100.0.3.0/25	N7
100. 0. 000000	11.	1	0	0	X	X	X	X	X	100.0.3.128/27	N3
100. 0. 000000	11.	1	0	1	X	X	X	X	X	100.0.3.160/27	N4
100. 0. 000000	11.	1	1	0	0	0	0	X	X	100.0.3.192/30	R1-R2
100. 0. 000000	11.	1	1	0	0	0	1	X	X	100.0.3.196/30	R1-R3

b)
(i) Datos de entrada: D = 400 km, vt = 1 Mbit/s, Lt = 220 bytes, La = 20 bytes, vp = 2×10^8 m/s
Calculo de la duración de las PDUs y acks
Tt = Lt / vt = 220 * 8 / 10^6 = 1.76 ms
Ta = La / vt = 20 * 8 / 10^6 = 0.16 ms
Calculo del tiempo de propagación
Tp = D / vp = 400×10^3 / 2×10^8 = 2 ms
Calculo del tiempo de ciclo
Tc = Tt + Ta + 2*Tp = 5.92 ms
Calculo de las eficiencias
$E_{S\&W}$ = Tt / Tc = 0.297
$E_{GBN} = E_{SR} = 1$

(ii) Cálculo de la ventana optima
Wopt = ceil(Tc / Tt) = 4 PDUs

(iii) Cálculo del temporizador
To ≥ Tc = 5.92 ms por lo tanto To = 6.5 ms

c)
(i) Datos de entrada: GBN, Pb = 3×10^{-5}, To = Tc = 5.92 ms
Calculo del número medio de transmisiones
Nt = 1 / $(1-Pb)^{(Lt+La)}$ = 1 / $(1-3\cdot10^{-5})^{(220 + 20)*8}$ = 1.06
Calculo de la eficiencia
E = Tt / ((Nt-1)To + Tt) = 0.834

(ii) Datos de entrada: E = 0.9
Calculo del temporizador mínimo
To = (Tt/E - Tt) / (Nt-1) = 3.26 ms

Calculo del tiempo de propagación mínimo

To = Tc = Tt + Ta + 2Tp = 3.26 ms

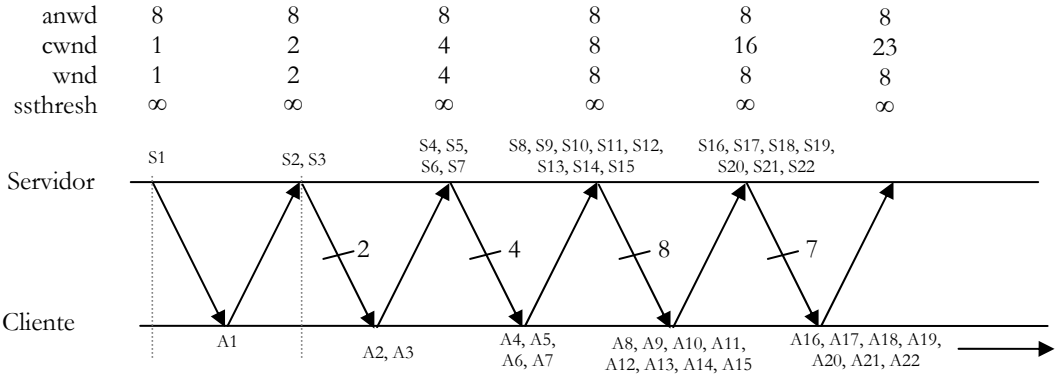
Tp = (Tc - Tt - Ta)/2 = 0.67 ms

Calculo de la distancia mínima

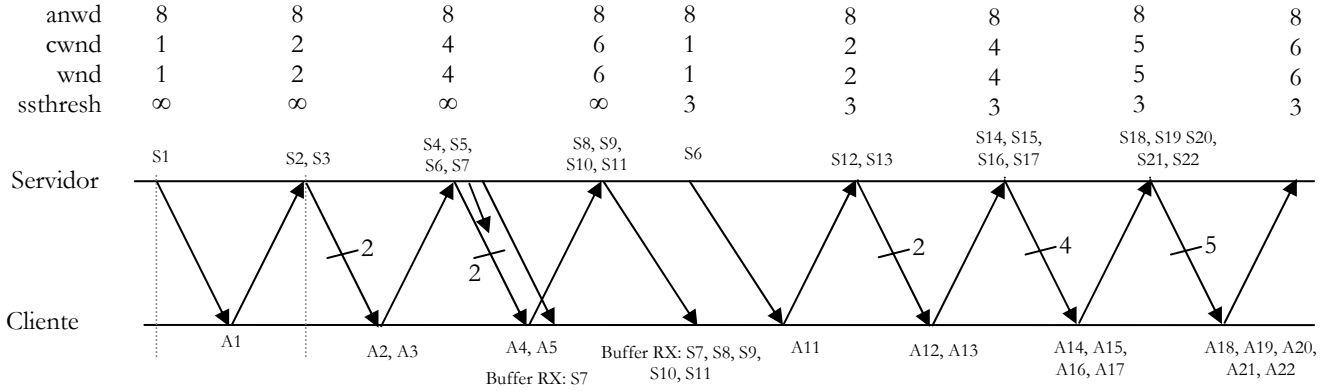
D = Tp * vp = $0.67\times10^{-3} * 2\times10^{8}$ = 134 km

d)

(i)



(ii)



Problema 3.1.8.

a)

20 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 23 IPs
La mínima potencia de dos superior/igual a 23 es $2^5 = 32$
=> se necesitan por lo menos 5 bits para el hostID.

8 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 11 IPs
La mínima potencia de dos superior/igual a 11 es $2^4 = 16$
=> se necesitan por lo menos 4 bits para el hostID.

10 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 13 IPs
La mínima potencia de dos superior/igual a 13 es $2^4 = 16$
=> se necesitan por lo menos 4 bits para el hostID.

50 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 53 IPs
La mínima potencia de dos superior/igual a 53 es $2^6 = 64$
=> se necesitan por lo menos 6 bits para el hostID.

Necesitamos coger 2 bits de subnetID para crear las 4 redes N1, N2, N3 y N4.
Sumando los bits del hostID de las redes que más necesitan (6) con los bits del subnetID necesitamos en total:
6 + 2 = 8 bits

Pero la máscara del rango inicial es de 25, solo hay 7 bits disponibles para el subnetID y el hostID. Hay que usar mascaras variables y adaptarla a cada red.

netID 25 bits	subnetID	hostiD	Direccion de red/mascara	Red
140. 10. 0. 0	0	X X X X X X	140.10.0.0/26	N4
140. 10. 0. 0	1	0 X X X X X	140.10.0.64/27	N1
140. 10. 0. 0	1	1 0 X X X X	140.10.0.96/28	N2
140. 10. 0. 0	1	1 1 X X X X	140.10.0.112/28	N3

b)

Adquisición	Red/mascara	Gateway	Interfaz	Métrica
C	10.0.1.0/24	-	e1	1
C	10.0.2.0/24	-	e2	1
C	10.0.3.0/24	-	e0	1
R	10.0.0.0/24	10.0.1.1	e1	2
R	N4	10.0.3.3	e0	2
R	N1	10.0.3.2	e0	3
R	N2	10.0.3.2	e0	3
R	N3	10.0.3.2	e0	3
R	10.0.4.0/24	10.0.3.2	e0	3
S	0.0.0.0/0	10.0.3.2	e0	-

c)

(i) Actualización cada 30 segundos

Red	Mascara	Métrica
10.0.1.0	/24	1
10.0.0.0	/24	2
10.0.2.0	/24	1

(ii) Actualización al pasar 30 segundos

Red	Mascara	Métrica
10.0.1.0	/24	16
10.0.0.0	/24	16
10.0.2.0	/24	1

(iii) Al detectar la caída, el router envía en seguida este mensaje

Red	Mascara	Métrica
10.0.1.0	/24	16
10.0.0.0	/24	16

d)

(i) IP en IP; IP publica origen 140.0.0.1, destino 160.0.0.1; IP privada origen 10.0.1.10, destino 10.0.4.40
(ii) NAT dinámico; IP origen 140.0.0.9, destino 3.3.5.5
(iii) una primera vez IP en IP; IP publica origen 160.0.0.1, destino 140.0.0.1; IP privada origen 10.0.4.40, destino 3.3.5.5
una segunda vez NAT dinámico; IP origen 140.0.0.10, destino 3.3.5.5

e)

La conexión no tiene perdidas. Habrá un transitorio donde el slow start hará que la ventana de congestión del servidor vaya aumentando hasta llegar al valor de la ventana anunciada por el cliente que es de 8192 bytes. A partir de este instante, la ventana de transmisión queda a un valor constante (régimen estacionario) de 8192 bytes.
Entonces, la velocidad efectiva de la conexión será de:

vef = min(enlance más lento, wnd / RTT) = 8192 bytes / 100 ms = 640 kbit/s

Problema 3.1.9.

a)

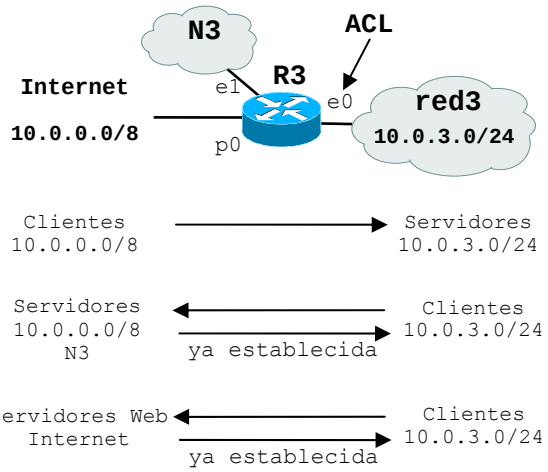
2 redes ya ocupadas: 187.4.0.0/30 y 187.4.0.4/30

10 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 13 IPs
La mínima potencia de dos superior/igual a 13 es $2^4 = 16$
=> se necesitan por lo menos 4 bits para el hostID.

