Examen – 24 de febrero de 2014

(ref: solredes20140224.odt)

Instrucciones

- **Indique su nombre completo y número de cédula en cada hoja.**
- **Numere todas las hojas e indique la cantidad total de hojas que entrega en la primera.**
- **Escriba las hojas de un solo lado y utilice una caligrafía claramente legible.**
- **Comience cada pregunta teórica y cada ejercicio en una hoja nueva.**
- **Sólo se responderán dudas de letra. No se responderán dudas de ningún tipo los últimos 30 minutos del examen.**
- **El examen es individual y sin material. Apague su teléfono celular mientras esté en el salón del examen.**
- **Es obligatorio responder correctamente al menos 15 puntos en las preguntas teóricas y 20 de los problemas prácticos.**
- **El puntaje mínimo de aprobación es de 60 puntos.**
- **Para todos los ejercicios, si es necesario, puede suponer que dispone de los tipos de datos básicos (p.ej. lista, cola, archivo, string, etc.) y sus funciones asociadas (ej: tail(lista), crear(archivo), concatenar(string, string).**
- **Justifique todas sus respuestas.**
- **Duración: 3 horas. Culminadas las 3 horas el alumno no podrá modificar las hojas a entregar de ninguna forma.**

Preguntas Teóricas

Pregunta 1 (8 puntos)

a) Explique cómo un servidor web identifica el tipo de navegador (y por lo tanto también podría identificar el tipo de dispositivo) desde donde recibe un GET, de forma de definir qué versiones de los diferentes objetos de una página web son devueltos.
b) Ejemplifique la utilidad de implementar lo explicado en la parte anterior.

Solución

a)
Lo realiza a través de la interpretación del valor del campo "User-Agent" contenido en el encabezado de los mensajes GET de HTTP. Dicho campo contiene información que permite inferir el navegador que se está utilizando y el sistema operativo y eventualmente la plataforma donde está instalado.

Lo siguiente no forma parte de la respuesta solicitada. Se incluye con el objetivo de ejemplificar.

Ejemplos de valores de dicho campo:
- GET desde un **Google Chrome** instalado en una **computadora** con **SO Linux**
Mozilla/5.0 (X11; **Linux x86_64**) AppleWebKit/537.36 (KHTML, like Gecko) **Chrome/32.0.1700.77** Safari/537.36
- GET desde un **Google Chrome** instalado en un **smartphone** con **SO Android**
Mozilla/5.0 (Linux; **Android 4.2.2; SGH-I337M** Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) **Chrome/32.0.1700.99 Mobile** Safari/537.36

b)

Si el servidor web identifica desde qué tipo de terminal se realiza la petición podrá "customizar" la respuesta buscando que sea la más adecuada para el cliente (navegador). Por ejemplo, si la solicitud viene desde un *smartphone* se buscará desplegar, del contenido total (el que se le desplegaría al usuario ante una consulta proveniente desde un navegador instalado en una computadora convencional) lo más relevante, considerando que el usuario del *smartphone* no está dispuesto ni le resulta muy sencillo recorrer las páginas web tradicionales. De allí que aparecen URLs del estilo **www.sitio.com.uy**, **m.sitio.com.uy** y/o **www.sitio.com.uy/m**.

Pregunta 2 (6 puntos)

Considere un enlace L con capacidad C, sobre el cual solamente se establecen tres conexiones TCP (no existe otro tráfico TCP, UDP, etc).

a) Suponiendo que cada una de las conexiones TCP intentan trasmitir a la mayor tasa posible, cuál será la tasa de transferencia de c/u de ellas en régimen?

b) Si se inicia un flujo UDP de tasa C/2 y se mantienen las conexiones TCP anteriores, cuál será la nueva tasa de c/u de las conexiones TCP en régimen?

