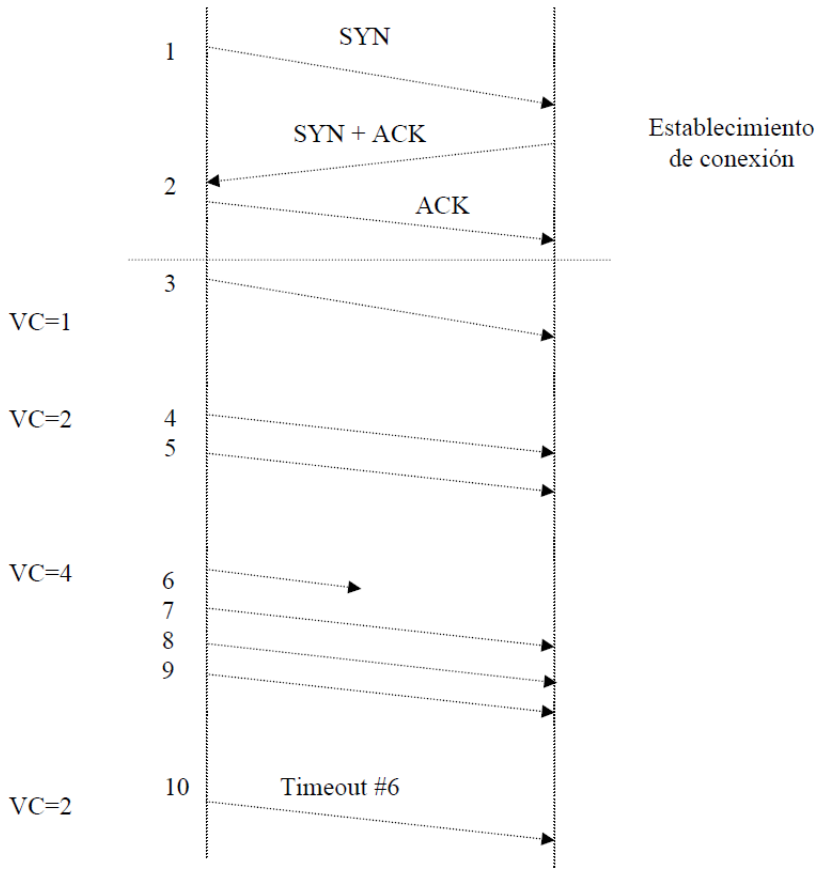
Redes II – UNLP
Examen Final 01/09/2012 – Solución

Este examen tiene 8 preguntas con un total de 100 puntos

1. [15 puntos] En la comunicación entre dos computadores mediante una red Ethernet se utiliza el protocolo TCP. Si el tamaño de ventana que cada uno de ellos anuncia es de 16383 bytes y suponiendo un flujo constante de datos en ambos sentidos y que se pierde el sexto paquete enviado por el computador que inicia la conexión ¿Cuál será el tamaño de la ventana de congestión del computador que inició la conexión, tras enviar el décimo paquete? Considere MSS = 1460 bytes y que se aplica control de congestión tipo Reno.

Solución: Sabiendo que el tamaño máximo de segmento se ajusta al MTU de Ethernet (MSS = 1460 bytes sin cabeceras), podemos calcular el umbral, en número de segmentos, en el que se deja de aplicar Slow Start y se empieza a aplicarse congestion avoidance. En concreto este umbral en bytes es de 16383/2, lo que implica 5,6 segmentos. Por tanto, desde un tamaño de ventana de congestión de 1 segmento, hasta un tamaño de 5 segmentos se aplica Slow Start. A partir de un tamaño de 6 segmentos hasta que la ventana está completamente abierta se aplica congestion avoidance. A continuación se muestra el intercambio de segmentos junto con la evolución de la ventana de congestión.



VC: Ventana de congestión
Los ACKs no están indicados ya que el otro extremo está enviando segmentos de datos y puede que los ACK vayan implícitos.

2. [10 puntos] El control de flujo TCP, basado en ventana deslizante, dispone de una indicación de ventana (buffer disponible en el otro extremo) que limita la inyección de segmentos en la conexión. El tamaño máximo que se puede indicar es de 64 KB. Esta limitación, ¿ podría afectar a las prestaciones del TCP cuando se utilizan redes de alta velocidad (Ej.: Gigabit Ethernet 1Gbps) con RTTs del orden de 2 ms. ?

Solución: El protocolo de ventana deslizante permite alcanzar altas índices de utilización, siempre y cuando ajustemos bien los tamaños de ventana. La utilización máxima sería aquella en la que podemos enviar segmentos sin reconocimiento hasta que nos llegue el reconocimiento del primero. En ausencia de errores, estaríamos ocupando el canal continuamente ;-). Si tenemos una red de capacidad 1 Gbps y el RTT es de 2 ms., antes de que nos pueda llegar un reconocimiento habríamos enviado 250 KB !!. Si tuviésemos una ventana de ese tamaño, alcanzaríamos la utilización máxima. Por tanto, esta limitación del TCP afecta directamente a las prestaciones en redes de alta velocidad.

3. [10 puntos] ¿Qué sucedería si por error recibiera UDP un datagrama UDP destinado a otra máquina (con otra dirección IP)?

Solución: La cabecera UDP contiene un campo de checksum OPCIONAL, que utiliza para su cálculo, entre otras cosas, la dirección IP destino lo que permite comprobar si el datagrama UDP ha llegado a la dirección correcta. Por lo tanto, en nuestro caso existirían dos situaciones posibles:

- Checksum en cero: Significaría que no se ha calculado y, por lo tanto, el proceso UDP intentaría entregar los datos a través del puerto especificado en el datagrama UDP.
- Checksum distinto de cero: Al comprobarlo se detectaría el error y se descartaría el datagrama

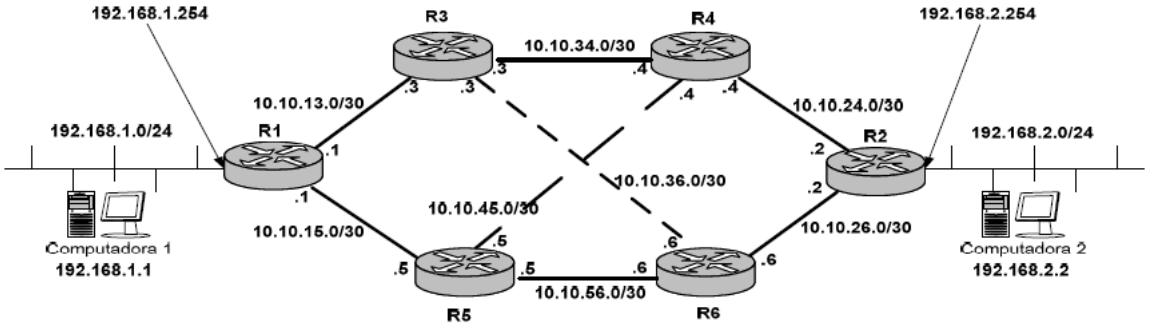
4. [15 puntos] Sea R un router BGP del sistema autónomo AS1 que recibe la siguiente información de otro router BGP con el que tiene abierta una conexión:

Redes alcanzables	Vector de Ruta
212.128.0/22	AS3, AS1
193.147.168/22	AS3, AS4, AS2, AS5, AS6, AS7

Indique la accíón tomada por el router R al recibir esas rutas.

Solución: Descarta la primera por estar en la lista.

5. [15 puntos] En la red de la figura asuma que se utiliza RIPv2 como protocolo de ruteo.



Escriba la tabla de ruteo del router R6.

Solución:

6. [10 puntos] La principal diferencia de BGP respecto del resto de protocolos de routing es que:

   A. BGP no puede funcionar en entornos "classless" (CIDR)

   B. Emplea una mética más sofisticada que la mayoría de los protocolos de routing

   C. Permite establecer restricciones para impedir el tráfico de tránsito

   D. Con BGP no está permitido crear topologías malladas

Solución: C

7. [15 puntos] El host H1 se encuentra en una red en la que se filtran los paquetes que entran y sólo se permiten paquetes de conexiones Web. El propietario de H1 quiere utilizar un programa peer-to-peer que utiliza normalmente el puerto TCP 6881 (aunque puede configurarse otro) pero no le funciona porque se eliminan los paquetes al no ser de conexiones web.

   ¿Cómo puede lograr que funcione el programa a pesar del filtro? ¿Puede conseguirlo si en H1 tiene activado el servidor Web? ¿Cómo cambia esto si el programa peer-to-peer utiliza UDP?

Solución: Puede configurar el programa peer-to-peer para usar el puerto 80 y así es indistinguible del trafico web.

Si hay un servidor web, el puerto 80 estará ocupado y no podrá usarlo el programa P2P.

Si el programa usa UDP, puede utilizar el puerto 80 a la vez que el servidor web, pero entonces tampoco funcionará porque los paquetes UDP del puerto 80 no son conexiones web.

8. [10 puntos] Para implementar una VPN, bastará con:

   A. Una red de conmutación de paquetes

   B. Solicitar una dirección IP fija para el servidor de túnel VPN

   C. Instalar algún dispositivo /software que cumpla las funciones de iniciador de túnel antes de que los paquetes de datos ingresen en Internet.

   D. Implementar algún sistema de autenticación de usuario antes de que este inicie una cesión en la VPN.

   E. Son necesarias todas y cada una de las opciones anteriores trabajando en conjunto.

Solución: E

Redes II
Examen Final– 3/8/2013
Solución

Este examen tiene 8 preguntas con un total de 100 puntos

1. [15 puntos] Determine el tamaño óptimo de ventana para una sesión TCP en la que el RTT = 100mseg, MSS = 600 bytes y velocidad de la interfaz 128 Kbps.

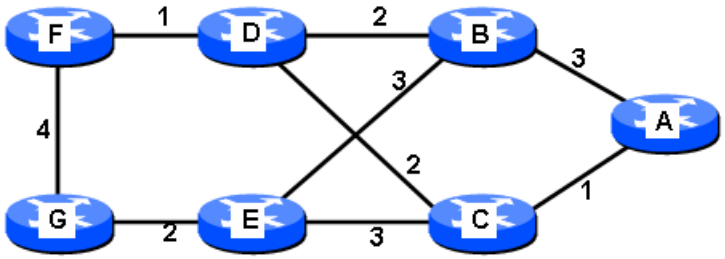
Solución:

$$W = RTT \times Rate = 1600\, bytes$$

2. [10 puntos] Puntualice las diferencias entre una consulta iterativa y una recursiva por parte del serviçio DNS

Solución: Una consulta iterativa se caracteriza por el hecho de que para poder obtener el resultado final, se necesita realizar varias consultas intermedias. En el peor de los casos es cuando tengo que recorrer todo el árbol hasta llegar al servidor de nombres autoritativos del dominio deseado.
Una consulta recursiva es aquella consulta en la cual el servidor de nombre sale a consultar y obtener el resultado por nosotros. Debemos aclarar la diferencia entre consulta recursiva y un servidor que acepte consultas recursivas. Un servidor acepta consultas recursivas, si en el caso de que hagamos la consulta recursiva, sale a obtener los resultados intermedios y nos responde el resultado final directamente.

3. [10 puntos] Se desea utilizar OSPF en la red siguiente:



Indique el árbol correspondiente al nodo D.

Solución:
D-F(1)
D-B(2)
D-C(2)
D-F-G(5)
D-B-E(5)
D-C-A(3)

4. [15 puntos] Resolver teniendo en cuenta el esquema de red indicado en hoja aparte.