50 direcciones IP para NAT, la mínima potencia de dos superior/igual a 50 es $2^6 = 64$
=> se necesitan por lo menos 6 bits para el hostID.

netID 25 bits				subnetID					hostID		Direccion de red/mascara	Red
187.	4.	0.	0	0	0	0	0	0	X	X	187.4.0.0/30	R2-ISP
187.	4.	0.	0	0	0	0	0	1	X	X	187.4.0.4/30	R3-ISP
187.	4.	0.	0	0	0	1	X	X	X	X	187.4.0.16/28	N1
187.	4.	0.	0	0	1	0	X	X	X	X	187.4.0.32/28	N2
187.	4.	0.	0	0	1	1	X	X	X	X	187.4.0.48/28	N3
187.	4.	0.	0	1	X	X	X	X	X	X	187.4.0.64 - 187.4.0.127	NAT

b)



Lista de acceso

```
permitir    TCP     10.0.0.0/8    ≥1024     10.0.3.0/24    ≤1023
permitir    TCP     10.0.0.0/8    ≤1023     10.0.3.0/24    ≥1024    establecido
permitir    TCP     N3            ≤1023     10.0.3.0/24    ≥1024    establecido
permitir    TCP     0.0.0.0/0     =80       10.0.3.0/24    ≥1024    establecido
prohibir    IP      0.0.0.0/0               0.0.0.0/0
```

c)

(i) Datos de entrada: GBN, D = 4000 km, vt = 500 kbit/s, Lt = 1500 bytes, To = 100 ms, vp = 2×10^8 m/s, Pb = 5×10^{-6}

Calculo de la duración de las PDUs

$Tt = Lt / vt = 1500 * 8 / 500\times10^3 = 24$ ms

Calculo del tiempo de propagación

$Tp = D / vp = 4000\times10^3 / 2\times10^8 = 20$ ms

Calculo del tiempo de ciclo

$Tc = Tt + 2*Tp = 64$ ms

Calculo del número medio de transmisiones

$Nt = 1 / (1-Pb)^{Lt} = 1 / (1 - 5\times10^{-6})^{1500*8} = 1.062$

Calculo de la eficiencia

$E = Tt / ((Nt-1)To + Tt) = 0.795$

(ii) Datos de entrada: S&W, D = 0, vt = 5 Mbit/s, Lt = 500 bytes, To = 1 ms

Calculo de la duración de las PDUs

$Tt = Lt / vt = 500 * 8 / 5\times10^6 = 0.8$ ms

Calculo del tiempo de propagación

$Tp = D / vp = 0$

Calculo del número medio de transmisiones data la eficiencia

$Nt = (Tt / E – Tt) / To + 1 = 1.206$

Calculo de la probabilidad de error en un bit

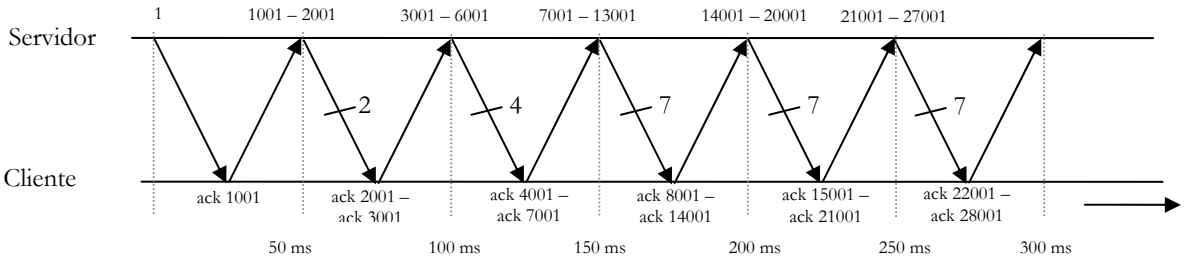
$Pb = (1 - 1 / Nt) / Tt = 4.27\times10^{-5}$

d)

(i) MSS = 1000 bytes, RTT = 50 ms, RTO = 150 ms

Datos del servidor al cliente, solo interesa $awnd_{cliente}$ = 7000 bytes = 7 MSS

anwd	7	7	7	7	7	7	7
cwnd	1	2	4	8	15	22	29
wnd	1	2	4	7	7	7	7
ssthresh	∞	∞	∞	∞	∞	∞	∞



(ii) Calculo de la velocidad efectiva

vef = min(enlace más lento, wnd / RTT) = wnd / RTT = 7000 bytes / 50 ms = 1.12 Mbit/s

Problema 3.1.10.

a)

N1: 25 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 28 IPs
La mínima potencia de dos superior/igual a 28 es $2^5 = 32$
=> se necesitan por lo menos 5 bits para el hostID.

N2: 10 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 13 IPs
La mínima potencia de dos superior/igual a 13 es $2^4 = 16$
=> se necesitan por lo menos 4 bits para el hostID.

N3: 5 hosts + 1 interfaz router + dirección de red + dirección de broadcast = 8 IPs
La mínima potencia de dos superior/igual a 8 es $2^3 = 8$
=> se necesitan por lo menos 4 bits para el hostID.

N4 = N3

Necesitamos coger 2 bits de subnetID para crear las 4 redes N1, N2, N3 y N4.
Sumando los bits del hostID de las redes que más necesitan (5) con los bits del subnetID necesitamos en total:
5 + 2 = 7 bits

Pero la máscara del rango inicial es de 26, solo hay 6 bits disponibles para el subnetID y el hostID. Hay que usar mascaras variables y adaptarla a cada red.

netID 26 bits	subnetID	hostiD	Direccion de red/mascara	Red
187. 0. 0. 00	0	X X X X X	187.0.0.0/27	N4
187. 0. 0. 00	1	0 X X X X	187.0.0.32/28	N1
187. 0. 0. 00	1	1 0 X X X	187.0.0.48/29	N2
187. 0. 0. 00	1	1 1 X X X	187.0.0.56/29	N3

b)

Tabla de encaminamiento de R2

Adquisición	Red/mascara	Gateway	Interfaz	Métrica
C	10.0.0.0/24	-	e0	1
C	N1	-	e1	1
C	N2	-	e2	1
C	187.0.0.64/30	-	p0	1
C	10.8.0.0/30	-	tun0	1
C	10.8.1.0/30	-	tun1	1
R	10.0.1.0/24	10.0.0.1	e0	2
R	10.0.2.0/24	10.0.0.1	e0	2
R	10.0.3.0/24	10.0.0.1	e0	2
R	10.1.0.0/24	10.8.0.2	tun0	2

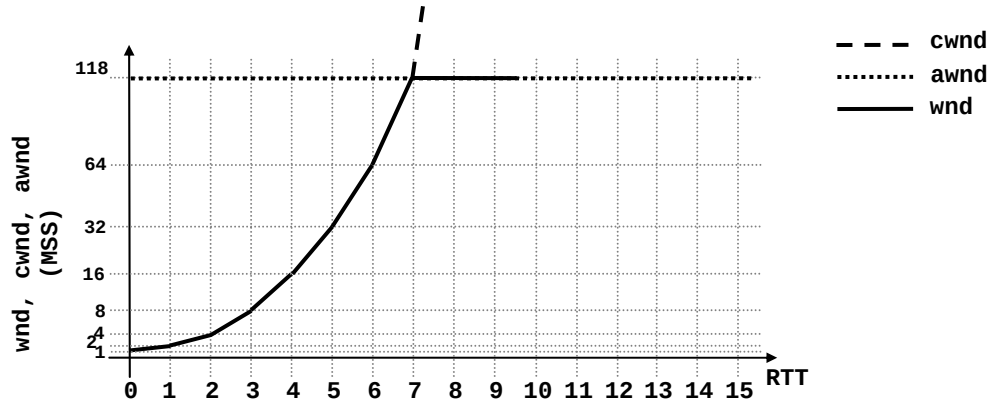
R	10.2.0.0/24	10.8.1.2	tun1	2
R	N3	10.8.0.2	tun0	2
R	N4	10.8.1.2	tun1	2
S	0.0.0.0/0	187.0.0.66	p0	-

c)