Solución

a)
Se puede ver que TCP cumple con la propiedad de equidad (*fairness*), y por lo tanto tenderá a repartir el ancho de banda equitativamente, es decir, una tasa de C/3 para cada conexión.

b)
UDP no tiene control de congestión, y por lo tanto intentará usar toda la capacidad que necesita, es decir C/2.
Las conexiones TCP, siguiendo el principio de equidad, se repartirán la capacidad restante, es decir, una tasa de C/6 para cada una.

Pregunta 3 IRC (10 puntos)

a) Identifique los elementos principales de la arquitectura de IP móvil, y en particular explique los conceptos de dirección permanente y dirección cedida (*COA – care of address*) de un nodo móvil.
b) Explique la función de agente propio (*home agent*) en el encaminamiento de paquetes entre un nodo corresponsal y un nodo móvil.

Solución

a)
red propia (*home network*).
red visitada (*visited network*).
nodo móvil.
nodo corresponsal.
agente propio (*home agent*).
agente ajeno (*foreign agent*).
red de área extensa (*wan*).
Direccionamiento.

se puede ver un esquema general en el capítulo 6, fig. 6.22

La dirección permanente del nodo móvil es la que se le adjudica en la *home network*.
La dirección cedida (COA) es la que obtiene el nodo móvil en la red visitada (por ejemplo mediante DHCP).

b)
En el esquma de **enrutamiento indirecto**, el nodo correspondiente que quiere enviar un datagrama al nodo móvil desconoce que está en una red visitada y tiene una COA; por lo tanto envía datagramas a la dirección permanente del nodo móvil. Estos datagramas llegarán a la *home network*, y deberán ser interceptados por el *home agent*, quién deberá redirigirlos al nodo móvil. Esto es posible porque el *home agent* conoce la COA del nodo móvil; para preservar la integridad del datagrama, se encapsula en un datagrama con la nueva dirección de destino (la COA).

En el esquema de **enrutamiento directo**, el nodo correspondiente interroga al *home agent* sobre la COA del nodo móvil, y envía los datagramas directamente a la red visitada, evitando que el tráfico sea redirigido en la *home network*.

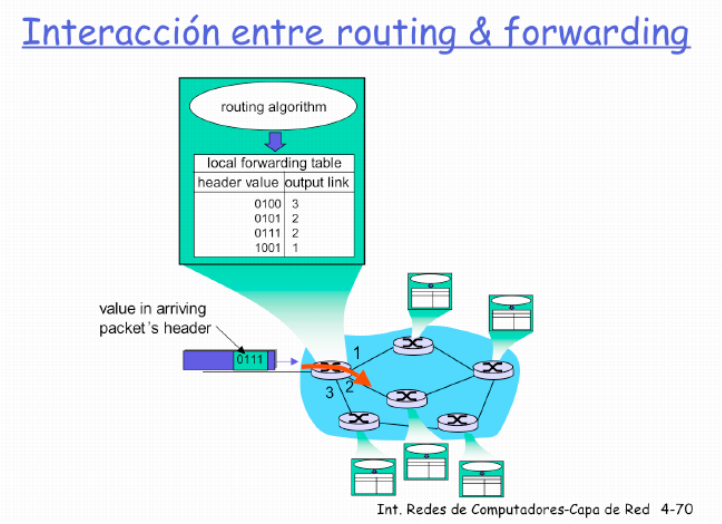
Pregunta 3 RC (10 puntos)

a) En un contexto unicast, describa los procesos de forwarding y enrutamiento, y explique como se relacionan.
b) En un contexto broadcast, describa un proceso de flooding, y explique como se puede transformar en flooding controlado.

Solución

a)
El proceso de enrutamiento permite determinar el camino entre nodos de la red, típicamente mediante intercambio de información de topología y ejecución de un algoritmo en cada nodo para determinar el camino al resto de los nodos.
El proceso de *forwarding* consiste en copiar cada paquete entrante a un nodo al puerto de salida adecuado para que siga su camino en la red (o entregarlo a un proceso local si el

destinatario es el propio nodo). La tabla de *forwarding*, que asocia destinos con puertos (o interfaces) del nodo/router, se construye en base a la información de enrutamiento.



b)

Pregunta 4 (8 puntos)

Describa el funcionamiento de la herramienta *traceroute*, explicando sobre qué protocolo(s) funciona y cómo lo(s) usa.