   (a) Dada la siguiente tabla de ruteo, realizar el menor número de modificaciones (cambiar, agregar, eliminar rutas) de manera tal que todas las redes se puedan comunicar. (Suponer que la tabla de los otros routers están completas, es decir, conocen como llegar a todas las redes)

Tabla de router F

Destino	Máscara	Próximo salto	Interfaz salida
192.168.32.0	/24	–	Eth0
192.168.64.0	/24	–	Eth1
192.168.128.0	/24	–	Eth2
192.168.28.0	/23	192.168.128.1	Eth2
192.168.24.0	/21	192.168.64.1	Eth1
192.168.16.0	/20	192.168.32.1	Eth0

Solución: El único problema es que la red 192.168.30.0/28 matchea en 192.168.24.0/21 y sale por Eth1. Habría que agregar una entrada más en la tabla de ruteo:

Tabla de router F

Destino	Máscara	Próximo salto	Interfaz salida
192.168.30.0	/24	192.168.32.1	Eth0

   (b) Escribir la tabla del router B con la menor cantidad de entradas posibles y que permita alcanzar a todas las redes. (Suponer que la tabla de los otros routers están completas, es decir, conocen como llegar a todas las redes).

Solución:

Tabla de router F

Destino	Máscara	Próximo salto	Interfaz salida
192.168.16.0	/24	–	Eth0
192.168.32.0	/24	–	Eth1
192.168.30.0	/24	192.168.16.1	Eth0
0.0.0.0	–	192.168.32.2	Eth1

5. [15 puntos] A continuación se incluye el volcado de la información de un analizador de protocolos para varios segmentos TCP (sólo se incluye la información relevante para este ejercicio):

```
Frame 1 (74 on wire, 74 captured)
Internet Protocol, Src Addr: 212.128.1.44, Dst Addr: 212.128.1.45
Transmission Control Protocol:
 Source port: 1072
 Destination port: 80
 Sequence number: 3852871073
 Flags: 0x0002 (SYN)
Frame 2 (60 on wire, 60 captured)
Internet Protocol, Src Addr: 212.128.1.45, Dst Addr: 212.128.1.44
```

```
Transmission Control Protocol:
 Source port: 80
 Destination port: 1072
 Sequence number: 3809911689
 Acknowledgement number: 3852871075
 Flags: 0x0012 (SYN, ACK)
Frame 3 (54 on wire, 54 captured)
Internet Protocol, Src Addr: 212.128.1.44, Dst Addr: 212.128.1.45
Transmission Control Protocol:
 Source port: 1072
 Destination port: 80
 Sequence number: 3852871074
 Acknowledgement number: 3809911690
 Flags: 0x0010 (ACK)
Frame 4 (357 on wire, 357 captured)
Internet Protocol, Src Addr: 212.128.1.44, Dst Addr: 212.128.1.45
Transmission Control Protocol:
Source port: 1072
 Destination port: 80
 Sequence number: 3852871074
 Acknowledgement number: 3809911690
 Flags: 0x0018 (PSH, ACK)
 Hypertext Transfer Protocol
 GET /~jgb/test.html HTTP/1.0\r\n
 User-Agent: Mozilla/4.07 [en] (X11; I; Linux 2.2.15 i586; Nav)\r\n
 Host: gsyc.escet.urjc.es\r\n
 \r\n
```

Estos segmentos corresponden al principio de la traza de una interacción HTTP entre un navegador y un servidor web. Responda a las siguientes preguntas:

(a) Uno de los números de secuencia (Sequence number) o de asentimiento (Acknowledgement number) está mal (no corresponde con lo que debe ocurrir en una implementación válida de TCP). ¿Cuál es? ¿Qué valor debería tener? ¿Por qué?

(b) Los tres primeros segmentos de la traza no tienen datos. ¿Por qué? ¿Para qué sirven esos segmentos?

(c) ¿Qué segmentos envía el navegador? ¿Qué segmentos envía el servidor web? ¿Por qué puede determinarlo?

(d) ¿Por qué no está activado el flag ACK del segmento 1?

Solución:

(a) El número de asentimiento del segmento 2 (Frame 2) debería ser 3852871074, que es el siguiente al número de secuencia del segmento 1 (esto es, el número del primer byte que se espera recibir).

(b) Son los tres segmentos de establecimiento de conexión.

(c) El navegador envía los segmentos 1, 3 y 4. El servidor el segmento 2. Hay varias formas de saberlo.
La primera, que la conexión la abrirá el navegador cuando el usuario decide descargar la página correspondiente, y por lo tanto el primer paquete lo enviará el navegador. Siendo la dirección origen IP de éste la 212.128.1.44, está claro que las tramas 3 y 4 tienen la misma dirección origen. La trama 2, sin embargo, está enviada por 212.128.1.45, que es la dirección destino del primer segmento, y por tanto, el servidor.
Otra forma de saberlo es fijarse en el segmento 4, donde comienza la interacción HTTP. Los datos de ese segmento TCP son claramente una petición HTTP, y por tanto ha de emitirlo el navegador. Fijándose en las direcciones origen y destino de ese paquete pueden hacerse las mismas deducciones que se comentan en el párrafo anterior.

(d) Porque es el primer segmento, en el que se está empezando a establecer la conexión, y sólo el que la inicia está proponiendo un número de secuencia. La otra parte aún no ha propuesto uno, y por tanto no hay nada que asentir, y ni se sabe aún con qué número se debería asentir. Por lo tanto no hay que tener en cuenta el contenido del campo ?Número de Asentimiento? y por ello no se activa el flag ACK.

6. [10 puntos] La principal diferencia de BGP respecto del resto de protocolos de routing es que:

   A. BGP no puede funcionar en entornos 'classless'(CIDR)
   B. Emplea una mética más sofisticada que la mayoría de los protocolos de routing
   C. Permite establecer restricciones para impedir el tráfico de tránsito
   D. Con BGP no está permitido crear topologías malladas

Solución: C

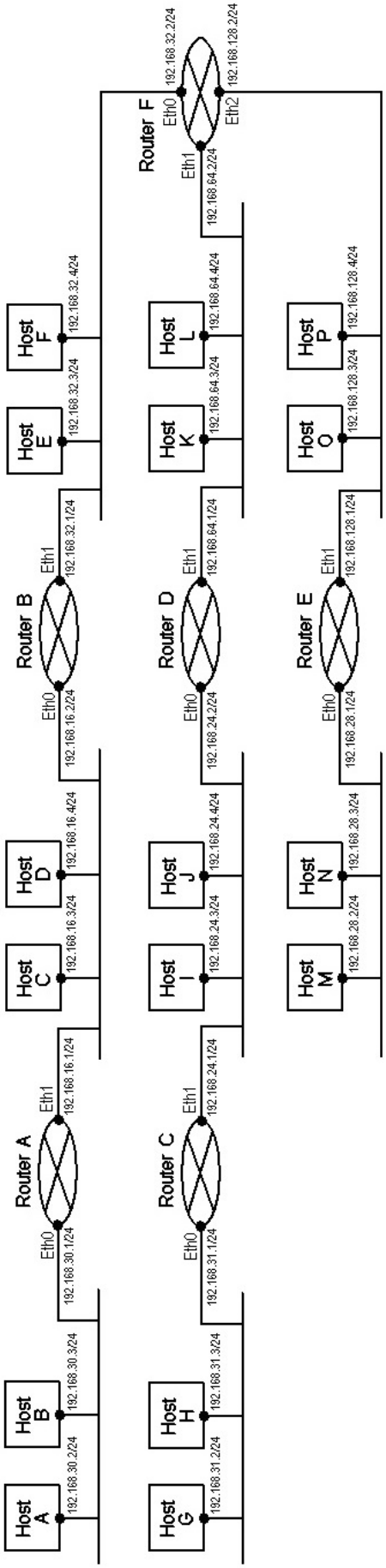
7. [10 puntos] Para enviar un archivo binario por correo electrónico hay que usar la siguiente codificación:

   A. MIME Base 32
   B. MIME Base 64
   C. MIME Quoted-Printable
   D. MIME text/bin

Solución: B

8. [15 puntos] Proponga un sistema seguro y eficiente para distribuir claves que se emplearán para encriptar mensajes con un algoritmo simétrico. Las mismas se deben transmitir con la firma correspondiente.

Solución: Enviarlas como un mensaje más en un sistema tipo RSA con firma digital. Para detalles remitirse a la bibliografía


Router A
Eth0
192.168.30.1/24
Eth1
192.168.16.1/24
Router B
Eth0
192.168.16.2/24
Eth1
192.168.32.1/24
Router C
Eth0
192.168.31.1/24
Eth1
192.168.24.1/24
Router D
Eth0
192.168.24.2/24
Eth1
192.168.64.1/24
Router E
Eth0
192.168.28.1/24
Eth1
192.168.128.1/24
Router F
Eth0
192.168.32.2/24
Eth1
192.168.64.2/24
Eth2
192.168.128.2/24
Host A
192.168.30.2/24
Host B
192.168.30.3/24
Host C
192.168.16.3/24
Host D
192.168.16.4/24
Host E
192.168.32.3/24
Host F
192.168.32.4/24
Host G
192.168.31.2/24
Host H
192.168.31.3/24
Host I
192.168.24.3/24
Host J
192.168.24.4/24
Host K
192.168.64.3/24
Host L
192.168.64.4/24
Host M
192.168.28.2/24
Host N
192.168.28.3/24
Host O
192.168.128.3/24
Host P
192.168.128.4/24

Ejercicio 4

Redes II – UNLP
Examen Final 09/08/2014 – Solución

Este examen tiene 8 preguntas con un total de 100 puntos

1. [15 puntos] El buffer de recepción del extremo B de una conexión TCP establecida entre los procesos A y B tiene capacidad para almacenar un máximo de 4000 bytes de datos. El primer segmento que envió el proceso A a B tenía el número de secuencia 2300. En el instante t1 B recibe un nuevo segmento que contiene 300 bytes de datos, y cuyo número de secuencia es el 3501. Tras recibir este segmento, B compone un segmento con el número de ack 3401. Suponiendo que la aplicación en B ha consumido los 200 primeros bytes de datos que le envía A, ¿Qué valor incluirá B en el campo de ventana de dicho segmento?

   A. 2700

   B. 2500

   C. 4000

   D. 3100

   Solución: D

2. [15 puntos] En una PC C se ha recibido un segmento TCP que le envía otro host A destinado al puerto 80 de C y con origen en el puerto 4000 de A. Este segmento lleva el flag SYN activado y el número de secuencia 7777. Especifique los campos relevantes del segmento TCP que C le enviará a A conisderando que aceptó la conexión. Identifique el servicio solicitado y los roles cumplidos por A y C.

3. [10 puntos] Al encapsularse los mensajes de RIP en datagramas UDP:

   A. RIP no sufre de problemas de la fragmentación de datagramas IP

   B. RIP no sufre los problemas de descartado de paquetes por congestión en routers.

   C. Los mensajes de RIP se desencapsulan por número de puerto del datagrama UDP

   D. Los mensajes de RIP se desencapsulan por número de protocolo en el datagrama IP

   Solución: C

4. [10 puntos] Sea R un router BGP del sistema autónomo AS1 que recibe la siguiente información de otro router BGP con el que tiene abierta una conexión:

Redes alcanzables	Vector de Ruta
212.128.0/22	AS3, AS1
193.147.168/22	AS3, AS4, AS2, AS5, AS6, AS7

   Indique la accíón tomada por el router R al recibir esas rutas.

Solución: Descarta la primera por estar en la lista.

5. [15 puntos] Se realizó la captura de las siguientes tramas Ethernet:(tenga en cuenta que se extrajeron los bytes de preámbulo.