(i) IP en IP túnel0; IP publica origen 187.0.0.65, destino 187.0.0.69; IP interna origen 10.0.1.10, destino 10.1.0.10
(ii) PAT en R2; IP origen 187.0.0.65, destino 147.8.8.8
(iii) IP en IP túnel0; IP publica origen 187.0.0.69, destino 187.0.0.65; IP interna origen 10.1.0.10, destino 147.8.8.8
PAT en R2; IP origen 187.0.0.65, destino 147.8.8.8
(iv) IP en IP túnel 0; IP publica origen 187.0.0.69, destino 187.0.0.65; IP interna origen 10.1.0.10, destino 10.2.0.10
IP en IP túnel 1; IP publica origen 187.0.0.65, destino 187.0.0.73; IP interna origen 10.1.0.10, destino 10.2.0.10

d)

(i) MSS = 552 bytes
Datos del servidor al PC1, awnd depende del buffer RX de PC1 que es de 65136 bytes = 118 MS
RTT = 2 * Tp = 2 * 50 ms = 100 ms



(ii) Calculo de la velocidad efectiva
vef = min(enlace más lento, wnd / RTT) = min(20 Mbit/s, 65136 bytes / 100 ms) = 5.2 Mbit/s

Problema 3.2.1.

a)

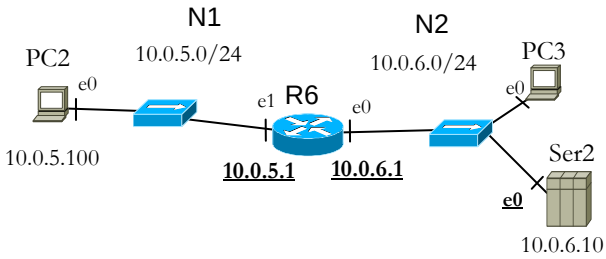
Un direccionamiento valido. Nota *: 2 para la dirección de red y la de broadcast

Red	@IP necesarias	Bits para hostID	Direcciones IPs								Red / Mascara
			netID	subnetID				hostID			
A1	5 + 2* = 7	8 = 2^3 => 3 bits	131.1.8.	0	0	0	0	0	X	X	X	131.1.8.0/29
A2	20 + 2* = 22	32 = 2^5 => 5 bits	131.1.8.	0	0	1	X	X	X	X	X	131.1.8.32/27
A3	30 + 2* = 32	32 = 2^5 => 5 bits	131.1.8.	0	1	0	X	X	X	X	X	131.1.8.64/27
PPP_{R2-R3}	2 + 2* = 4	4 = 2^2 => 2 bits	131.1.8.	0	1	1	0	0	0	X	X	131.1.8.96/30
A4	el resto		131.1.8.	1	X	X	X	X	X	X	X	131.1.8.128/25

No se usan las direcciones:
De 131.1.8.8 a 131.1.8.31
De 131.1.8.100 a 131.1.8.127

b)

PC2 ping a Ser2



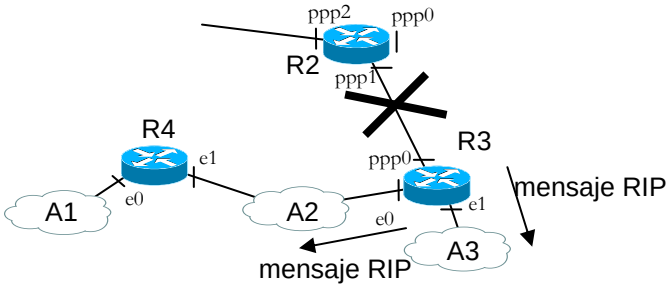
Eth		ARP					IP		ICMP
@src	@dst	Query / Response	MAC sender	IP sender	MAC receiver	IP receiver	@src	@dst	Echo RQ/RP
PC2-e0	FF-FF	Q	PC2-e0	10.0.5.100	-	10.0.5.1	-	-	-
R6-e1	PC2-e0	R	PC2-e0	10.0.5.100	R6-e1	10.0.5.1	-	-	-
PC2-e0	R6-e1	-	-	-	-	-	10.0.5.100	10.0.6.10	RQ
R6-e0	FF-FF	Q	R6-e0	10.0.6.1	-	10.0.6.10	-	-	-
Ser2-e0	R6-e0	R	R6-e0	10.0.6.1	Ser2-e0	10.0.6.10	-	-	-
R6-e0	Ser2-e0	-	-	-	-	-	10.0.5.100	10.0.6.10	RQ
Ser2-e0	R6-e0	-	-	-	-	-	10.0.6.10	10.0.5.100	RP
R6-e1	PC2-e0	-	-	-	-	-	10.0.6.10	10.0.5.100	RP

c)

Si en los routers no está activa la agregación de rutas (sumarización), la tabla de encaminamiento es la siguiente:

Adquisición	Red / máscara	Gateway	Interfaz	Métrica
C	A3 , 131.1.8.64/27	-	e1	1
C	A2 , 131.1.8.32/27	-	e0	1
C	PPP_{R2-R3} , 131.1.8.96/30	-	ppp0	1
R	A1 , 131.1.8.0/29	R4-e1	e0	2
R	10.0.3.0/24	R2-ppp1	ppp0	2
R	VLAN1 , 10.0.1.0/24	R2-ppp1	ppp0	3
R	VLAN2 , 10.0.2.0/24	R2-ppp1	ppp0	3
R	A4 , 131.1.8.128/25	R2-ppp1	ppp0	3
R	10.0.4.0/24	R2-ppp1	ppp0	3
R	N1 , 10.0.5.0/24	R2-ppp1	ppp0	4
R	N2 , 10.0.6.0/24	R2-ppp1	ppp0	4
S	0.0.0.0/0	R2-ppp1	ppp0	-

d)



Split horizon está activo, así que enviará a sus vecinos A2 y A3, dos mensajes RIP (uno por cada sub-red) que contiene solo la parte de la tabla de encaminamiento que no ha aprendido de A2 y de A3 respectivamente.

Poison reverse está también activo así que en los dos mensajes se especifica que la métrica es ahora infinito (16). También triggered update está activo, así que los dos mensajes se envían inmediatamente sin esperar los 30 segundos entre una actualización y la siguiente.

Los dos mensajes a A2 y A3 son iguales y señalan la caída del enlace entre R3 y R2 y por lo tanto la indisponibilidad de todas las rutas de R3 donde R2 aparecía como gateway.

Red	Máscara	Métrica
131.1.8.96	/30	16
10.0.3.0	/24	16
10.0.1.0	/24	16
10.0.2.0	/24	16
131.1.8.128	/25	16
10.0.4.0	/24	16
10.0.5.0	/24	16
10.0.6.0	/24	16

e)
El router R2 tiene el NAT activo, así que la dirección privada de PC1 10.0.2.55 se convierte en 200.0.0.13. La IP destino es de Internet y se mantiene.

@IP destino	@IP origen
200.20.10.135	200.0.0.13

f)
Entre el router R2 y el router R5 hay un túnel activo, así que se encapsula el datagrama con direcciones privadas destino 10.0.6.10 y origen 10.0.2.55 en un datagrama con direcciones publicas destino 200.0.0.16 y origen 200.0.0.13 que son las dos direcciones a los extremos del túnel.

Túnel		@IP privadas	
@IP destino	**@IP origen**	**@IP destino**	**@IP origen**
200.0.0.16	200.0.0.13	10.0.6.10	10.0.2.55

Problema 3.2.2.

a)
Mascara inicial 22.
50 usuarios + interfaces de los routers + IPred + IPbroadcast < 64 = 2^6 --> 6 bits para el hostID.
Quedan 4 bits para el subnetID => 2^4 = 16 subredes posibles
Hay 9 subredes, 4 bits son suficientes
Mascara subredes = 22 + 4 = 26

netID							subnetID				hostID						@IP red	@IP broadcast
Peso	128	64	32	16	8	4	2	1.	128	64	32	16	8	4	2	1		
10.8.	0	0	0	1	1	1	0	0.	0	0	X	X	X	X	X	X	10.8.28.0	10.8.28.63
10.8.	0	0	0	1	1	1	0	0.	0	1	X	X	X	X	X	X	10.8.28.64	10.8.28.127
10.8.	0	0	0	1	1	1	0	0.	1	0	X	X	X	X	X	X	10.8.28.128	10.8.28.191
10.8.	0	0	0	1	1	1	0	0.	1	1	X	X	X	X	X	X	10.8.28.192	10.8.28.255
10.8.	0	0	0	1	1	1	0	1.	0	0	X	X	X	X	X	X	10.8.29.0	10.8.29.63
10.8.	0	0	0	1	1	1	0	1.	0	1	X	X	X	X	X	X	10.8.29.64	10.8.29.127
10.8.	0	0	0	1	1	1	0	1.	1	0	X	X	X	X	X	X	10.8.29.128	10.8.29.191
10.8.	0	0	0	1	1	1	0	1.	1	1	X	X	X	X	X	X	10.8.29.192	10.8.29.255
10.8.	0	0	0	1	1	1	1	0.	0	0	X	X	X	X	X	X	10.8.30.0	10.8.30.63
10.8.	0	0	0	1	1	1	1	0.	0	1	X	X	X	X	X	X	10.8.30.64	10.8.30.127
10.8.	0	0	0	1	1	1	1	0.	1	0	X	X	X	X	X	X	10.8.30.128	10.8.30.191
10.8.	0	0	0	1	1	1	1	0.	1	1	X	X	X	X	X	X	10.8.30.192	10.8.30.255
10.8.	0	0	0	1	1	1	1	1.	0	0	X	X	X	X	X	X	10.8.31.0	10.8.31.63
10.8.	0	0	0	1	1	1	1	1.	0	1	X	X	X	X	X	X	10.8.31.64	10.8.31.127
10.8.	0	0	0	1	1	1	1	1.	1	0	X	X	X	X	X	X	10.8.31.128	10.8.31.191
10.8.	0	0	0	1	1	1	1	1.	1	1	X	X	X	X	X	X	10.8.31.192	10.8.31.255