Solución

Sección 4.4, pág. 345.

Pregunta 5 (8 puntos)

a) Identifique los componentes del retardo en las redes de paquetes, y señale cuáles son los más significativos.
b) Señale las diferencias entre el ancho de banda y la velocidad de propagación en el medio.
c) ¿En qué componente del retardo influye la congestión?

Solución

a)

Retardo de procesamiento en el nodo.
Por ejemplo chequeo de paridad (CRC), determinar enlace de salida (enrutamiento).

Retardo de encolamiento (buffering).
Espera en colas del enlace de salida para trasmisión.

Retardo de trasmisión.
Sea R=ancho de banda del enlace (bps) y L=longitud del paquete (bits), el tiempo de envío = L/R.

Retardo de propagación.
Sea d = longitud del enlace físico y s = velocidad de propagación en el medio, el retardo de propagación = d/s.

b)

Ancho de Banda de una interfaz es la cantidad de bits que esta puede introducir en el medio de transmisión por unidad de tiempo.

La velocidad de propagación es la velocidad con la que un bit viaja dentro del medio físico de transmisión. Es una característica del medio, por ejemplo s~2x108 m/seg en cobre.

c)

El retardo de encolamiento depende del nivel de congestión del router ya que a más datagramas llegando por segundo a la cola más larga será esta y más tiempo deberá esperar un datagrama en ella hasta que sea reenviado.

Problemas Prácticos

Problema 1 (30 puntos)

Sea el protocolo AX.25-- *(Amateur Packet Radio Link Layer Protocol Reducido)* de capa enlace (ver especificación más abajo).

Se cuenta con las siguientes funciones para el acceso al medio, e interconexión con la capa superior y procesamiento de FCS (Frame Check Sequence):

- `getBit(b)`; recibe en b el siguiente bit recibido en la transmisión. En caso de no disponer de bit para entregar bloquea el retorno hasta contar con un bit.
- `putBit(b)`; transmite a la capa física un bit para su envío.
- `getDatosTrama(address,info);` solicita a la capa superior los datos que debe contener la trama que será enviada y los devuelve por referencia. Los campos se entregan con todos los bits contenidos en la trama sin la aplicación de bit *stuffing*. Función bloqueante que retorna cuando dispone de una trama a transmitir.
- `upDatosTrama(address,info)`; entrega a la capa superior los datos de la trama recibida. Los parámetros corresponden a los campos de la trama *address* e *info* respectivamente sin la aplicación de bit *stuffing*. .
- `bool checkFCS(trama,FCS)`; devuelve true en caso de chequear el FCS con la trama y en caso contrario false.
- `getFCS(trama,FCS)`; calcula el FCS para la trama pasada por parámetro.

Especificación AX25-- :

Una transmisión AX.25-- se compone de tramas compuesta de diferentes campos. Las tramas tiene el siguiente formato:

Flag	**Address**	**Info**	**FCS**	**Flag**
011110	112 a 224 bits	N* 8 bits	16 bits	011110

El campo de ***Flag*** (valor 011110) indica el comienzo y el final de una trama. Para asegurar que el campo *flag* no se repite se utiliza *bit stuffing* (añadir en la emisión un cero cada vez que se encuentren 3 bits consecutivos de valor 1 y con un procedimiento inverso en la recepción, donde si se encuentren 3 bits consecutivos de 1, hay que suprimir el 0 que sigue en caso de no ser una flag).

El campo ***Address*** tiene un tamaño entre 112-224 bits. Una dirección AX25-- contiene 55 bits y se le agrega 0 en caso que contenga otra dirección y 1 en caso de ser la última. La trama contiene como mínimo 2 direcciones y 4 como máximo.