Trama 1:

```
00 18 39 97 4c 44 00 19 66 0b 45 b4 08 00 45 00
00 3d cc ba 00 00 80 11 3c 7f c0 a8 b3 6a 57 45
66 1e 31 f2 06 18 00 29 98 4c 10 9f a6 d6 46 e5
93 89 00 0c 63 dc 00 00 00 00 00 02 00 00 00 00
00 00 08 00 00 00 00 00 00 00 00
```

Trama 2:

```
00 18 39 97 4c 44 00 19 66 0b 45 b4 08 00 45 00
00 3d cc bb 00 00 80 11 a3 c4 c0 a8 b3 6a bd ab
98 71 31 f2 93 3e 00 29 71 fe 10 9f a6 d6 46 e5
93 89 00 0c 64 4a 00 00 00 00 00 02 00 00 00 00
00 00 08 00 00 00 00 00 00 00 00
```

Trama 3:

```
00 19 66 0b 45 b4 00 18 39 97 4c 44 08 00 45 00
00 28 98 e3 40 00 68 06 b6 5c 96 8c b8 f0 c0 a8
b3 6a 1e 52 0c c4 7f e8 71 29 3b e1 50 45 50 10
ff ff 43 f6 00 00 27 d0 00 00 00 00
```

Trama 4:

```
00 19 66 0b 45 b4 00 18 39 97 4c 44 08 00 45 00
00 28 e8 a7 00 00 70 06 11 c1 51 ae 8a a6 c0 a8
b3 6a e1 1a 0f 67 00 00 00 00 ea 76 ef 17 50 14
00 00 95 58 00 00 85 08 00 00 00 00
```

Se pide: Analizar los campos relevantes de la información de nivel de transporte que contienen.

Solución:

1.

```
User Datagram Protocol
Source port: 12786 (12786)
Destination port: 1560 (1560)
Length: 41
```

2.

```
User Datagram Protocol
Source port: 12786 (12786)
Destination port: 37694 (37694)
Length: 41
```

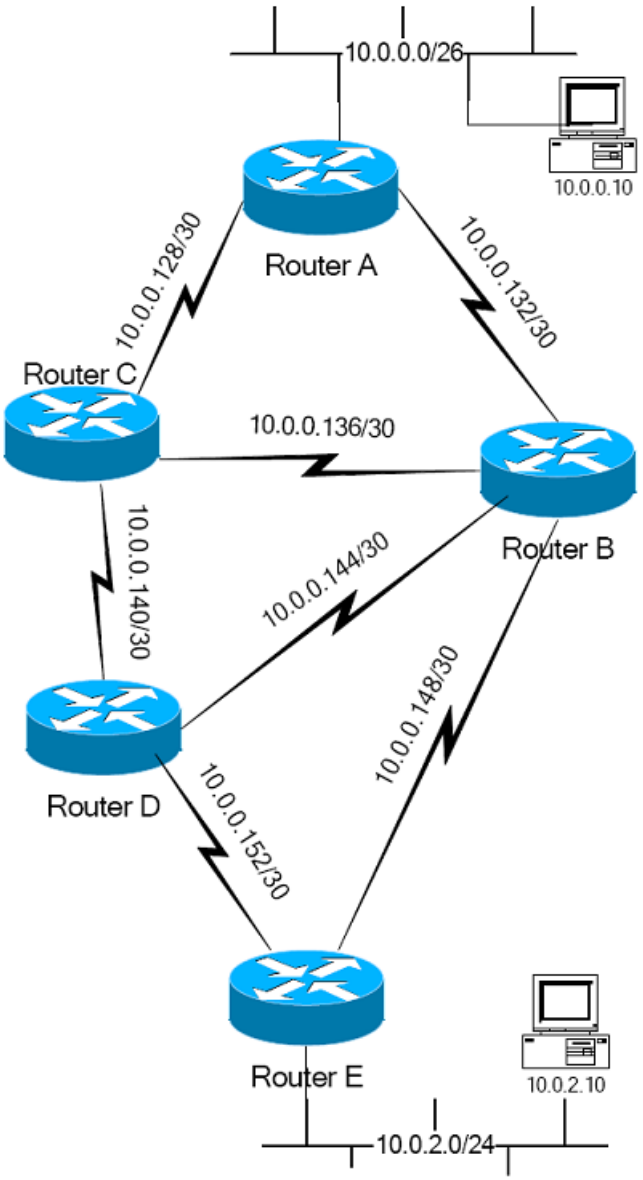
3.

```
Transmission Control Protocol
Source port: 7762 (7762)
Destination port: 3268 (3268)
Sequence number: 7f e8 71 29
Acknowledgement number: 3b e1 50 45
Header length: 20 bytes
Flags: 0x10 (ACK)
Window size: 65535
Checksum: 0x43f6
```

4.

```
Transmission Control Protocol
Source port: 57626 (57626)
Destination port: 3943 (3943)
Sequence number: 0
Acknowledgement number:ea 76 ef 17
Header length: 20 bytes
Flags: 0x14 (RST, ACK)
Window size: 0
Checksum: 0x9558
```

6. [10 puntos] La red de la figura constituye un dominio de ruteo OSPF.



Determine las rutas encontradas por el Router D según el algoritmo empleado por OSPF así como la tabla de ruteo resultante. En caso de faltar direcciones IP asígnelas.

7. [10 puntos] Para realizar la transferencia de archivos con el servicio FTP:
   A. Se utiliza el mismo port en el cliente y en el servidor
   B. Se utilizan dos sesiones, una de control bidireccional y otra de datos unidireccional
   C. Se establece sólo una sesión de datos dado que el control está provisto por TCP
   D. El cliente establece primero una sesión con el servidor.

Solución: D

8. [15 puntos] Proponga un sistema seguro y eficiente para distribuir claves que se emplearán para encriptar mensajes con un sistema asimétrico tipo RSA. Las mismas se deben transmitir con la firma correspondiente.

Solución: Enviarlas como un mensaje más en un sistema tipo RSA con firma digital. Para detalles remitirse a la bibliografía

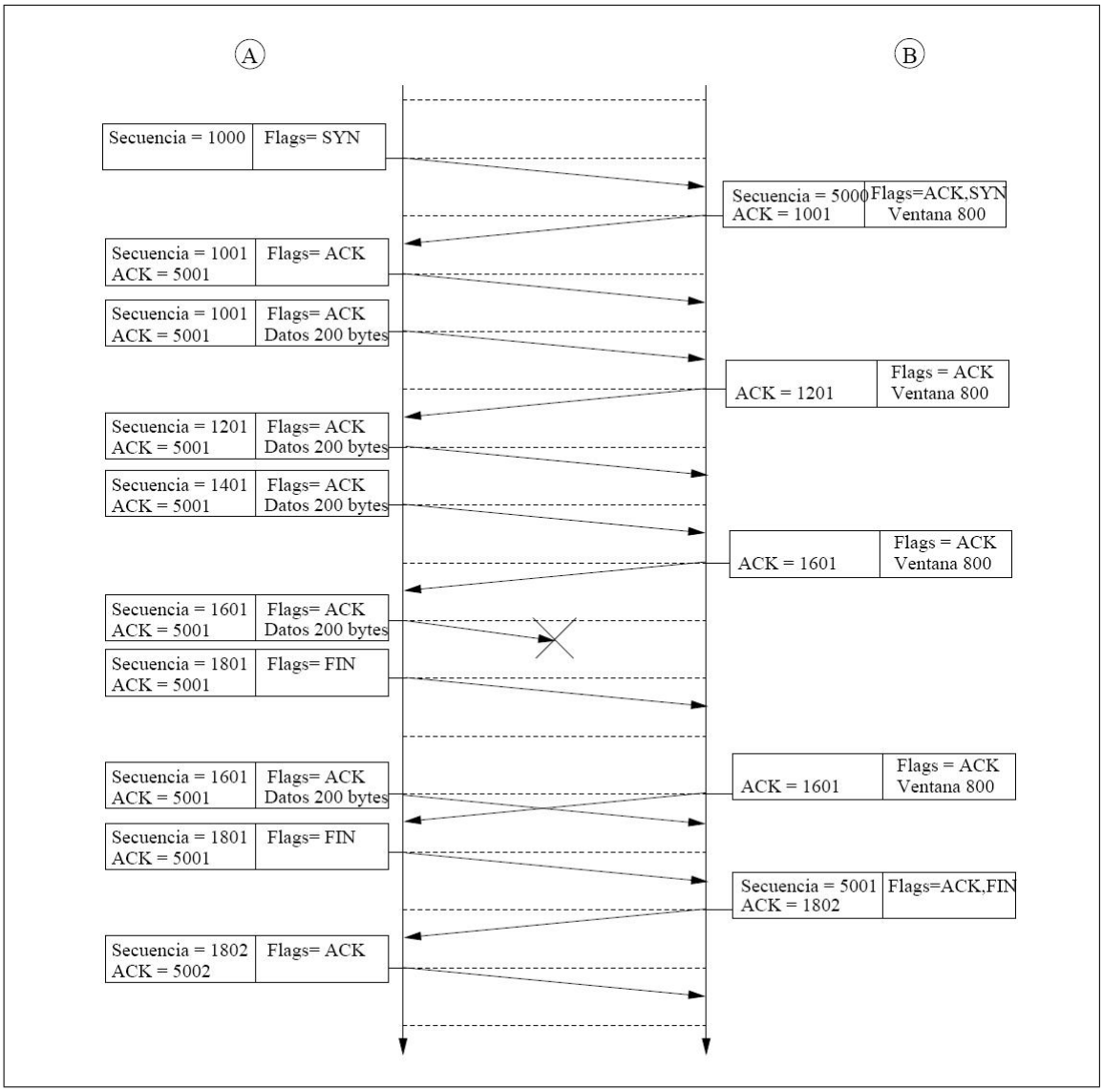
Redes II – UNLP
Examen Final 12/07/2014 – Solución

Este examen tiene 8 preguntas con un total de 100 puntos

1. [15 puntos] Complete la secuencia de envío de segmentos TCP reflejada en la figura, incluyendo el cierre de la conexión, en la que las líneas horizontales representan tics de reloj, sabiendo que:

   - No se perderá ningún segmento en la transmisión excepto el cuarto con datos enviado por A.
   - Los segmentos no dibujados (excepto el anteriormente citado) tardarán en llegar al destino medio tic de reloj, y no se perderán.
   - A está utilizando arranque lento (Slow Start) para prevenir la congestión.
   - A tiene que enviar a B 800 bytes de datos, una vez enviados procederá a cerrar la conexión.
   - B no desea enviar datos a A.
   - B enviará asentimientos a A cuando haya recibido dos segmentos de A desde el último segmento asentido o cuando hayan sucedido 2 tics de reloj desde desde el último segmento recibido.
   - El plazo de retransmisión de segmentos en A (timeout) es de 3 tics de reloj.
   - A usa un tamaño fijo de datos de 200 bytes.
   - B siempre enviará un valor de 800 en el campo de tamaño de la ventana de recepción.
   - Tanto A como B sólo transmiten segmentos coincidiendo con el tic de reloj.
   - A enviará segmentos con datos siempre que pueda.

Solución:



2. [10 puntos] Determine el tamaño óptimo de ventana para una sesión TCP en la que el RTT = 100mseg, MSS = 600 bytes y velocidad de la interfaz 128 Kbps.

Solución:

$$W = RTT \times Rate = 1600\,bytes$$

3. [10 puntos] ¿Cuáles dos de las siguientes afirmaciones son correctas respecto de protocolos de ruteo basados en distancia vectorial y link-state?