Red	IP/mascara
N1	10.8.28.0/26

N2	10.8.28.64/26
N3	10.8.28.128/26
N4	10.8.28.192/26
N5	10.8.29.0/26
N6	10.8.29.64/26
N_R4-R5	10.8.29.128/26
N7	10.8.29.192/26
N8	10.8.30.0/26

b)
La interfaz fe0 del router R5 es un puerto de trunk para configurar 3 VLANs, por lo tanto hay que asignarle 3 direcciones IP distintas.

Interfaz	**IP/mascara**
ppp0	10.8.30.129/26
fe0.1	147.83.31.1/28
fe0.2	147.83.31.17/28
fe0.3	147.83.31.33/28

c)
Mensajes periódicos de R3 a R4

R3 -> R4 con split horizon

red	mascara	métrica
N2	/26	1
N3	/26	1

R3 -> R4 sin split horizon

red	mascara	métrica
N2	/26	1
N3	/26	1
N6	/26	1

d)
Tabla de encaminamiento de R4

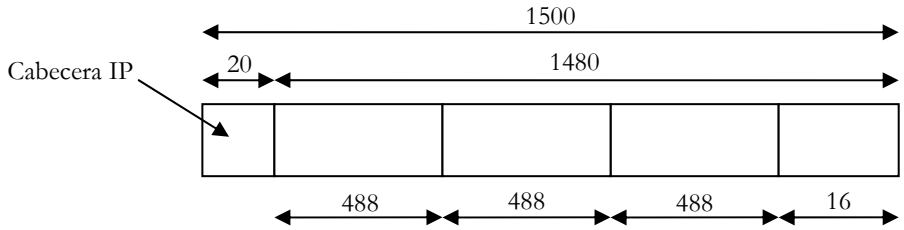
Adquisición	Red/mascara	Gateway	Interfaz	Métrica
C	N5/26	-	e1	1
C	N6/26	-	e0	1
C	N_R4-R5/26	-	ppp0	1
R	N1/26	R3-e2 (o R2-e1)	e0 (o e1)	3
R	N2/26	R3-e2	e0	2
R	N3/26	R3-e2	e0	2
R	N4/26	R2-e1	e1	2
R	N7/26	R5-ppp0	ppp0	2
R	N8/25	R5-ppp0	ppp0	2
R	N9/28	R5-ppp0	ppp0	2
R	N10/28	R5-ppp0	ppp0	2
R	N11/28	R5-ppp0	ppp0	2
S	0.0.0.0/0	R5-ppp0	ppp0	-

e)
R7 recibe el datagrama de 1500 bytes de PC2 y mirando la tabla de encaminamiento sabe que debe reenviarlo por la red N8 hacia PC3. Siendo el datagrama de 1500 bytes más grande de la MTU de 512 bytes de la red N8, R7 debe fragmentar. Siendo el flag DF desactivo, R7 puede fragmentar.
Del datagrama original, R7 quita la cabecera IP y fragmenta lo que queda. Cada fragmento debe ser múltiplo de 8. Por lo tanto se coge la longitud máxima de un fragmento que es 492 bytes (los restantes 20 bytes de los 512 bytes sirven para la cabecera IP) y se ve si es múltiplo de 8.

492 / 8 = 61.5 ---> número no entero.

Se coge el múltiplo entero más grande menor de 492 bytes. Eso es coger la parte entera de la división anterior y multiplicarla por 8

61 * 8 = 488



Numero fragmento	Flag DF	Flag MF	Offset	Longitud total
1	0	1	0	508
2	0	1	488	508
3	0	1	976	508
4	0	0	1464	36

f)

(i) 147.83.31.12 ya es una dirección pública, se aplica PAT
IP origen: 160.0.0.1
IP destino: 147.83.31.12

(ii) Tunneling
IP origen: 160.0.0.1
IP destino: 140.0.0.1

Problema 3.2.3.

a)

Calculo del mínimo valor de hostID para cada red

	Usuarios	Interfaz router	Red y broadcast	Total IP	Múltiplo 2	hostID
Red R-R1	0	2	2	4	$2^2 = 4$	2
Red R-R2	0	2	2	4	$2^2 = 4$	2
Red 1	5	1	2	8	$2^3 = 8$	3
Red 2	5	1	2	8	$2^3 = 8$	3
Red 3	5	1	2	8	$2^3 = 8$	3
Red 4	28	1	2	31	$2^5 = 32$	5
Red 5	50	1	2	53	$2^6 = 64$	6

Para asignar las IP conviene empezar con las redes con máscaras más pequeñas

netID	subID		hostID						@IP red	@IP broadcast	Red
peso	128	64	32	16	8	4	2	1			
202. 0. 1.	1	0	X	X	X	X	X	X	202.0.1.128	202.0.1.191	Red 5
202. 0. 1.	1	1	0	X	X	X	X	X	202.0.1.192	202.0.1.223	Red 4
202. 0. 1.	1	1	1	0	0	X	X	X	202.0.1.224	202.0.1.231	Red 3
202. 0. 1.	1	1	1	0	1	X	X	X	202.0.1.232	202.0.1.239	Red 2
202. 0. 1.	1	1	1	1	0	X	X	X	202.0.1.240	202.0.1.247	Red 1
202. 0. 1.	1	1	1	1	1	0	X	X	202.0.1.248	202.0.1.251	Red R-R1
202. 0. 1.	1	1	1	1	1	1	X	X	202.0.1.252	202.0.1.255	Red R-R2

Las mascara son

- 2 bits de hostID => mascara 32 – 2 = 30
- 3 bits de hostID => mascara 32 – 3 = 29
- 5 bits de hostID => mascara 32 – 5 = 27
- 6 bits de hostID => mascara 32 – 6 = 26

/24	hostID								Mascara	Redes
peso	128	64	32	16	8	4	2	1		
255.255.255.	1	1	1	1	1	1	0	0	255.255.255.252	Red R-R1 y Red R-R2

255.255.255.	1	1	1	1	1	0	0	0	255.255.255.248	Red 1, Red 2 y Red 3
255.255.255.	1	1	1	0	0	0	0	0	255.255.255.224	Red 4
255.255.255.	1	1	0	0	0	0	0	0	255.255.255.192	Red 6

b)

(i) PC1 ping a PC3
N5: @IP origen 10.0.3.10, @IP destino 10.0.11.30
Internet: @IP origen 201.0.1.1, @IP destino 201.0.1.2 (IPenIP @IP origen 10.0.3.10, @IP destino 10.0.11.30)
N11: @IP origen 10.0.3.10, @IP destino 10.0.11.30

(ii) PC1 ping a Ser2
N5: @IP origen 10.0.3.10, @IP destino 209.85.135.99
Internet: @IP origen 202.0.1.10, @IP destino 209.85.135.99 (NAT dinámico en R1)

(iii) PC1 ping a PC3
N11: @IP origen 10.0.11.30, @IP destino 209.85.135.99
Internet: @IP origen 201.0.2.1, @IP destino 209.85.135.99 (PAT en R2)

c)

Direcciones IP internas de los routers, 3 direcciones cada interfaz porque hay 3 VLANs.

R2:	10.0.11.1/24	10.0.12.1/24	10.0.13.1/24
R3:	10.0.21.1/24	10.0.22.1/24	10.0.23.1/24
R4:	10.0.31.1/24	10.0.32.1/24	10.0.33.1/24

Problema 3.2.4.

a)

5 servidores públicos + router + broadcast + red = 8 @IP --> 3 bits para hostID, mascara 29
200.0.0.0/29

También se pueden asignar direcciones privadas, por ejemplo 192.168.0.0/29 y configurar un NAT estático (o también PAT estático siendo los puertos de los servidores distintos) en el router R1. Es fundamental que sea de tipo estático para que cada servidor tenga una única dirección visible desde Internet (o una tupla dirección-puerto en el caso de PAT).