El campo ***FCS*** (Frame Check Sequence) contiene 16 bits que permiten verificar el contenido de la trama enviada. El mismo se calcula para toda la trama sin considerar las flags ni la aplicación de *bit stuffing*.

Se pide:

a) Implemente el procedimiento de entramado y transmisión `enviar()` que solicita datos a la capa superior, arma la trama y envía la misma por el enlace físico.

b) Diseñe la máquina de estados que modela la recepción de los bits desde el canal físico y los devuelve sin *bit stuffing*.

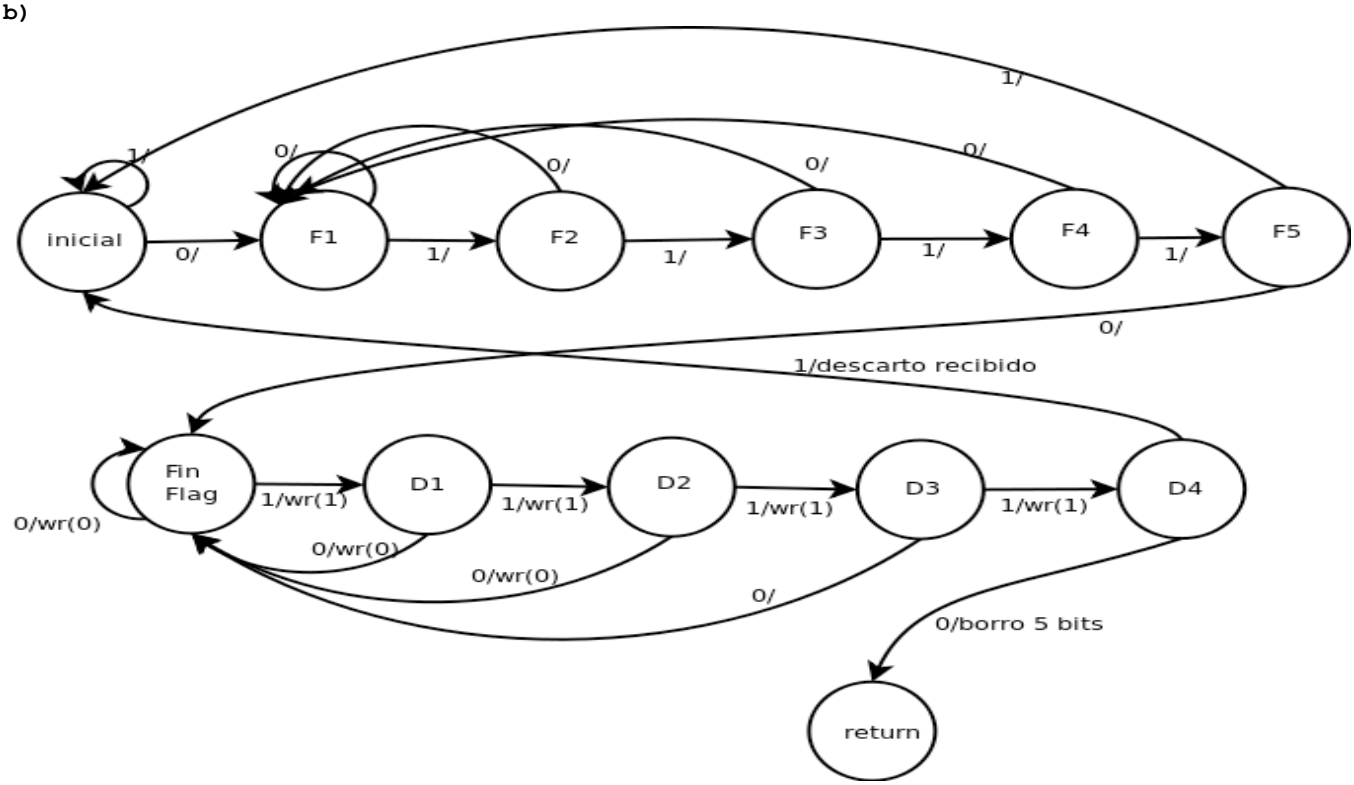
c) Implemente el procedimiento `recibir()` que solicita datos de la capa física y envía los datos recibidos a la capa superior. Las tramas que no cumplan con el formato AX25-- o no verifiquen el FCS, serán descartadas.