   A. Link state envía la tabla de ruteo completa por todas sus interfaces en intervalos regulares de tiempo.

   B. Distancia vectorial envía la tabla de ruteo completa por todas sus interfaces en intervalos regulares de tiempo.

C. Link state envía actualizaciones que contienen el estado de sus enlaces.

D. Distancia vectorial envía actualizaciones por sus interfaces que propaga por inundación.

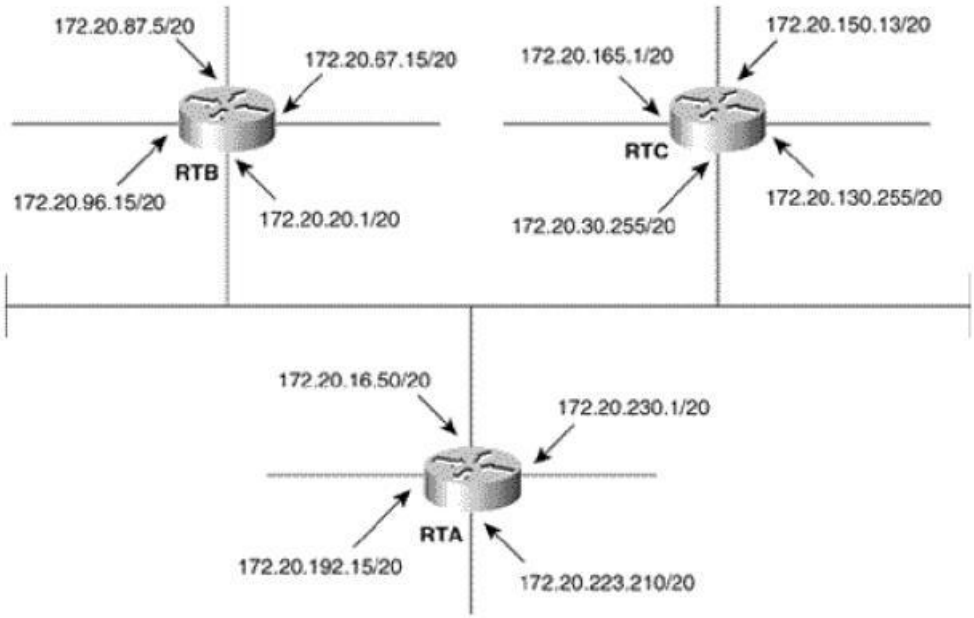
Solución: B y C

4. [15 puntos] En una red como la indicada en la figura los usuarios reportaron errores de conectividad. Indique cuáles son y como solucionarlos. Las tablas de Ruteo correspondientes son:

RTA ip route 172.20.96.0 255.255.240.0 172.20.20.1
ip route 172.20.82.0 255.255.240.0 172.20.20.1
ip route 172.20.64.0 255.255.240.0 172.20.20.1
ip route 172.20.160.0 255.255.240.0 172.20.30.255
ip route 172.20.144.0 255.255.240.0 172.20.30.255
ip route 172.20.128.0 255.255.240.0 172.20.30.255

RTB ip route 172.20.192.0 255.255.240.0 172.20.16.50
ip route 172.20.224.0 255.255.240.0 172.20.16.50
ip route 172.20.128.0 255.255.240.0 172.20.16.50
ip route 172.20.160.0 255.255.240.0 172.20.30.255
ip route 172.20.144.0 255.255.240.0 172.20.30.255
ip route 172.20.128.0 255.255.240.0 172.20.30.255

RTC ip route 172.20.192.0 255.255.240.0 172.20.16.50
ip route 172.20.208.0 255.255.255.0 172.20.16.50
ip route 172.20.224.0 255.255.240.0 172.20.16.50
ip route 172.20.96.0 255.255.240.0 172.20.20.1
ip route 172.20.82.0 255.255.240.0 172.20.20.1
ip route 172.20.64.0 255.255.240.0 172.20.20.1

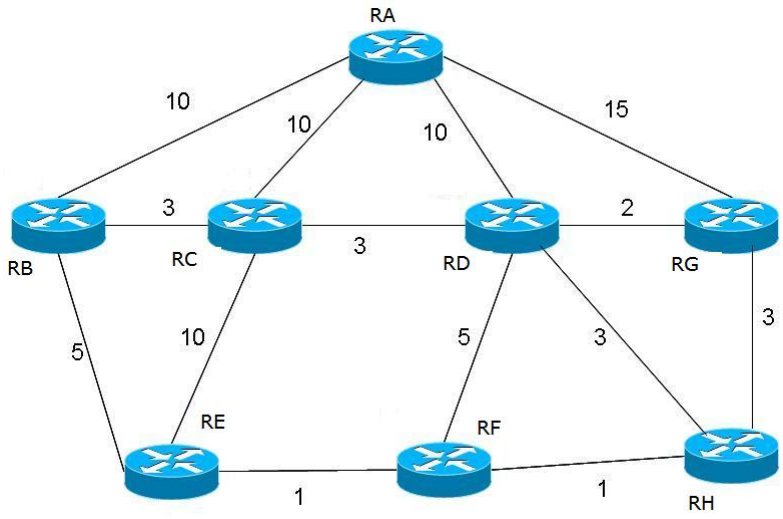


Solución: En RTA segunda fila la red destino debe ser 172.20.80.0

En RTB tercera fila la red destino debe ser 172.20.208.0

En RTC segunda fila la máscara debe ser 255.255.240.0

5. [15 puntos] Encuentre la tabla reducida del router RE considerando que en el sistema se utiliza un protocolo de ruteo basado en algoritmo "link-state".



Solución: Las rutas son:
RE-RF(1)
RE-RF-RH(2)
RE-RB(5)
RE-RF-RH-RD(5)
RE-RF-RH-RG(5)
RE-RB-RC(8)
RE-RB-RA(15)

6. [10 puntos] ¿Por qué motivo DNS puede encapsularse en TCP?

Solución: Si ocurre fragmentación no hay forma de garantizar el mensaje completo.

7. [10 puntos] Elija las aseveraciones que considere correctas respecto de BGP.
   A. Utiliza una arquitectura de link-state.
   B. Utiliza TCP como protocolo de transporte.
   C. Se encapsula en IP
   D. Los mensajes se propagan por inundación.

Solución: B

8. [15 puntos] FTP utiliza dos sesiones sobre un mismo port bien conocido en el servidor.
   A. Verdadero
   B. Falso

Solución: B

Redes – UNLP
Examen Final 11/07/2015 – Solución

Este examen tiene 8 preguntas con un total de 100 puntos

1. [10 puntos] En una conexión normal TCP, invocada por un servicio según paradigma cliente servidor, todos los segmentos tienen el flag ACK activado, excepto:

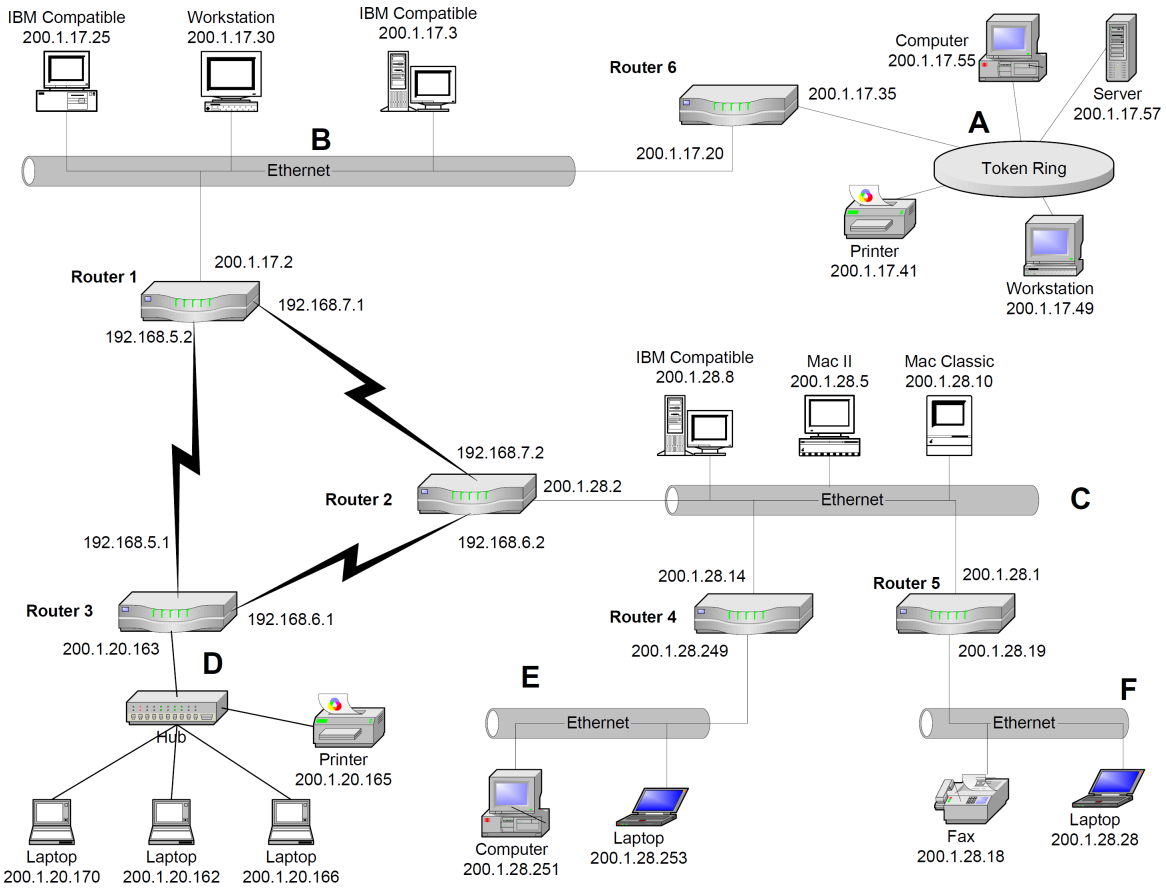
   A. el primer segmento enviado por el servidor

   B. el último segmento enviado por el cliente

   C. el primer segmento enviado por el cliente

Solución: C

2. [15 puntos] En relación al diagrama de red de la figura, en la que se adoptó RIPv2 como protocolo de ruteo:



(a) Indique la tabla de ruteo completa de los "routers", Router 3 y 6

(b) ¿Qué rutas propagará Router 2 por las interfaces, 192.168.7.2 y 192.168.6.2, sabiendo que se habilitó "poisoned reverse".

Solución: Identificamos las redes en primer lugar:

A: 200.1.17.32/27

B: 2001.17.0/27

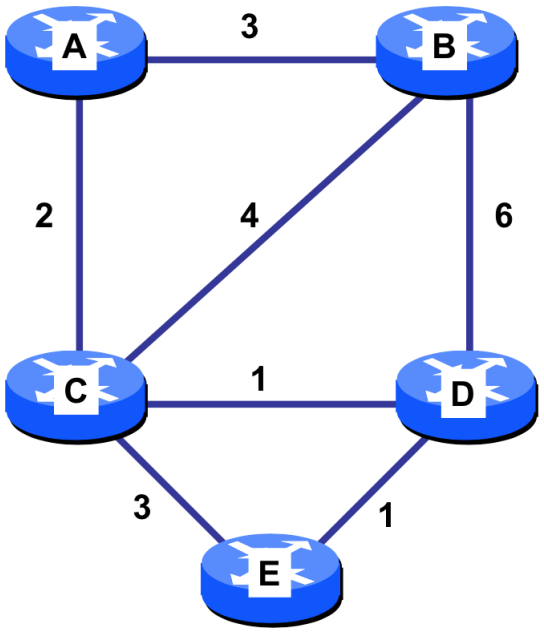
C: 200.1.28.0/28

D: 200.1.20.160/28

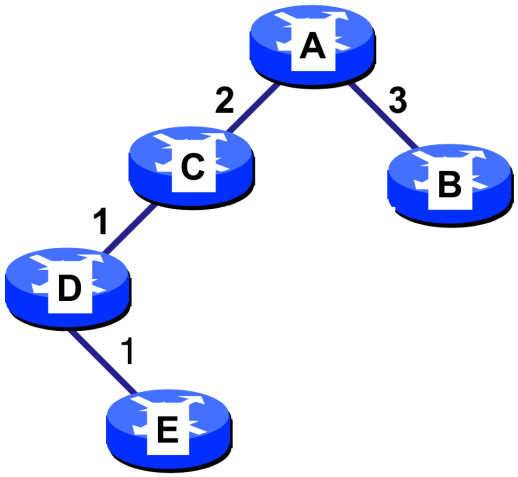
E: 200.1.28.248/29

F: 200.1.28.16/28

3. [15 puntos] Suponga que en una red como la de la figura siguiente:



en la que los números indican los valores de la métrica para cada enlace, se está utilizando OSPF. Desarrolle el árbol de rutas óptimas desde A hacia el resto de routers. Suponga que las métricas son aditivas, es decir que la métrica de una ruta es la suma de las métricas de los enlaces por los que pasa.