Redes privadas usamos direcciones privadas
10.0.0.0/24 para red R1-R2
10.0.1.0/24 para dirección
10.0.2.0/24 para contabilidad
10.0.3.0/24 para operativo
10.0.4.0/24 para servicios informáticos

Se necesitan 8 direcciones públicas para direccionamiento

b)

Se configura PAT dinámico (o NAT dinámico por puertos) en el router R1 usando la dirección publica de la interfaz ppp0.

c)

R1-ppp0: 200.0.0.9/30, R1-fe0: 200.0.0.1/29, R1-fe1: 10.0.0.1/24
R2-fe0: 10.0.0.2/24, R2-fe1: 10.0.1.1/24
R2-fe2.1: 10.0.2.1/24, R2-fe2.2: 10.0.3.1/24, R2-fe2.3: 10.0.4.1/24

	Destino	Mascara	Gateway	Interf	Hop
ISP-R1	80.0.0.0	30	-	ppp0	1
N2	200.0.0.0	29	-	fe0	1
R1-R2	10.0.0.0	24	-	fe1	1
N1	10.0.1.0	24	10.0.0.2	fe1	2
VLAN1	10.0.2.0	24	10.0.0.2	fe1	2
VLAN2	10.0.3.0	24	10.0.0.2	fe1	2
VLAN3	10.0.4.0	24	10.0.0.2	fe1	2
	0.0.0.0	0	80.0.0.2	ppp0	-

Tabla R1

	Destino	Mascara	Gateway	Interf	Hop
R1-R2	10.0.0.0	24	-	fe0	1
N1	10.0.1.0	24	-	fe1	1
VLAN1	10.0.2.0	24	-	fe2.1	1
VLAN2	10.0.3.0	24	-	fe2.2	1
VLAN3	10.0.4.0	24	-	fe2.3	1
N2	200.0.0.0	29	10.0.0.1	fe0	2
	0.0.0.0	0	10.0.0.1	fe0	-

Tabla R2

d)

1) Interfaz fe0 out (también se puede agrupar con 3) y configurar en ppp0 in)

IPdestino/masc	puerto_destino	IPorigen/masc	puerto_origen	protocolo	estado	acepta/rechaza
200.0.0.0/29	http	0.0.0.0/0	>1023	TCP	any	acepta
200.0.0.0/29	DNS	0.0.0.0/0	>1023	TCP	any	acepta
200.0.0.0/29	mail	0.0.0.0/0	>1023	TCP	any	acepta
200.0.0.0/29	fax	0.0.0.0/0	>1023	TCP	any	acepta
200.0.0.0/29	ssh	0.0.0.0/0	>1023	TCP	any	acepta
0.0.0.0/0	any	0.0.0.0/0	any	any	any	rechaza

2) Interfaz fe1 in

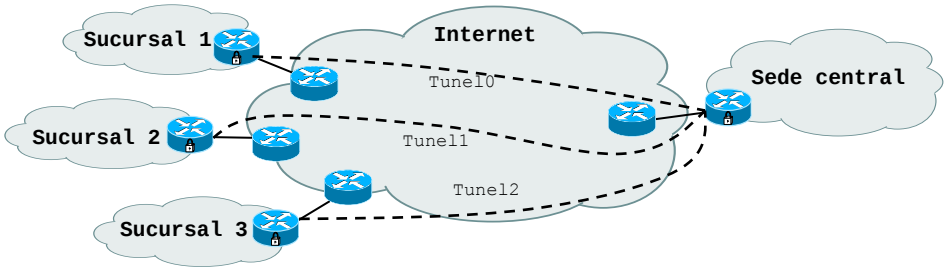
0.0.0.0/0	<1024	10.0.1.0/24	>1023	any	any	acepta
0.0.0.0/0	<1024	10.0.2.0/24	>1023	any	any	acepta
0.0.0.0/0	<1024	10.0.3.0/24	>1023	any	any	acepta
0.0.0.0/0	any	0.0.0.0/0	any	any	any	rechaza

3) Interfaz fe1 out

10.0.1.0/24	>1023	0.0.0.0/0	<1024	any	established	acepta
10.0.2.0/24	>1023	0.0.0.0/0	<1024	any	established	acepta
10.0.3.0/24	>1023	0.0.0.0/0	<1024	any	established	acepta
0.0.0.0/0	any	0.0.0.0/0	any	any	any	rechaza

e)

Tres túneles



f)

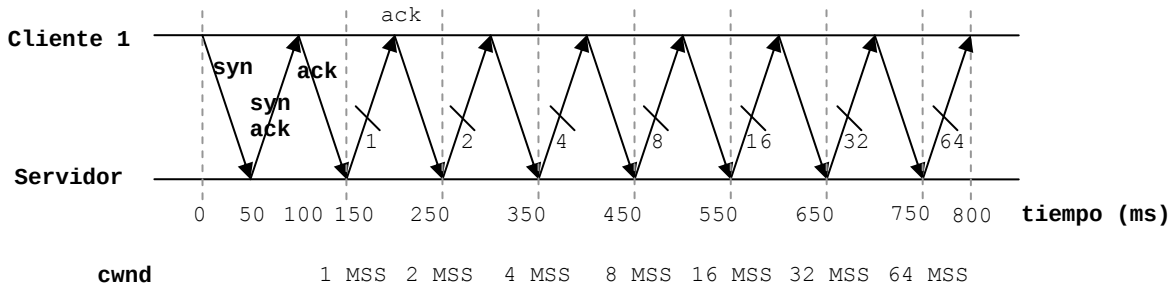
Direcciones de los túneles:

Tunel0 entre 84.0.0.1 y 84.0.1.1, interfaz tun0 en R1: 10.100.0.1/24, interfaz tun0 en R3: 10.100.0.2/24
Tunel1 entre 84.0.0.1 y 84.0.2.1, interfaz tun0 en R1: 10.100.1.1/24, interfaz tun0 en R4: 10.100.1.2/24
Tunel2 entre 84.0.0.1 y 84.0.3.1, interfaz tun0 en R1: 10.100.2.1/24, interfaz tun0 en R5: 10.100.2.2/24

Problema 3.3.1.

a)

Datos de entrada: MSS = 512 butes, RTT = 2*50 ms = 100 ms



b)

(i) Hay que determinar si la velocidad máxima de transmisión la impone el TCP o el nivel físico.

vef = min(enlace más lento, wnd / RTT)

El enlace más lento entre Servidor y Cliente 1 es el de 8 Mbps.

La ventana de transmisión se calcula como wnd = min(cwnd, awnd)

Visto que no hay perdidas, el máximo valor alcanzable por la ventana de transmisión wnd lo impone la ventana anunciada awnd es decir 65536 bytes.

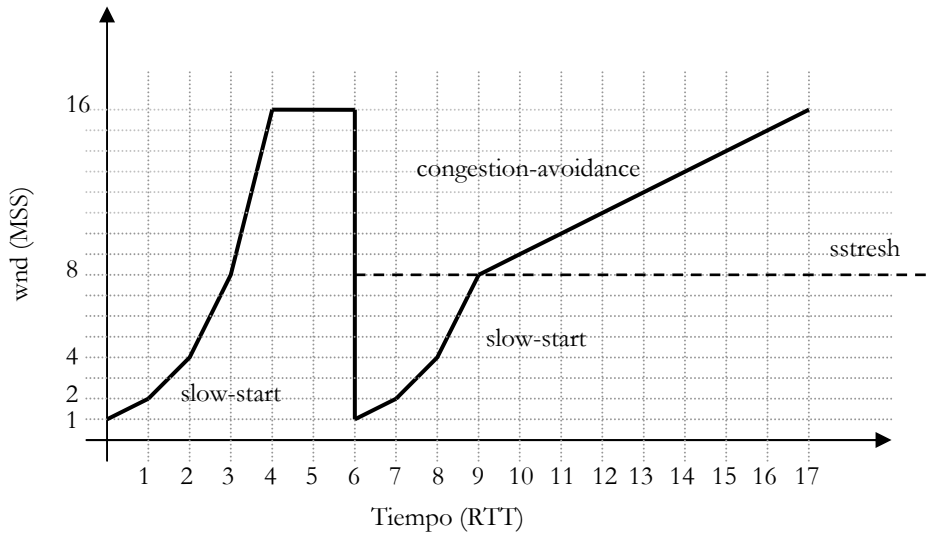
vef = min(8 Mbps, 65535*8 / 0.1) = min(8 Mbps, 5.24 Mbps) = 5.24 Mbps

(ii) La máxima ventana de transmisión es de 65535 bytes.
(iii) En una ventana de transmisión máxima caben 65535 / 512 = 128 segmentos.
(iv) Visto que la ventana va duplicándose cada RTT, para alcanzar 128 segmentos, se tardan 7 RTT (27 = 128)
Así que se tardan 7 RTT = 700 ms para alcanzar la ventana máxima.
A estos hay que sumarle el establecimiento de la conexión con el three-way handshaking que es de 150 ms.
Total 850 ms.

