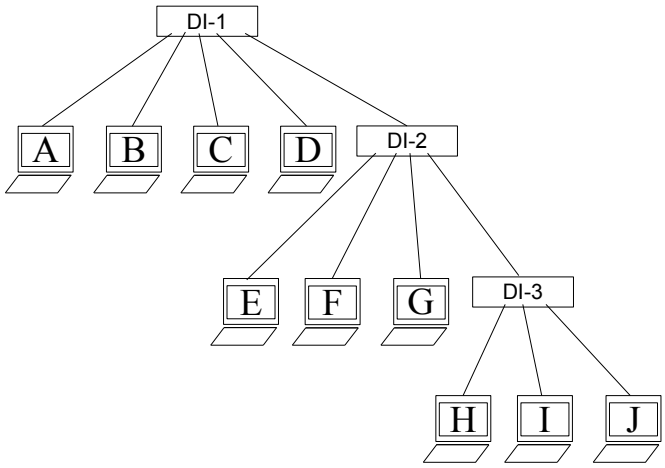
2º Parcial de Redes - ETSIA - 9 de junio de 2011

Apellidos, Nombre:_____
Grupo de matrícula:_____

1. (2 puntos) En la siguiente figura se proporciona la topología de una red Ethernet. Los dispositivos: DI-1, DI-2 y DI-3 de la figura representan los diferentes dispositivos de interconexión (Router, Switch y/o Hub) que conforman dicha red. Indica de qué tipo de dispositivo de interconexión se trata en cada una de las siguientes situaciones. Justifica tu respuesta. Nota: DI-1, DI-2 y DI-3 no tienen por qué ser del mismo tipo de dispositivo en todos los apartados.



a) Si A envía una trama a J, llegará una copia de la trama original a las tarjetas de red situadas en las máquinas E, F, G y J.

Si únicamente reciben copia de la trama J y las máquinas conectadas a DI-2, quiere decir que tanto A como J están conectadas a Switches, ya que estos separan dominios de colisión, de forma que impiden que las demás máquinas conectadas a ellos reciban tramas no dirigidas a ellas. Por otra parte, si E, F y G reciben copia de la trama, será porque están conectadas a un Hub, que no separa dominios de colisión y por lo tanto la trama que recibe DI-2 dirigida a J, será retransmitida por todos los puertos del dispositivo DI-2 excepto por el que fue recibida. Por todo ello, tenemos que DI-1 y DI-3 son Switches y DI-2 un Hub.

b) Si A realiza una difusión Ethernet recibirán una copia de la trama las estaciones B, C, D y DI-2. Instantes después H envía una trama a A, y sólo A recibe una trama que contiene el datagrama.

Al realizar A una difusión Ethernet, deben recibir la trama todas las máquinas pertenecientes a dicha red Ethernet. Que únicamente la reciben las máquinas conectadas a DI-1 y el dispositivo DI-2 significa que DI-2 es un Router, capaz de separar dominios de colisiones y de difusión.

Por otro lado, si cuando H envía una trama a A, y sólo A recibe la trama que contiene el datagrama, es porque, DI-1 y DI-3 son Switches. DI-1 y DI-3 sólo transmiten la trama por el enlace que encamine hacia A, ya que son capaces de separar dominios de colisión.

c) B inicia el envío de una trama a I, al mismo tiempo J inicia una transmisión dirigida a B, de modo que B está transmitiendo y recibiendo simultáneamente. Tanto I como B reciben una copia de la trama original sin que se produzcan colisiones.

Para conseguir este comportamiento, DI-1, DI-2 y DI-3 deben de ser switches, que únicamente retransmitirán la trama por el enlace que encamine hacia el destino de la misma. Además para que B pueda estar transmitiendo y recibiendo simultáneamente, DI-1 debe funcionar en modo full-duplex.

d) Se realiza una transmisión de A a B y simultáneamente otra de D a G y otra de I a J. Se produce una colisión, que reciben las estaciones: E, F, G, H, I y J.

Si se produce una colisión que afecta a las máquinas E,F,G (conectadas a DI-2) y H, I y J (conectadas a DI-3) es porque DI-2 y DI-3 son Hubs, que no separan dominio de colisión (son incapaces de determinar porque enlace deben de retransmitir la trama, ya que trabajan a nivel físico y no de enlace). Sin embargo, el hecho de que las estaciones conectadas a DI-1 no se vean afectadas por ninguna colisión, implica que DI-1 es un switch, capaz de separar dominios de colisión.