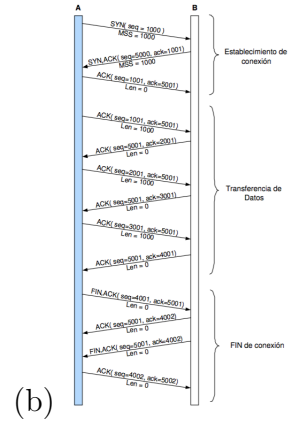
Solución:

4. [10 puntos] (a) ¿Cómo se elige el numero de secuencia inicial de una conexión TCP? Indique las razones para esta elección.

   (b) Realice un diagrama de una conexión TCP hipotética entre A y B donde A envía a B tres segmentos con 1000 bytes de datos cada uno y luego cierra la conexión. Indique los números de secuencia de los segmentos intercambiados y las banderas (flags) relevantes en los paquetes de establecimiento y fin de conexión. Suponga que los números de secuencia iniciales elegidos por A y B son 1000 y 5000 respectivamente.

Solución:

(a) El problema en la utilización de los números de secuencia es evitar la reutilización de los mismos durante el tiempo de vigencia. Con tiempo de vigencia nos referimos a un tiempo T, múltiplo del tiempo de vida que puede tener un segmento TCP y su reconocimiento. De no respetarse se pueden llegar a confundir segmentos o reconocimientos de una conexión anterior que podrían ser erróneamente considerados como pertenecientes a la conexión actual. Como primera aproximación se elige el número de secuencia como los 32 bits menos significativos de un reloj interno del host, este reloj tiene que continuar su funcionamiento de forma independiente. De esta manera no estaría duplicando números de secuencia iniciales.



(b)

5. [15 puntos] Un cliente FTP se conecta a un servidor FTP, realizando la autentificación del usuario. A partir de ese momento ejecuta los siguientes comandos FTP en la máquina local:

```
cd pruebas
dir
get *.jpeg
```

El contenido del directorio pruebas son los ficheros: pepe.gif, listado.jpeg, enero.doc, informe.jpeg. Indique el número de conexiones de control y de datos que intervienen en todo el proceso.

Solución: 1 conexión de control y 3 conexiones de datos.

6. [15 puntos] Sean 5 máquinas A, B, C, D y E conectadas a Internet. Excepto la máquina E, todas las demás pertenecen a la compañía de los hermanos Cenizo, especializada en la detección de plagas en Internet.
El nombre de dominio DNS de esta compañía se llama plagas.com. Los nombres de dominio de las máquinas A, B, C y D son, respectivamente: A.plagas.com, B.plagas.com, C.plagas.com, D.plagas.com. Algunas máquinas alojan servidores de DNS:
La máquina A aloja un servidor de DNS que es secundario para el dominio .com
La máquina C aloja un servidor de DNS que es primario para el dominio plagas.com
La máquina D aloja un servidor de DNS que es secundario para el dominio plagas.com
La máquina E envía un mensaje de consulta de DNS al servidor DNS de la máquina A, preguntando por el nombre B.plagas.com. En función de la razón por la que E pueda haber enviado el mensaje de consulta a A, ¿Qué hará a continuación el servidor de DNS de la máquina A? Detalle todos los mensajes de DNS que reciba o envíe A a partir de ese momento.

Solución: La máquina envía un mensaje de consulta de DNS al servidor DNS de la máquina A, preguntando por el nombre B.plagas.com.
En función de la razón por la que E pueda haber enviado el mensaje de consulta a A, A hará lo siguiente:
Si A tiene en la cache DNS la respuesta, A responde a E inmediatamente con la dir IP de B: 212.128.2.10.
Si A no tiene en la cache la respuesta:
1) Si la consulta de E es en modo iterativo (por ejemplo porque E tiene un servidor de DNS que está haciendo una consulta a A), A enviará a E la dirección IP de los servidores DNS del dominio plagas.com: 212.128.3.10 (C), 212.128.4.10 (D). Al recibir esta respuesta, E enviará la pregunta a C o a D.
2) Si la consulta de E es en modo recursivo (por ejemplo porque E es un cliente de DNS que tiene a A como su servidor de DNS), A enviará la consulta DNS a C o a D, preguntando por la dirección IP de B.plagas.com. Cualquiera de estos servidores tiene en su mapa la dirección IP de B, por lo que se la enviará a A. A entonces le enviara ? la respuesta a E con la dir IP de B: 212.128.2.10

7. [10 puntos] ¿ Qué funcionalidad de IPSec nos da integridad de los datos transmitidos, pero no confidencialidad?

   A. AH (Autentication Header)

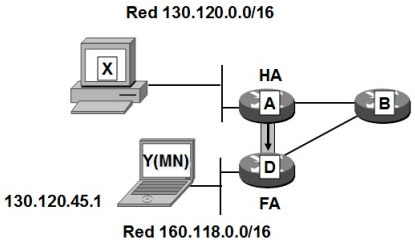
   B. ESP (Encapsulating Security Payload)

   C. IKE (Internet key Exchange)

   D. Cualquiera de los anteriores

Solución: A

8. [10 puntos] Dado el escenario:



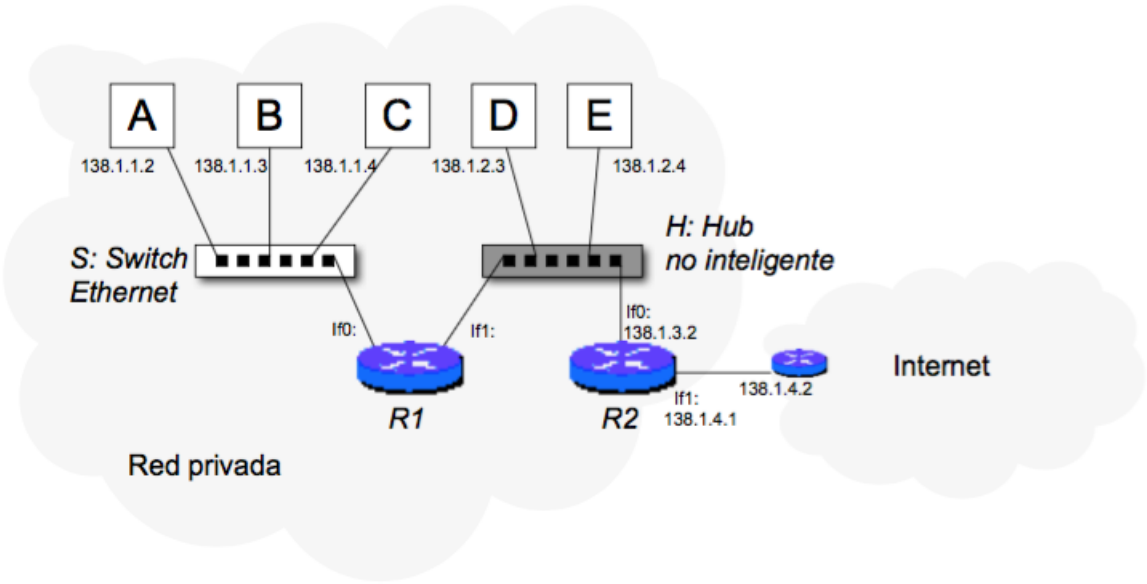
Donde Y es un nodo móvil IP, FA el Foreign Agent y A el Home Agent. Y se ha registrado correctamente, estableciendose un tunel de $HA - - > FA$.
¿ Que ocurrirá al ejecutar X, ping Y?

Solución: No obtendrá respuesta dado que Y resultará nodo inaccesible.

Redes – UNLP
Examen Final 03/09/2016 – Solución

Este examen tiene 2 preguntas con un total de 100 puntos

1. En la siguiente figura se muestra una red privada de una empresa conectada a Internet, donde A, B, C, D y E son máquinas, S es un switch Ethernet, H es un hub no inteligente y R1 y R2 son routers.



Teniendo en cuenta la figura, responda a las siguientes preguntas:

(a) [20 puntos] Un intruso desea espiar el tráfico que envía y recibe la máquina A. El intruso tiene acceso a la máquina B y a la máquina D y puede leer cualquier paquete que se reciba en la interfaz de red de la máquina B y en la de la máquina D. Explique detalladamente en cuál de las dos máquinas el intruso obtendría más información sobre el tráfico que intercambia la máquina A.

(b) [20 puntos] Se desea que todas las máquinas de la red privada dispongan de acceso a Internet. Se conocen las direcciones IP de todas las máquinas y las del router R2 (véase la figura). Indique cuáles deberían ser las tablas de encaminamiento de las máquinas y de los routers, y las direcciones IP de R1 en sus interfaces If0 e If1. Tenga en cuenta que las direcciones IP de las máquinas y las del router R2 no se pueden modificar.

(c) [30 puntos] En el hub no inteligente H se detecta un datagrama IP del que se conoce la siguiente información:

```
Dirección IP origen: 138.1.1.2.
Dirección IP destino: 139.1.1.1.
Protocolo de nivel de transporte TCP.
Campo de datos de TCP:
            GET / HTTP/1.1\r\n
            Host: www.telematicos.ar\r\n
             r\n
```

Indique que otros datagramas IP se habrán enviado previamente para que el datagrama descripto haya podido enviarse. Para cada uno de estos datagramas indique sus direcciones IP origen y destino y todo lo que pueda saber sobre el contenido de su campo de datos.

Nota: Se conoce la siguiente configuración de DNS:

- La máquina E tiene instalado un servidor de DNS, que es secundario del dominio ar.
- Todas las máquinas de la red privada tienen configurado como servidor de DNS a la máquina E.
- Existe un servidor de DNS del dominio raíz en la dirección IP 140.1.1.1.
- Existe un servidor de DNS del dominio ar en la dirección IP 140.2.2.2.
- Existe un servidor de DNS del dominio telematicos.ar en la dirección IP 140.3.3.3.
- Todos los servidores de DNS tienen sus cachés vacías.

Solución:

(a) Si el intruso estuviera en la máquina B, dado que B esta conectado a un switch Ethernet solo podría espiar el tráfico que A y B intercambiasen. Cualquier tráfico que emitiera A con destino a otra máquina diferente de B, el switch Ethernet no lo copiará en la interfaz de red a la que está conectada B solo lo copiará en la interfaz de red donde estuviera el destino.

Si el intruso estuviera en la máquina D, dado que D esta conectado a un hub no inteligente, D podría espiar el tráfico que A intercambiase con cualquier máquina salvo a B y C, es decir, todas las máquinas de Internet, D y E. El hub no inteligente copiará todo el tráfico que reciba por una interfaz en el resto de las interfaces. En concreto todo el tráfico que reciba el hub no inteligente de la interfaz a la que esta conectado R1, o de la interfaz a la que esta conectado E, o de la interfaz a la que esta conectado R2, lo copiara en la interfaz a la que esta conectada D. Desde D, el intruso no podrá espiar el tráfico que intercambian A con B y C.