c)

vef = min(enlace más lento, wnd / RTT) = min(640 kbps, 16384 * 8 / 0.1) = min(640 kbps, 1.31 Mbps)
vef = 640 kbps, la impone el nivel físico
Wopt = ceil(640 kbps * RTT)/(512*8)) = 16

d)



Problema 3.3.2.

a)

(i) MSS de 1460 bytes
(ii) La ventana anunciada awnd es de 64240 bytes, como no hay pedidas, esta coincide con la ventana de transmisión wnd=64250 bytes = 44 MSS
(iii) vef = min(enlace más lento, wnd / RTT) = min(10Mbps, 64240 * 8 / (2 * 50 ms)) = 5.14 Mbps
(iv) Duración = 726857231 bytes * 8 / 5.14Mbps = 1131 s

b)

Muy probablemente en el PC1 porque aparece la IP privada de PC1. Si fuera en el servidor público, PC1 debería tener una IP pública.

c)

En total en la red Ethernet hay 5 servidores transmitiendo; considerando que hay una eficiencia del 100%, eso hace que cada servidor puede transmitir durante un 20% del tiempo. Eso hace bajar la velocidad efectiva a

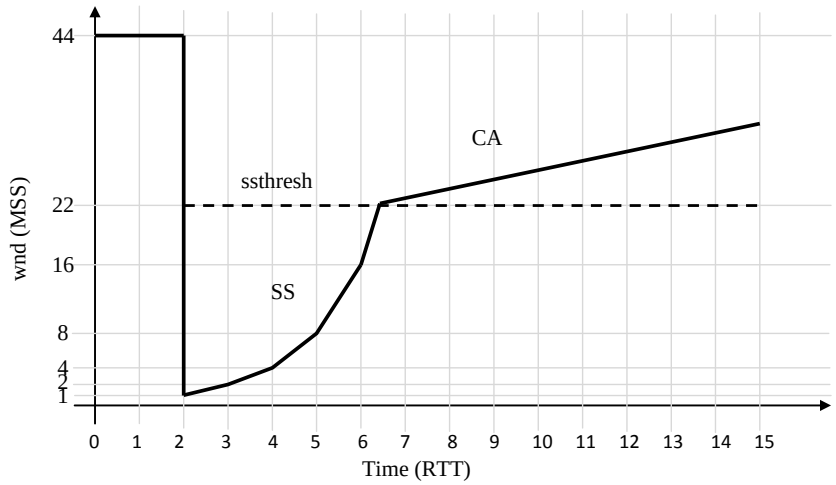
vef = min(enlace más lento, wnd / RTT) = min(10 Mbps * 20%, 64240 * 8 / (2 * 50 ms)) =
= min(2 Mbps, 5.14 Mbps) = 2 Mbps
Duración = 726857231 bytes * 8 / 2Mbps = 2907 s

d)

Con un windows scale de 4, la velocidad efectiva es

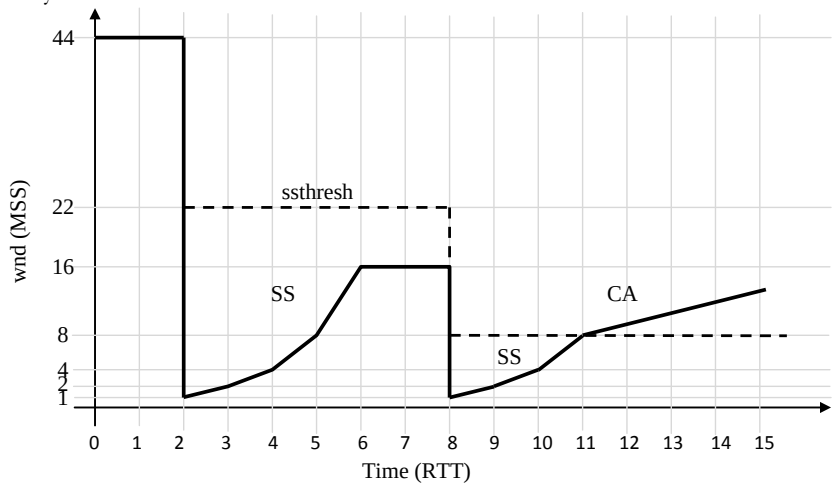
vef = min(10Mbps, 64240 * 8 * 4/ (2 * 50 ms)) = min(10 Mbps, 20.5 Mbps) = 10 Mbps
Duración = 726857231 bytes * 8 / 10 Mbps = 581 s

e)



f)

cwnd = 23360 bytes = 16 MSS



Problema 3.3.3.

a)

Datos de entrada: GBN, Pb = 10^{-6}, Lt = 1500 bytes, La = 40 bytes, vt = 20 Mbps, To = 110 ms, RTT (2*Tp) = 100ms

(i) Calculo del número medio de transmisiones

$Nt = 1 / (1-Pb)^{Lt+La} = 1 / (1-10^{-6})^{(1500+40)*8} = 1.012$

Calculo de la duración de las PDUs y de los acks.

$Tt = Lt / vt = 1500*8 / 20•106 = 0.6$ ms

$Ta = La / vt = 40*8 / 20•106 = 0.016$ ms

Calculo de la eficiencia

$E = Tt / ((Nt-1)*To + Tt) = 0.6 / ((1.012-1)*110+0.6) = 0.31$

(ii) Calculo de la velocidad efectiva conocida la eficiencia

$vef = vt * E = 20$ Mbps $* 0.31 = 6.2$ Mbps

(iii) Calculo del tiempo de ciclo

$Tc = 2*Tp + Ta + Tt = 100 + 0.016 + 0.6 = 100.616$ ms

Calculo de la ventana óptima

$Wopt = ceil(Tc / Tt) = ceil(100.616 / 0.6) = 168$ PDUs

(iv) Intuitivamente, bajaría la eficiencia porque en el cálculo de E, Tt sería más pequeño.

Efectivamente con Lt = 100bytes

$Nt = 1.0011$

$E = 0.245$

b)

Datos de entrada: TCP, MSS = 1460 bytes, RTT (2*Tp) = 100ms

(i) Con window scale desactivado y sin errores, el valor de la ventana máxima es de 65535 bytes debido al hecho que el campo de la ventana enunciada en una cabecera TCP ocupa 16 bits y por lo tanto el número máximo representable con este espacio es de 2^{16}-1=65535.

vef = min(enlace mas lento, wnd / RTT) = min(20 Mbps, 65535 * 8/ 100 ms) = min(20 Mbps, 5.24 Mbps)

vef = 5.24 Mbps

Con TCP la vef es menor. Efectivamente con GBN era 6.2 Mbps, con TCP es 5.24 Mbps.

(ii) Con window scale a 8, la ventana máxima seria 65535*8 bytes y por lo tanto

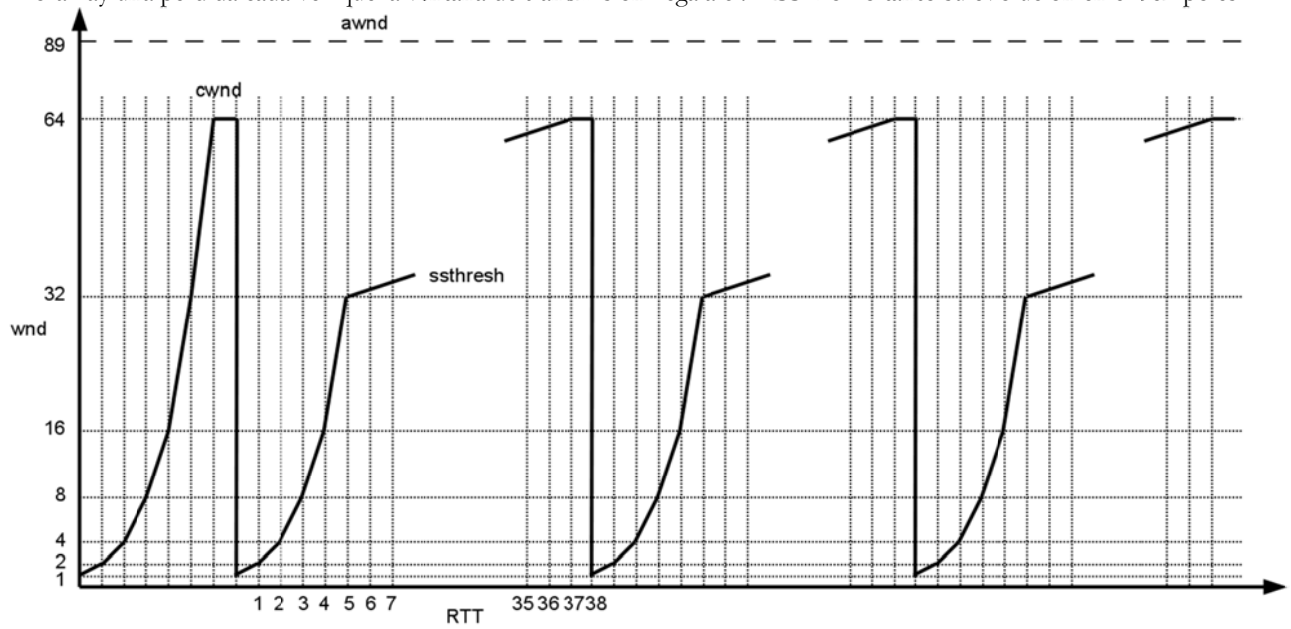
vef = min(enlace mas lento, wnd / RTT) = min(20 Mbps, 65535*8*8/ 100 ms) = min(20 Mbps, 41.94 Mbps)

vef = 20 Mbps

Ahora con TCP la vef es superior al caso con GBN.