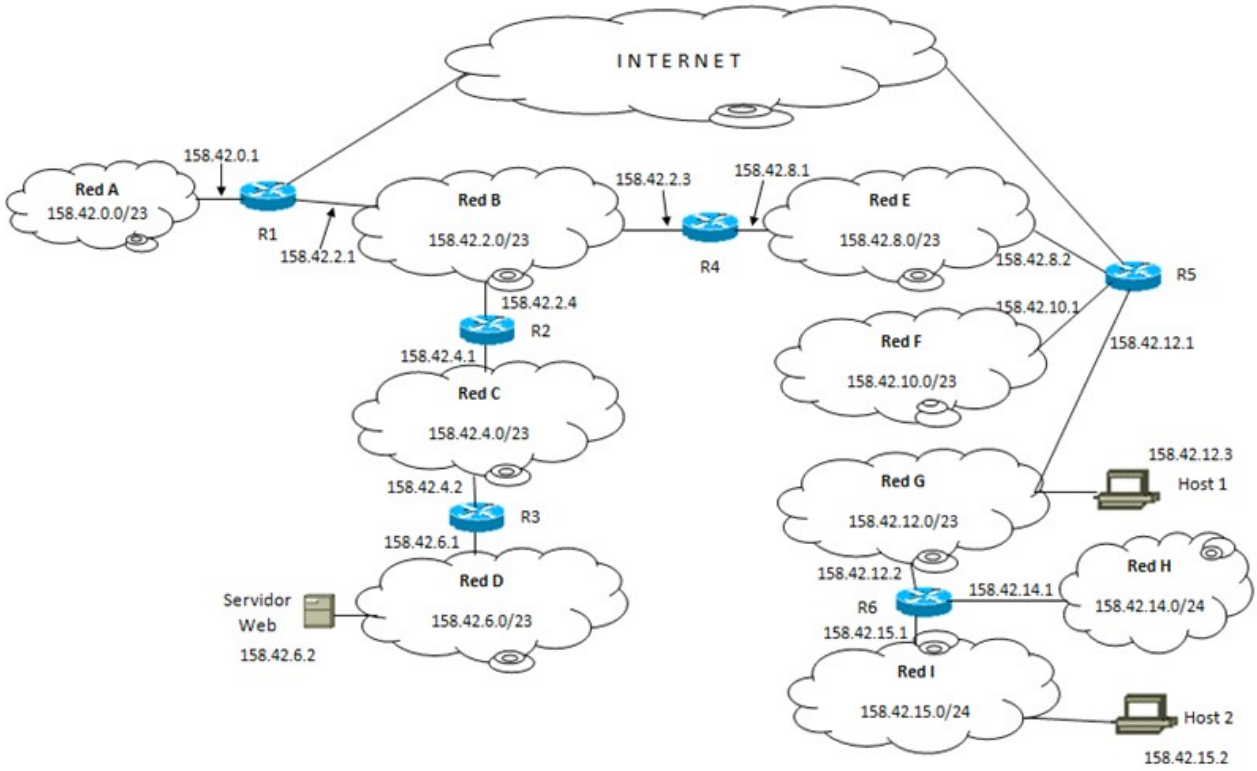
2. (1 punto) Dado un canal de comunicaciones con un ancho de banda de 3000 Hz, a) ¿cuántos armónicos lo atravesarán si transmitimos de forma periódica el carácter de 8 bits 01100001 a 9600 bps? Justifica tu respuesta.

Dado que transmitimos de forma periodica un carácter de 8 bits a 9600 bps, tendremos 1200 caracteres por segundo. Esta es la frecuencia fundamental de la señal. Sabiendo que los armónicos de la señal están equiespaciados, tan solo queda dividir 3000 Hz entre 1200 Hz y quedarnos con la parte entera. Es decir, atravesarán el canal 2 armónicos.

b) ¿Qué ocurrirá si se aumenta la velocidad de transmisión?

Si se aumenta la velocidad de transmisión, aumentará la frecuencia fundamental, de acuerdo a lo explicado en el apartado a), y por tanto disminuirá el número de armónicos que atraviesen el canal.

3. (2,75 puntos) La red corporativa de cierta institución presenta la topología de la figura. El tamaño máximo de las subredes A, B, C, D, E, F y G es de 500 hosts cada una y para las subredes H e I el tamaño máximo es de 250 hosts cada una. La institución dispone de la dirección de red 158.42.0.0/20.