Por tanto, el intruso podría espiar más tráfico si se instala en la máquina D.

(b)

2. *a*) Las direcciones IP de R1 podrían ser (hay más soluciones):
   - En If0: 138.1.1.1
   - En If1: 138.1.2.1 y 138.1.3.1

   b) Las tablas de encaminamiento de las máquinas:

Tabla de encaminamiento de A, B y C		
Destino	Máscara	Vecino
138.1.1.0	255.255.255.0	0.0.0.0
0.0.0.0	0.0.0.0	138.1.1.1

Tabla de encaminamiento de D y E		
Destino	Máscara	Vecino
138.1.2.0	255.255.255.0	0.0.0.0
0.0.0.0	0.0.0.0	138.1.2.1

   c) La tabla de encaminamiento de R1:

Destino	Máscara	Vecino
138.1.1.0	255.255.255.0	0.0.0.0
138.1.2.0	255.255.255.0	0.0.0.0
138.1.3.0	255.255.255.0	0.0.0.0
0.0.0.0	0.0.0.0	138.1.3.2

   d) La tabla de encaminamiento de R2:

Destino	Máscara	Vecino
138.1.3.0	255.255.255.0	0.0.0.0
138.1.4.0	255.255.255.0	0.0.0.0
138.1.1.0	255.255.255.0	138.1.3.1
138.1.2.0	255.255.255.0	138.1.3.1
0.0.0.0	0.0.0.0	138.1.4.2

(c)

```
Los datagramas IP que se habrán enviado anteriormente son:
Solicitud de DNS desde A hasta E preguntando por la IP de la máquina www.telematicos.ar.
    IP origen: 138.1.1.2
    IP destino: 138.1.2.4

    Solicitud de DNS preguntando por la IP asociada a www.telematicos.ar.
Dado que E es servidor secundario del dominio es conoce cuál es el servidor de DNS
del dominio telematicos.ar.
Por tanto, no sera necesario preguntar al servidor raíz, ni al servidor de ar.
    IP origen: 138.1.2.4
    IP destino: 140.3.3.3
    Solicitud de DNS preguntando por la IP asociada a www.telematicos.ar.

Respuesta desde el servidor de DNS con la resolución de la IP asociada a www.telematicos.ar.
    IP origen: 138.3.3.3
    IP destino: 138.1.2.4
    Respuesta de DNS indicando que la IP de www.telematicos.ar es 139.1.1.1.

Respuesta desde E con la resolución de la IP asociada a www.telematicos.ar.
   IP origen: 138.1.2.4
   IP destino: 138.1.1.2

 Respuesta de DNS indicando que la IP de www.telematicos.ar es 139.1.1.1.
```

2. 30 puntos Un administrador de red esta utilizando OSPF como protocolo interno de ruteo. Se conocen los siguientes paquetes de estado del enlace:

Estado del Enlace de A	
C	2

Estado del Enlace de B	
C	2
E	1

Estado del Enlace de D	
C	3
F	2
G	4

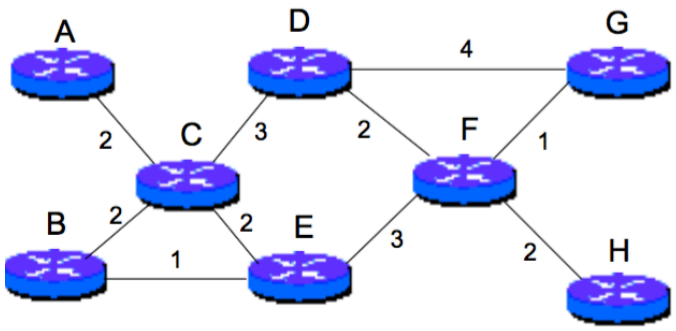
Estado del Enlace de E	
B	1
C	2
F	3

Estado del Enlace de G	
D	4
F	1

Estado del Enlace de H	
F	2

Dibuje la topología de la red del administrador, escriba los paquetes de estado del enlace de los nodos C y F y obtenga el árbol resultante para el nodo C.

Solución:



Estado del Enlace de C	
A	2
B	2
D	3
E	2

Estado del Enlace de F	
D	2
E	3
G	1
H	2

C-A(2),C-B(2),C-D(3),C-E(2),C-E-F(5),C-E-F-G(6),C-E-F-H(7)

Facultad de Informática | UNIVERSIDAD NACIONAL DE LA PLATA

Redes
Examen Final– 12/08/2017
Solución

Este examen tiene 6 preguntas con un total de 100 puntos

1. [15 puntos] En una conexión normal TCP, invocada por un servicio según paradigma cliente servidor, todos los segmentos tienen el flag ACK activado, excepto:

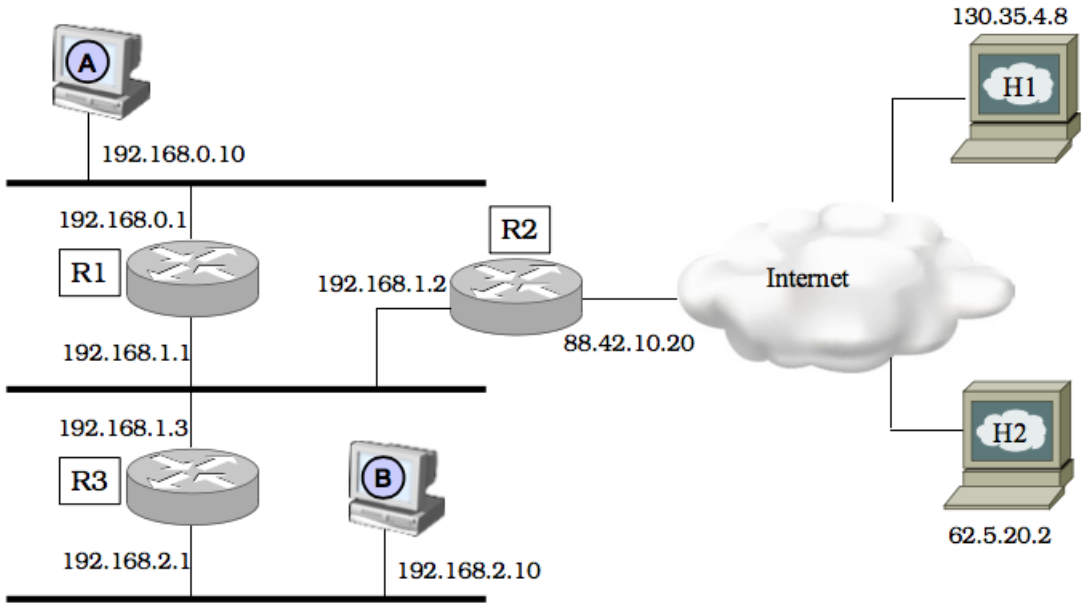
   A. el primer segmento enviado por el servidor

   B. el último segmento enviado por el cliente

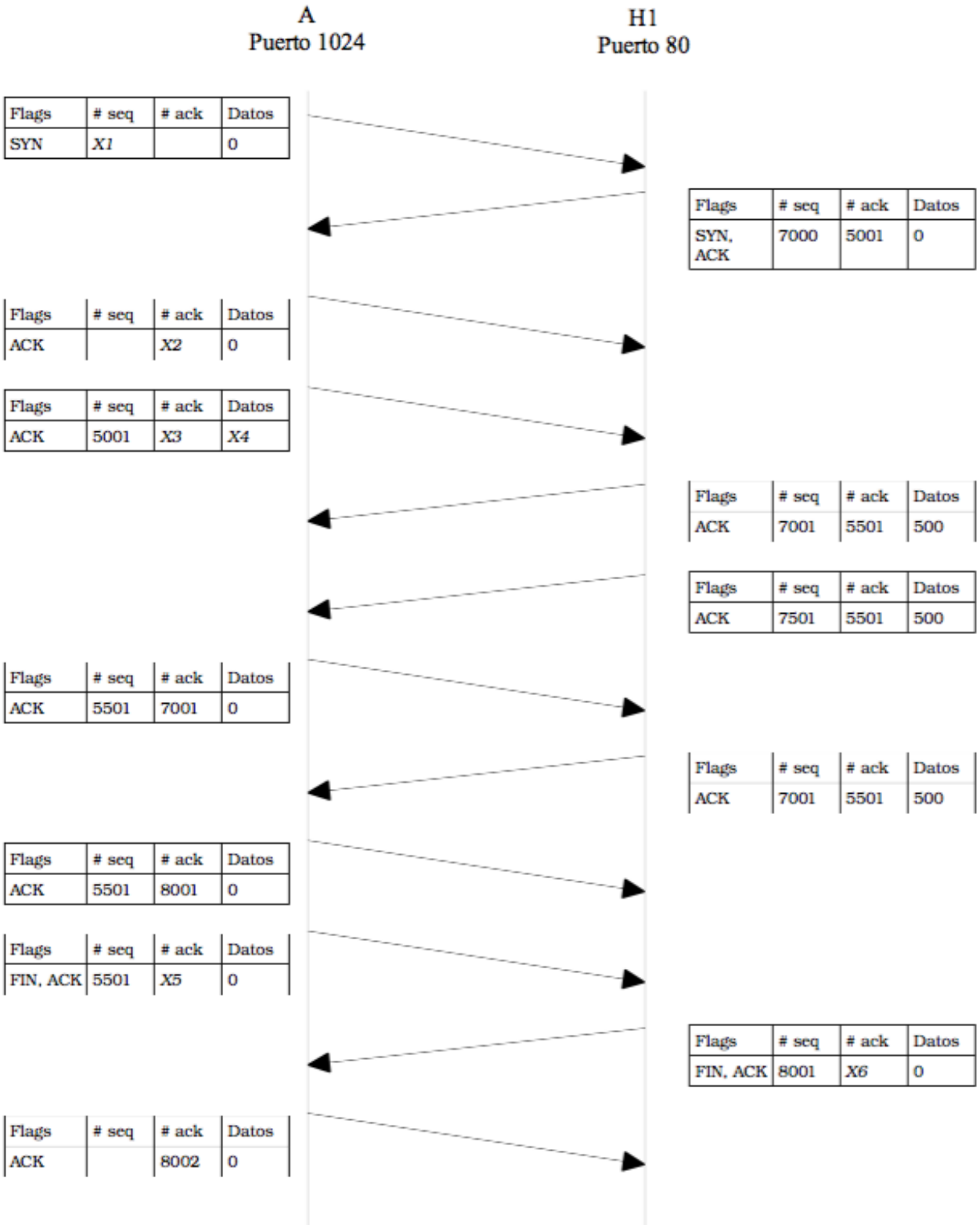
   C. el primer segmento enviado por el cliente

Solución: C

2. En la red de la figura,



A y H1 realizan la siguiente comunicación TCP:



Los campos son:

- Flags: flags de TCP activos
- # seq: numero de secuencia

- # ack: numero de asentimiento
- Datos: tamaño del campo de datos en bytes

La mascara de red en la red privada es 255.255.255.0. Se pide:

(a) [20 puntos] Represente las tablas de rutas completas de A, B, R1 y R3, tales que permitan que A y B puedan comunicarse entre ellos y con Internet.

(b) [5 puntos] ¿Que cantidad de datos se han intercambiado A y H1?. Justifique.

(c) [5 puntos] Determine los parametros X_i.