(iii) Con window scale a 2, la ventana máxima es 65535*2 = 89.7 MSS

Ahora hay una perdida cada vez que la ventana de transmisión llega a 64 MSS. Por lo tanto su evolución en el tiempo es



(iv) Aproximadamente será

vef = (1 + 2 + 4 + 8 + 16 + 32 + 33 + 34 +...+ 64)MSS / 38 RTT = 4.96 Mbps

c)

Datos de entrada: UDP, 256 bytes de datos cada 100ms

(i) Con UDP no hay ningún tipo de control sobre la velocidad, por lo tanto el sistema va al máximo permitido. En este caso son 256 bytes cada 100 ms

vef = 256 bytes * 8 / 100 ms = 20.5 kbps

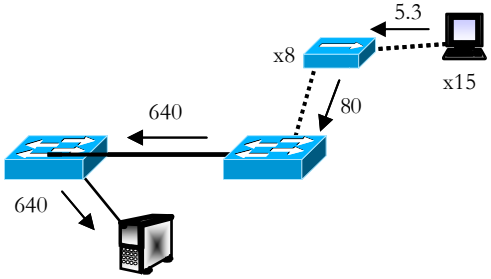
(ii) Como se pierde un 10% y no hay recuperación

vef = 20.5 kbps – 20.5 kbps * 0.1 = 18.45 kbps

Problema 3.4.1.

a)

La eficiencia de los hubs es del 80% entonces, a su máxima capacidad, transmiten 80 Mbps a S3. Como hay 8 hubs conectados a S3, en el enlace S1-S3 hay 8x80 = 640 Mbps. Como es inferior a la capacidad del enlace (1Gbps), no hay congestión en S3. Como transmiten solo estaciones de la VLAN1 al servidor (que es también de la VLAN1), las tramas van directamente de S1 al servidor (sin pasar por el router). Siendo el enlace S1-servidor de 1 Gbps, no hay congestión en S1.



Por lo tanto:

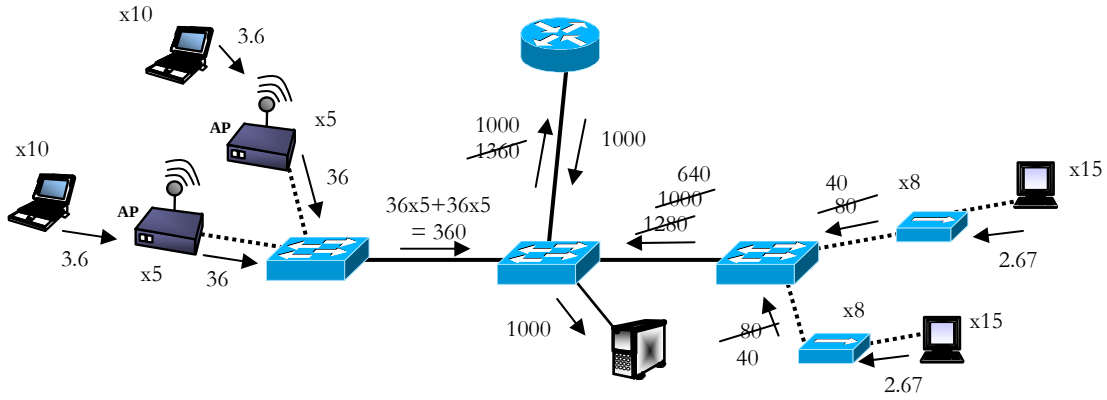
(i) Los cuellos de botellas son los hubs

(ii) El CSMA/CD de las estaciones controla y reparte los 80 Mbps de cada hub.

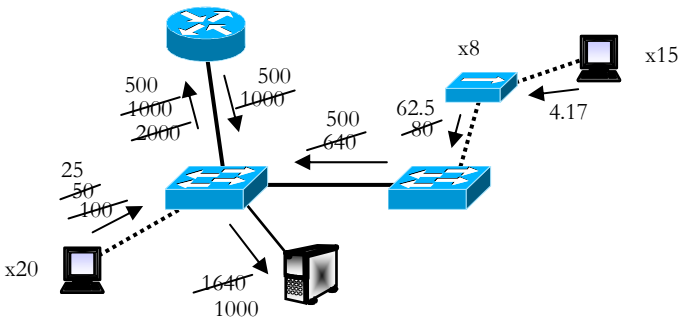
(iii) Las 15 estaciones de cada hub se reparten equitativamente los 80 Mbps, por lo tanto 80/15 = 5.3 Mbps.

b)
Empezamos con la parte izquierda de la red. La eficiencia de los APs es del 66.7% entonces, a su máxima capacidad, transmiten 54x0.667 = 36 Mbps a S2 (que es inferior a la capacidad del enlace FastEthernet). Como hay 5 APs en la VLAN2 y otros 5 en la VLAN3, a la salida de S2 hay 36x5+36x5 = 360 Mbps. Como es inferior a la capacidad del enlace S2-S1 (1 Gbps), no hay congestión en S2.
A la derecha hay también estaciones de las VLAN2 y VLAN3. Como en el caso del punto A, cada hub transmite 80 Mbps a S3. Como hay 8 hubs en la VLAN2 y otros 8 en la VLAN3, a la salida de S3 hay 80x8+80x8 = 1280 Mbps. Como se supera la capacidad del enlace (1 Gbps), S3 solo transmite 1000 Mbps.
A diferencia del caso anterior, ahora las estaciones pertenecen a VLAN distintas del servidor por lo tanto hay que pasar por el enlace de trunk del router. Sumando lo que entra en S1, por el trunk debería pasar 1000+360 = 1360 Mbps. Como supera la capacidad del trunk (1 Gbps), S1 debe hacer control de flujo y limitar la transmisión a 1000 Mbps. A partir de aquí no hay más restricciones siendo el enlace S1-servidor de 1 Gbps.

Por lo tanto:
(i) El cuello de botella general es el trunk S1-R1. En WiFi el cuello son los APs.
(ii) El control de flujo de S1 reparte los 1000 Mbps del trunk de manera equitativa entre los dos enlaces de entrada (S2-S1 y S3-S1). Como por el enlace S2-S1 pasan 360 Mbps, que es menor de la mitad del trunk (500 Mbps), S1 solo limita el enlace S3-S1 a 1000-360 = 640 Mbps. Siendo el enlace FDX, el control de flujo se hace con tramas de pausa. En los APs la velocidad se regula por CSMA/CA.
(iii) Volviendo atrás, S3 reparte estos 640 Mbps entre los 16 hubs conectados (640/16 = 40 Mbps). Como estos enlaces son HDX, S3 hace control de flujo con tramas de jabber. Las 15 estaciones de cada hub se reparten los 40 Mbps (40/15 = 2.67 Mbps). Por el otro lado, S2 no necesita hacer control de flujo. Los 36 Mbps de cada APs se reparten entre las 10 estaciones (36/10 = 3.6 Mbps) a través del CSMA/CA.



c)
Para las estaciones de la VLAN1 es como el caso A y por el enlace S3-S1 se intentan transmitir 640 Mbps. Las 20 estaciones de la VLAN4 tienen enlaces FastEthernet e intentan transmitir a 100 Mbps. Estas estaciones no pertenecen a la red del servidor y por lo tanto deben pasar por el trunk. Siendo 20 las estaciones, deberían pasar por el trunk 100x20 = 2000 Mbps que supera su capacidad. S1 limita entonces las estaciones a 50 Mbps cada una (1000/20 = 50 Mbps). Estos 1000 Mbps de vuelta del router deben sumarse a los 640 Mbps que vienen de la VLAN1 e ir al servidor (1000+640 = 1640 Mbps). Como supera la capacidad del enlace S1-servidor (1 Gbps), S1 debe limitar las entradas.