2º Parcial de Redes - ETSIA - 9 de junio de 2011

Apellidos, Nombre:_____
Grupo de matrícula:_____

a) Teniendo en cuenta que la interfaz del router R1 con la red A tiene la dirección IP 158.42.0.1, asigna direcciones IP a cada una de las redes de la organización – indicando máscara y dirección de difusión dirigida – y a cada uno de los dispositivos que lo requieran para su correcto funcionamiento. La asignación de direcciones IP debe cumplir que las tablas de encaminamiento de los routers tengan el mínimo número de entradas.

158.42.00000**000**0.00000000 → 158.42.0.0/23 RED A
158.42.00000**001**0.00000000 → 158.42.2.0/23 RED B
158.42.00000**010**0.00000000 → 158.42.4.0/23 RED C
158.42.00000**011**0.00000000 → 158.42.6.0/23 RED D
158.42.00001**00**0.00000000 → 158.42.8.0/23 RED E
158.42.00001**01**0.00000000 → 158.42.10.0/23 RED F
158.42.00001**10**0.00000000 → 158.42.12.0/23 RED G
158.42.00001**11**0.00000000 → 158.42.14.0/24 RED H
158.42.00001**11**1.00000000 → 158.42.15.0/24 RED I

b) Obtén las tablas de encaminamiento para los routers R1, R5 y R6 y para el host 1.

Tabla de encaminamiento del router R1			
Destino	***Máscara***	***Ruta***	***Interfaz***
158.42.0.0	/23	0.0.0.0	158.42.0.1
158.42.2.0	/23	0.0.0.0	158.42.2.1
158.42.4.0 (C,D)	/22	158.42.2.4	158.42.2.1
158.42.8.0 (E,F,G,H,I)	/21	158.42.2.3	158.42.2.1
0.0.0.0	0.0.0.0	A.B.C.D	a.b.c.d
Tabla de encaminamiento del router R5			
Destino	***Máscara***	***Ruta***	***Interfaz***
158.42.8.0	/23	0.0.0.0	158.42.8.2
158.42.10.0	/23	0.0.0.0	158.42.10.1
158.42.12.0	/23	0.0.0.0	158.42.12.1
158.42.14.0 (H,I)	/23	158.42.12.2	158.42.12.1
158.42.0.0 (A,B,C,D)	/21	158.42.8.1	158.42.8.2
0.0.0.0	0.0.0.0	E.F.G.H	e.f.g.h
Tabla de encaminamiento del router R6			
Destino	***Máscara***	***Ruta***	***Interfaz***
158.42.12.0	/23	0.0.0.0	158.42.12.2
158.42.14.0	/24	0.0.0.0	158.42.14.1
158.42.15.0	/24	0.0.0.0	158.42.15.1
0.0.0.0	0.0.0.0	158.42.12.1	158.42.12.2

Tabla de encaminamiento del host 1			
Destino	***Máscara***	***Ruta***	***Interfaz***
158.42.12.0	/23	0.0.0.0	158.42.12.3
158.42.14.0	/23	158.42.12.2	158.42.12.3
0.0.0.0	0.0.0.0	158.42.12.1	158.42.12.3

4. (0,5 puntos) ¿Es posible que aparezcan en la columna "Ruta" de la tabla de encaminamiento de un router (R1) otro router (R2) conectado en una red distinta a las que está conectado el router R1? Razona la respuesta.

En la columna ruta de la tabla de encaminamiento de un router (r1) no puede aparecer otro router (r2) que no esté conectado a alguna de las redes en las que está conectado el primero (r1), dado que para que un router pueda entregar datagramas a otro router los dos deben estar conectados a una red común en la que estén ambos conectados.

5. (0,5 puntos) En el ordenador A se ha configurado iptables mediante las siguientes órdenes:

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

Se pide añadir las órdenes iptables necesarias para que el único tráfico permitido con el exterior sea el de acceso a un servidor web y a un servidor ssh que se ejecutan en el ordenador A. Se supone que los servidores escuchan en los puertos estándar establecidos por los protocolos HTTP y ssh.

```
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
**********
```

Si además se desea permitir el acceso a los servidores DNS situados en otros ordenadores habría que añadir:

```
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT
```

6. (0,5 puntos) ¿Cómo podemos saber si una dirección IP pertenece a nuestra red? ¿Qué información necesitamos conocer?

Podemos saber si una dirección IP pertenece a nuestra red comparando los bits pertenecientes al identificador de red de la dirección IP con los bits de identificación de red de nuestra IP o con la dirección de red de nuestra red.