Solución:

(a)

A:

192.168.0.0	0.0.0.0
0.0.0.0	192.168.0.1

B:

192.168.2.0	0.0.0.0
0.0.0.0	192.168.2.1

R1:

192.168.0.0	0.0.0.0
192.168.1.0	0.0.0.0
192.168.2.0	192.168.1.3
0.0.0.0	192.168.1.2

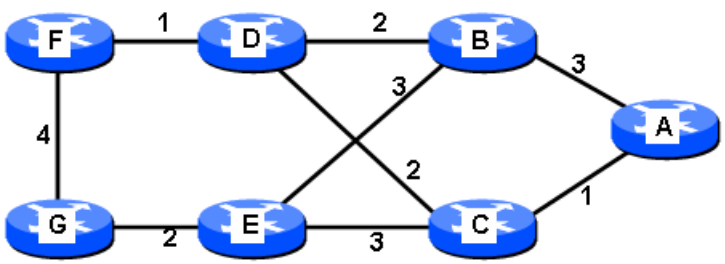
R3:

192.168.2.0	0.0.0.0
192.168.1.0	0.0.0.0
192.168.0.0	192.168.1.1
0.0.0.0	192.168.1.2

(b) A $\Leftarrow$ H1: 500 bytes. Es suficiente mirar los numeros de secuencia. El primer numero de secuencia útil es 5001 y el último es 5501. H1 $\Leftarrow$ A: 1000 bytes. H1 empieza en 7001 y acaba con 8001.

(c) X1: 5000; X2 = X3 = 7001; X4 = 500; X5 = 8001; X6=5502

3. [20 puntos] Se desea utilizar OSPF en la red siguiente:



Indique el árbol correspondiente al nodo D.

Solución:
D-F(1)
D-B(2)
D-C(2)
D-F-G(5)
D-B-E(5)
D-C-A(3)

4. [10 puntos] La principal diferencia de BGP respecto del resto de protocolos de routing es que:
   A. BGP no puede funcionar en entornos 'classless'(CIDR)
   B. Emplea una mética más sofisticada que la mayoría de los protocolos de routing
   C. Permite establecer restricciones para impedir el tráfico de tránsito
   D. Con BGP no está permitido crear topologías malladas

Solución: C

5. [10 puntos] Para enviar un archivo binario por correo electrónico hay que usar la siguiente codificación:
   A. MIME Base 32
   B. MIME Base 64
   C. MIME Quoted-Printable
   D. MIME text/bin

Solución: B

6. [15 puntos] Proponga un sistema seguro y eficiente para distribuir claves que se emplearán para encriptar mensajes con un algoritmo simétrico. Las mismas se deben transmitir con la firma correspondiente.

Solución: Enviarlas como un mensaje más en un sistema tipo RSA con firma digital. Para detalles remitirse a la bibliografía

Facultad de Informática | UNIVERSIDAD NACIONAL DE LA PLATA

Redes
Examen Final– 02/09/2017
Solución

Este examen tiene 6 preguntas con un total de 100 puntos

1. [20 puntos] Suponga que utiliza slow-start en una línea con un tiempo de ida y vuelta de 10 milisegundos. La ventana receptora es de 24 KBytes y el tamaño máximo de segmento es de 2 KBytes. ¿Cuanto tiempo pasará antes de poder enviar la primera ventana completa? Suponga que no hay congestión.

Solución: El crecimiento de la ventana se producirá de la siguiente forma:

Ciclo	Número de segmentos	Cantidad de KBytes	Tiempo transcurrido (ms)
Primero	1	2	0
Segundo	2	4	10
Tercero	4	8	20
Cuarto	8	16	30
Quinto	12	24	40

Por tanto la respuesta es: 40 milisegundos.

2. [15 puntos] Indique si es verdadera o falsa cada una de las siguientes afirmaciones, aclarando la elección adoptada:
   (a) Los protocolos de routing basados en el estado del enlace emplean algoritmos más complejos que los basados en el vector distancia, pero a cambio permiten obtener un detalle completo de la topología de la red.
   (b) La principal ventaja de utilizar múltiples niveles jerárquicos en un protocolo de routing estriba en la posibilidad de elegir la ruta óptima en cada caso.
   (c) En general los protocolos de red orientados a conexión (Frame Relay o ATM por ejemplo) permiten controlar mejor las situaciones de congestión que los no orientados a conexión, (IP o CLNP por ejemplo).

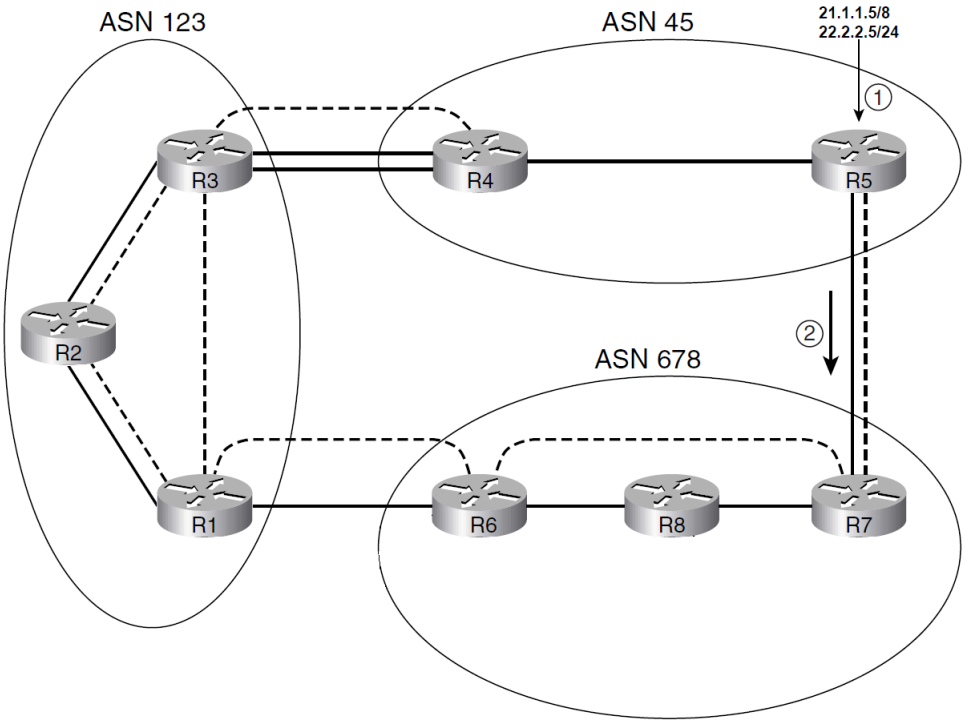
Solución:

(a) Verdadera. El routing basado en el vector distancia solo permite saber cual es el siguiente nodo en el camino óptimo para cada destino, pero se desconoce la ruta, solo se sabe la distancia. En routing basado en el estado del enlace cada nodo sabe la mejor ruta a cada destino, con lo que dispone de un 'mapa'completo de la red; esto requiere algoritmos mas complejos de cálculo de las rutas, pero permite un routing mas robusto.

(b) Falsa. La razón de establecer niveles jerárquicos es reducir la cantidad de información que maneja el protocolo de routing, pero esto puede hacer que las rutas no sean óptimas ya que cada nodo no "ve" toda la red.

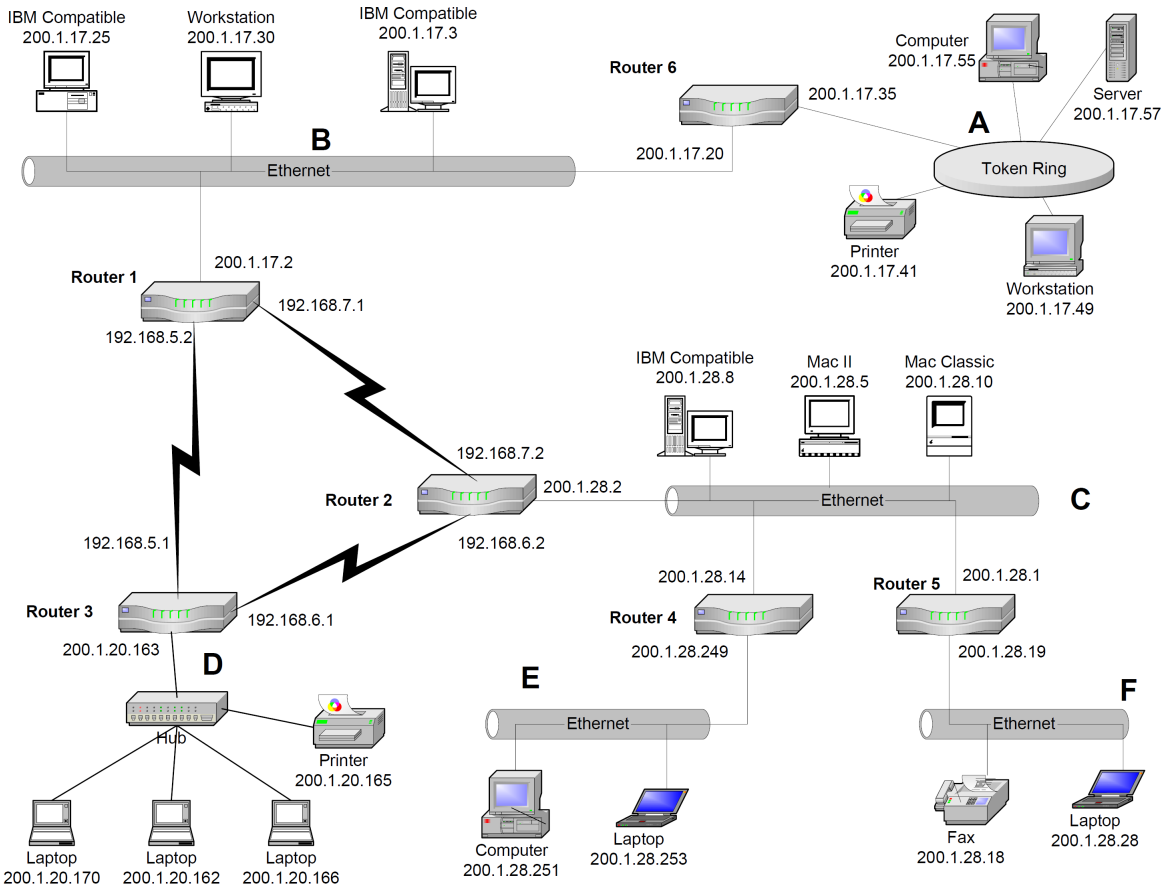
(c) Verdadera. Al ser orientados a conexión pueden ejercer control de admisión, cosa que no es factible en los protocolos de red no orientados a conexión. Además pueden aplicar todas las técnicas habituales en éstos.

3. [20 puntos] En el siguiente diagrama de red se da un caso de aplicación de BGP como ruteo externo. En el instante 1 el "Router" R5 incorpora las rutas que se indican en la figura. En el instante 2 las propaga a su compañero de borde R7. En línea punteada se representan las sesiones BGP, externas e internas entre los "Routers".
   Poco tiempo después del instante 2 un usuario del ASN 123(Sistema Autónomo 123) envía un datagrama al host 22.2.2.6/24 y recibe un mensaje de red inalcanzable.
   Indique posibles causas del mensaje.
   Indique las soluciones posibles.



Solución: La causa más probable es que se haya deshabilitado la sincronización en R6 y por tal motivo incorpora las rutas que les pasó R7 y las propaga al ASN 123. Todavía las nuevas rutas no están presentes en las tablas de los "Routers" internos del ASN 678; R8 todavía no aprendió esas rutas. La solución es habilitar sincronismo en R6 y por las dudas también habilitar la propagación a IGP de los EGP. Para que R7 propague las rutas a R8.

4. [15 puntos] En relación al diagrama de red de la figura, en la que se adoptó RIPv2 como protocolo de ruteo:



(a) Indique la tabla de ruteo completa de los "routers", Router 2 y 6

(b) ¿Qué rutas propagará Router 2 por las interfaces, 192.168.7.2 y 200.1.28.2, sabiendo que se habilitó "split horizon".