Por lo tanto:
(i) El cuello de botella general es el enlace S1-servidor
(ii) S1 usa control de flujo (tramas de pausa) para repartir la capacidad de 1000 Mbps entre los dos enlaces de entrada (S3-S1 y R1-S1). Cómo pero el router no puede hacer control de flujo, envía al servidor los 500 Mbps que le deja S1 y descarta el tráfico en exceso (la cola de salida del enlace se llena). Por lo tanto los 500 Mbps del router se reparten entre las estaciones de la VLAN4 y lo regula el TCP.
(iii) Volviendo atrás, las 20 estaciones de la VLAN4 se reparten equitativamente los 500 Mbps (500 / 20 = 25 Mbps). Los hubs de la VLAN1 se reparten los otros 500 Mbps (500 / 8 = 62.5 Mbps). Cada estación conectada a un hub tiene entonces 62.5 / 15 = 4.17 Mbps.

d)
En este caso:
(i) El cuello de botella es claramente la conexión a Internet de 20 Mbps
(ii) Si todas las estaciones son iguales, las perdidas en el buffer del router regulan las ventanas de congestión (TCP) de los hosts y esta capacidad se reparte equitativamente.
(iii) Cada estación tiene 20 Mbps / (15x8+15x8+15x8+10x5+10x5) = 43.48 kbps.

Problema 3.4.2.

a)
La VLAN1 se compone de dos partes, una conectada al SW2 y la otra al SW3.
A SW2 llegan 6 transmisiones de 80 Mbps cada una (es el 80% de 100 Mbps que pueden transmitir los Hubs). Por lo tanto de salida el SW2 transmite 80x6=480 Mbps hacia SW1.
A SW3 llegan 6 transmisiones de 80 Mbps cada una (es el 80% de 100 Mbps que pueden transmitir los Hubs). Por lo tanto de salida el SW3 transmite 80x6=480 Mbps hacia SW1.
Como el servidor está en la VLAN3 una vlan distinta de la de las estaciones, las tramas que llegan al SW1 de SW2 y SW3 deben pasar por el router R1. La eficiencia de SW1 es del 100%, es decir puede operar a 1000 Mbps, que es superior a la suma de lo que entra 480+480 = 960 Mbps y por lo tanto no hay cuello de botella en SW1. SW1 transmite estos 960 Mbps a R1 a través del enlace GigabitEthernet. R1 hace encaminamiento y devuelve estos 960 Mbps a SW1. Como este enlace es FullDuplex, puede operar a 1000 Mbps en ambos sentido así que tampoco en R1 hay cuello de botella. SW1 ahora retransmite los 960 Mbps al servidor S1. El enlace SW1-S1 es también de 1000 Mbps y por lo tanto tampoco hay cuello de botella.

(i) Los cuellos de botella son los hubs.
(ii) El CSMA/CD de las estaciones controla y reparte los 80 Mbps de cada hub.
(iii) Las 10 estaciones de cada hub se reparten equitativamente los 80 Mbps, por lo tanto 80/10 = 8 Mbps.

b)
Al caso anterior ahora hay que sumarle lo que transmiten las estaciones de la VLAN2.
Los APs operan a 128 Mbps pero tienen una eficiencia del 50%, es decir 64 Mbps. Estos 64 Mbps son los que los APs luego transmiten por el enlace FastEthernet (que soporta 100 Mbps) a los switch SW2 y SW3.
A SW2 llegan 5 transmisiones de 64 Mbps cada una. Por lo tanto el SW2 transmite de salida los 480 Mbps de los Hubs más los 64x5=320 Mbps de los APs, es decir un total de 480+320 = 800 Mbps hacia SW1.
A SW3 llegan 10 transmisiones de 64 Mbps cada una. Por lo tanto el SW3 transmite de salida los 480 Mbps de los Hubs más los 64x10=640 Mbps de los APs, es decir un total de 480+640 = 1120 Mbps hacia SW1. 1120 Mbps es superior a la capacidad de los enlaces, por lo tanto aquí habría un posible cuello de botella que reduce esta transmisión a 1000 Mbps.
SW1 recibe 800 Mbps de SW2 y 1000 Mbps de SW3. La suma da 1800 Mbps que es lo que debería transmitir luego a R1. Aquí tenemos el cuello de botella principal que reduce la salida de SW1 a R1 a 1000 Mbps. A partir de aquí hasta S1 ya no hay cuello de botella siendo todos los enlaces GigabitEthernet.

(i) El cuello de botella principal es el enlace de trunk entre SW1 y R1.
(ii) El SW1 hace control de flujo con tramas de pausa y reparte los 1000 Mbps entre SW2 y SW3. A su vez, SW2 y SW3 hacen control de flujo
(iii) Entre SW2 y SW1 habrá 500 Mbps que los hubs y APs se reparten equitativamente 500/11=45.5Mbps. Las 10 estaciones de cada hub tendrá 45.5/10 = 4.55 Mbps. Las estaciones de cada AP tendrá 45.5/10 = 4.55Mbps. Entre SW3 y SW1 habrá 500 Mbps que los hubs y APs se reparten equitativamente 500/16=31.25Mbps. Las 10 estaciones de cada hub tendrá 31.25/10 = 3.125 Mbps. Las estaciones de cada AP tendrá 31.25/5 = 6.25Mbps.

c)
Las 10 estaciones están en la misma VLAN que los servidores, no se pasa por el router R1. Cada estación transmite a su máximo que son 100 Mbps. Como los destinos son dos, cada estación establece dos conexiones TCP, una para cada servidor. Siendo las transmisiones iguales, TCP reparte estos 100 Mbps equitativamente entre S1 y S2, es decir cada estación transmite 50 Mbps a S1 y 50 Mbps a S2.
SW4 recibe 10 transmisiones a 100 Mbps (50 hacia S1 y 50 hacia S2) y transmite a SW1 10x100 = 1000 Mbps (500 hacia S1 y 500 hacia S2). SW1 recibe 1000 Mbps y retransmite 500 Mbps a S1 y otros 500 Mbps a S2.

(i) No hay cuello de botella.
(ii) No hay control de flujo porque no hay cuello de botella. El TCP de las estaciones hará que cada estación transmita la mitad del tiempo a S1 y la otra mitad a S2.
(iii) Todos los enlaces son FDX y las estaciones y servidores pertenecen a la misma VLAN. Las 10 estaciones transmiten a 100 Mbps (50 Mbps hacia cada servidor); SW4 transmite a SW1 a 1000 Mbps; los servidores recibirán a 500 Mbps cada uno.

d)
Como todos los enlaces son FDX y servidores y estaciones pertenecen a la misma VLAN, los dos sentidos de transmisión se pueden tratar de manera separada.
Para el sentido estaciones – servidores vale lo que ya determinado en el punto c).

Para el sentido servidores – estaciones, cada servidor transmite a su máxima capacidad que son 1000 Mbps. SW1 recibe dos entradas a 1000 Mbps y a la salida hacia SW4 se presentan 2000 Mbps que es superior a la capacidad del enlace SW1-SW4. Aquí hay un cuello de botella. SW1 solo puede transmitir 1000 Mbps y hace control de flujo hacia los servidores con tramas de pausa (enlace FullDuplex) reduciendo la transmisión de cada servidor a 500 Mbps.

(i) El cuello de botella es el enlace SW1-SW4.
(ii) SW1 hace control de flujo hacia los servidores enviando tramas de pausa para repartir los 1000 Mbps del enlace SW1-SW4 entre S1 y S2.
(iii) Cada servidor transmite a 500 Mbps. A la salida del SW1 habrá 1000 Mbps que luego se reparten entre las 10 estaciones que irán a 1000/10 = 100 Mbps.

e)
SW1 solo puede transmitir 1000 Mbps a R1. R1 pero solo puede transmitir 50 Mbps hacia Internet. Este es claramente el cuello de botella. R1 además no hace control de flujo y solo puede actuar en este caso el TCP de la siguiente manera. El buffer de salida de R1 hacia Internet irá llenándose siempre más porque lo que entra (1000 Mbps) es superior a lo que sale (50 Mbps). Cuando esté lleno, empezará a descartar datos. Como todas las estaciones son iguales, cada estación tendrá la misma probabilidad de perder datos. Cuando se pierden dato actúa el TCP que recupera la perdida y reduce la velocidad efectiva de transmisión reduciendo el valor de la ventana de congestión. Por lo tanto:

(i) El cuello de botella es la conexión a Internet de 50 Mbps
(ii) Si todas las estaciones son iguales, las perdidas en el buffer del router R1 regulan las ventanas de congestión de los hosts (es decir actúa TCP) y los 50 Mbps se reparten equitativamente entre las estaciones.
(iii) Cada estación irán a 50 Mbps / (6x10+5x10+6x10+10x5) = 227.3 kbps.

Anexos.

A.1. -Acrónimos

AP	Access Point
awnd	Advertised window (ventana anunciada)
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
cwnd	Congestion window (ventana de congestión)
GBN	Go back N
IP	Internet Protocol
LAN	Local Area Network
RTO	Retransmission Time-Out
RTS/CTS	Request To Send/Clear To Send
RTT	Round Trip Time
S&W	Stop & Wait
sack	Selective ack
SR	Selective Retransmission (retransmisión selectiva)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
wnd	Window (ventana de transmisión)