Para poder determinar los bits pertenecen al identificador de red, es necesario conocer la máscara de red. Por lo que necesitaríamos la máscara de red y la dirección IP de red de nuestra red o cualquier otra dirección IP de nuestra red.

2º Parcial de Redes - ETSIA - 9 de junio de 2011

Apellidos, Nombre:_____
Grupo de matrícula:_____

7. (0,75 puntos) ¿Qué problema resuelve que un protocolo de enlace proporcione transparencia de datos? ¿De qué formas puede resolverlo? Pon un ejemplo de utilización de cada una de las propuestas que indiques utilizando el envío de la secuencia 1000111101111111010100010. Considera como marcadores de inicio y fin la secuencia de bits 01111110.

La transparencia de datos resuelve el problema de que se puedan confundir los marcado de inicio o fin de trama, o cualquier otro carácter especial con los datos de la trama.

Se puede resolver aplicando las técnicas de relleno de bit o relleno de byte, dependiendo de si la transmisión está orientada a bit o a byte respectivamente.

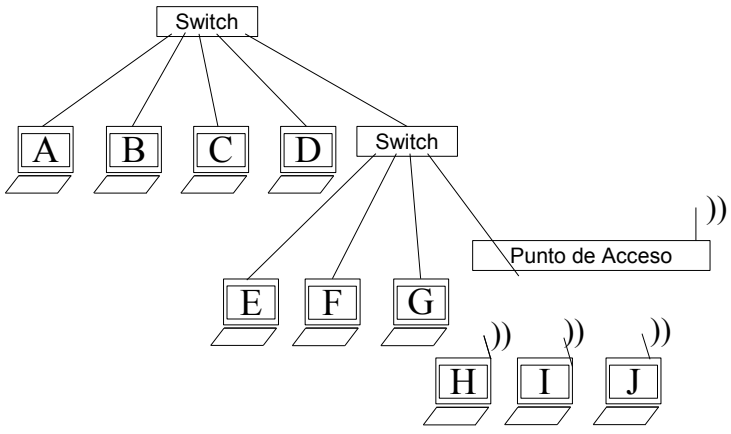
Ejemplo:
aplicando relleno de bit:

01111110 10001111011111 **0** 1010100010 01111110

aplicando relleno de byte:

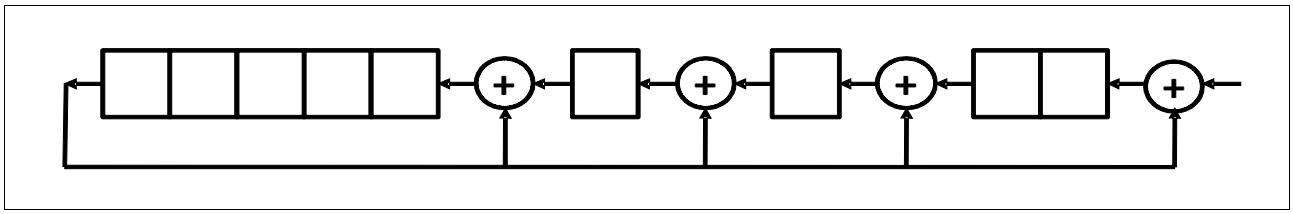
01111110 10001111 **01111101** 0111111010100010 01111110

8. (0,75 puntos) Dada la topología mostrada en la siguiente figura, se realiza una transmisión de A a J. Indica las direcciones físicas e IPs relacionadas que aparecen en la trama que recibe J conteniendo la petición ARP. Se asume que las caches arp de todos los sistemas están vacías.



Dirección 1 (Dir. Destino) : J
Dirección 2 (Dir. Origen): PA
Dirección 3 : A

9. (0,75 puntos) Se quiere enviar los datos D =1110001101. Dibuja la implementación hardware para calcular el CRC que habría que añadir a dichos datos si emisor y receptor han acordado utilizar el polinomio generador $x^9+x^4+x^3+x^2+1$



10. (0,5 puntos) Tal y como se observó en la práctica 9 (análisis del tráfico de red) ¿Qué sucede cuando se intenta establecer una conexión TCP con un puerto cerrado si el destino tiene instalado un cortafuegos?

El protocolo TCP especifica que frente a un intento de conexión a un puerto cerrado debe responderse mediante un segmento de tipo RST (Reset). Sin embargo, la existencia de un cortafuegos hace que se descarte la petición sin ningún tipo de respuesta. El efecto que se observa es el vencimiento repetido del temporizador de TimeOut, y por tanto múltiples retransmisiones del segmento de establecimiento de conexión, con un tiempo de espera que se duplica en cada intento.