5. [15 puntos] Indique, justificando la adopción, cuáles de las siguientes aseveraciones son correctas respecto del modo pasivo y activo de FTP

   A. El modo activo hace que el servidor FTP inicie la conexión con el cliente FTP

   B. El modo activo hace que el servidor FTP se quede "escuchando" en un port efímero y notifique al cliente FTP de ese número de port para que el cliente se conecte a éste.

   C. El modo pasivo hace que el servidor FTP, reserve y comience a "escuchar" en un port efímero y notifique al cliente FTP de ese número de port para que el cliente se conecte a éste.

   D. El modo pasivo no requiere que los números de ports sean transferidos entre el cliente y el servidor; el cliente simplemente crea una conexión de datos contra el port bien conocido 20 del servidor.

Solución: A y C

6. [15 puntos] Entre los protocolos sugeridos para implementar VPNs se encuentran:
   A. PPTP
   B. L2F
   C. L2TP
   D. IPSec
   E. B y C sólamente
   F. Todas las anteriores

Solución: F

Facultad de Informática | UNIVERSIDAD NACIONAL DE LA PLATA

Redes
Examen Final– 25/08/2018
Solución

Este examen tiene 3 preguntas con un total de 100 puntos

1. En la red de la figura adjunta se realizó una transferencia de archivo entre dos dispositivos de la misma. Debajo se vuelcan algunas tramas capturadas con la herramienta Wireshark.

```
No.     Time
43 29.071020
Ethernet II, Src: c8:4c:75:00:00:00, Dst: 6c:3b:e5:00:00:0f
Internet Protocol Version 4, Src: 10.0.8.10, Dst: 10.0.0.20
Transmission Control Protocol
    Source Port: 21
    Destination Port: 23161
    Sequence number: 419    (relative sequence number)
    Acknowledgment number: 91    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window size value: 1026
    Checksum: 0x8e1f [unverified]
    Urgent pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
File Transfer Protocol (FTP)
    229 Entering Extended Passive Mode\r\n
        Response code: Entering Extended Passive Mode (229)
        Response arg: Entering Extended Passive Mode
        Extended passive port: 61544
```

```
No.     Time
44 29.071086
Ethernet II, Src: 6c:3b:e5:00:00:0f, Dst:c8:4c:75:00:00:00
Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.8.10
Transmission Control Protocol
    Source Port: 26411
    Destination Port: 61544
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
    Flags: 0x002 (SYN)
    Window size value: 65535
    Checksum: 0x1103 [unverified]
    Urgent pointer: 0
    Options:
        TCP Option - Maximum segment size: 1460 bytes
        TCP Option - No-Operation (NOP)
        TCP Option - Window scale: 6
```

```
        TCP Option - SACK permitted
        TCP Option - Timestamps: TSval 4841202, TSecr 0

No.     Time
45 29.071123
Ethernet II, Src: c8:4c:75:00:00:00, Dst: 6c:3b:e5:00:00:0f
Internet Protocol Version 4, Src: 10.0.8.10, Dst: 10.0.0.20
Transmission Control Protocol
    Source Port: 61544
    Destination Port: 26411
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    1010 .... = Header Length: 40 bytes (10)
    Flags: 0x012 (SYN, ACK)
    Window size value: 65535
    Checksum: 0x9696 [unverified]
    Urgent pointer: 0
    Options:
        TCP Option - Maximum segment size: 1460 bytes
        TCP Option - No-Operation (NOP)
        TCP Option - Window scale: 6
        TCP Option - SACK permitted
        TCP Option - Timestamps: TSval 998380425, TSecr 4841202

No.     Time
 46 29.071128
Ethernet II, Src: 6c:3b:e5:00:00:0f, Dst: c8:4c:75:00:00:00
Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.8.10
 Transmission Control Protocol
    Source Port: 26411
    Destination Port: 61544
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x010 (ACK)
    Window size value: 1026
    Checksum: 0xc15f [unverified]
    Urgent pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps


No.     Time
54 29.072769
Transmission Control Protocol
    Source Port: 61544
    Destination Port: 26411
```

```
    Sequence number: 2049    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x011 (FIN, ACK)
   Window size value: 1026
   Checksum: 0xb95c [unverified]
    Urgent pointer: 0

No.     Time
55 29.072773
Transmission Control Protocol
    Source Port: 26411
    Destination Port: 61544
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 2050    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x010 (ACK)
    Window size value: 1026
    Checksum: 0xb95c [unverified]
    Urgent pointer: 0

No.     Time
56 29.072890
Transmission Control Protocol
    Source Port: 26411
    Destination Port: 61544
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 2050    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x011 (FIN, ACK)
    Window size value: 1026
    Checksum: 0xb95a [unverified]
    Urgent pointer: 0
```

(a) [15 puntos] identifique las sesiones activas en el instante correspondiente a la trama No.54

(b) [15 puntos] Indique ventajas de haber incluido la opción SACK.

(c) [10 puntos] ¿Cuál habrá sido el volumen de datos transferido?

(d) [15 puntos] ¿Con qué valor de ventana de recepción habrán finalizado la sesión indicada en la captura, ambos equipos?

Solución:

(a) Tenemos dos sesiones entre los mismos hosts
client, 10.0.0.20

server, 10.0.8.10
La sesión de control entre los ports 21 y 23161
La de datos entre 26411 y 61544

(b) Se retransmiten los segmentos faltantes solamente

(c) Basta restar los números de secuencia final e inicial = 2048 bytes.

(d) 1026 x 64 = 65664 (factor de escala 64)

2. Considerando la red de la figura adjunta en la que los enlaces son de 1Mbps excepto router6-router5 y router5-router1 que son de 1Gbps.
   (a) [15 puntos] Complete la tabla de ruteo de router6 si el protocolo empleado fue RIPv2.
   (b) [15 puntos] Habría alguna diferencia si el protocolo hubiera sido OSPF?

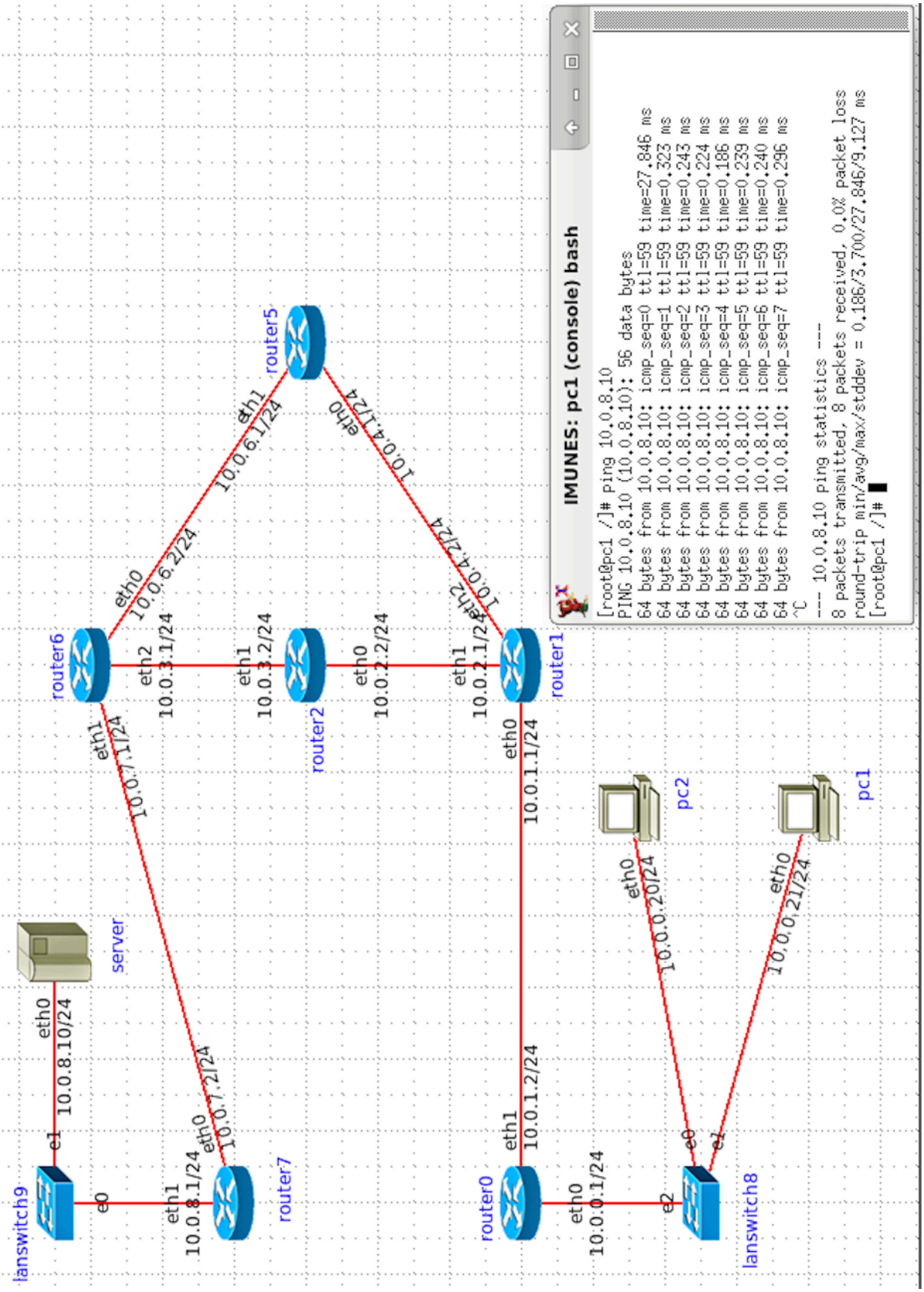
Solución:

(a)

(b) La diferencia es que por usar como métrica el camino más rápido la ruta para alcanzar la red 10.0.2.0/24 tendría como próximo salto la IP 10.0.6.1/24 en lugar de 10.0.3.2/24 como en el caso de RIP

3. [15 puntos] ¿Qué funcionalidad de IPSec nos da integridad de los datos transmitidos, pero no confidencialidad?
   A. AH (Autentication Header)
   B. ESP (Encapsulating Security Payload)
   C. IKE (Internet key Exchange)
   D. Cualquiera de los anteriores
   E. Todas las anteriores

Solución: A


IMUNES: pc1 (console) bash
[root@pc1 /]# ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10): 56 data bytes
64 bytes from 10.0.8.10: icmp_seq=0 ttl=59 time=27.846 ms
64 bytes from 10.0.8.10: icmp_seq=1 ttl=59 time=0.323 ms
64 bytes from 10.0.8.10: icmp_seq=2 ttl=59 time=0.243 ms
64 bytes from 10.0.8.10: icmp_seq=3 ttl=59 time=0.224 ms
64 bytes from 10.0.8.10: icmp_seq=4 ttl=59 time=0.186 ms
64 bytes from 10.0.8.10: icmp_seq=5 ttl=59 time=0.239 ms
64 bytes from 10.0.8.10: icmp_seq=6 ttl=59 time=0.240 ms
64 bytes from 10.0.8.10: icmp_seq=7 ttl=59 time=0.296 ms
^C
--- 10.0.8.10 ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.186/3.700/27.846/9.127 ms
[root@pc1 /]#
lanswitch9
server
router7
router6
router5
router2
router1
router0
pc2
pc1
lanswitch8
10.0.8.10/24
10.0.8.1/24
10.0.7.2/24
10.0.7.1/24
10.0.6.2/24
10.0.6.1/24
10.0.3.1/24
10.0.3.2/24
10.0.4.1/24
10.0.4.2/24
10.0.2.2/24
10.0.2.1/24
10.0.1.1/24
10.0.1.2/24
10.0.0.1/24
10.0.0.20/24
10.0.0.21/24