Solución

a)

```
// los datos se guardan en array de bits, y la función largo devuelve la cantidad de bits del
array.
int  eCU = 0; // cantidad de 1 consecutivos enviados

sendFlag(){
     putBit(0);
     putBit(1);
     putBit(1);
     putBit(1);
     putBit(1);
     putBit(0);
}

envioDatos(d){
    for (i=0;i < largo(d);i++){
        if ( d[i] == 1 ){
            eCU++;
        }else{
            eCU=0;
        }
        putBit(d[i]);
        if (eCU == 3){
            putBit(0);
            eCU=0;
    }

}

enviar(){
    while TRUE{
        getDatosTrama(a,i); // solicita trama a capa superior para envío
        sendFlag();
        eCU = 0;
        envioDatos(a);
        envioDatos(i);
         getFCS((a+i),fcs);
         envioDatos(fcs);
        sendFlag();
    }
}
```

b)



c)

```
// la función copy(dest,orig,cant) copia la cantidad cant de bits del array orig en el array
dest
getMessage(){
    estado= inicial;
    while TRUE{
        getBit(b);
        case estado of
        case inicial
            if ( b==0 ){ estado = F1}
        break;
        case F1
            if ( b==0 ){ estado = F1}else{estado=F2}
        break;
        case F2
            if ( b==0 ){ estado = F1}else{estado=F3}
        break;
        case F3
            if ( b==0 ){ estado = F1}else{estado=F4}
        break;
        case F4
            if ( b==0 ){ estado = F1}else{estado=F4}
        break;
        case F4
            if ( b==0 ){ estado = F1}else{estado=F5}
        break;
        case F5
            if ( b==0 ){ estado = FinFlag}else{estado=inicial}
        break;
        case FinFlag
            m[i] = b;
            i++;
            if ( b==1){estado=D1}
        break;
        case D1
            m[i] = b;
            i++;
            if ( b==0){estado=FinFlag}else{estado=D2}
        break;
        case D2
            m[i] = b;
            i++;
            if ( b==0){estado=FinFlag}else{estado=D3}
        break;
        case D3
            m[i] = b;
            i++;
            if ( b==0){estado=FinFlag}else{estado=D4}
        break;
        case D4
            m[i] = b;
            i++;
            if ( b==1){
                estado=inicial
            }else{
                i=i -5; // borro ultimos 5 bits
                estado=return
            }
        break;
        case return
            copy(msg,m[0],i); // cargo mensaje
            return msg;
        break;
    }
}


recibir(){
    while TRUE{
        m= getMessage();
```

```
        // determino largo de campo address
        if ( m[111]==1 ){
            fin=112;
        }else{ if (m[167] ==1){
            fin== 168;
        }else{
            fin=224
        }
        copy(a,m[0],fin); // paso campo recibido address
        copy(i,m[fin],largo(m)-fin-16); // cargo campo info
        copy(fcs,m[largo(m)-16],16); // cargo campo control
        if ( checkFCS(m,fcs){
                upDatosTrama(a,i);
        }
    }
}
```

Problema 2 (30 puntos)

Usted acaba de ser contratado en una empresa para desempeñar el cargo de administrador de red. La empresa dispone de 615 PCs conectados a una LAN 192.168.84.0/22, configurados de forma estática y, por razones históricas, el router posee la dirección LAN 192.168.84.254. Notar que la red 192.168.84.0/22 es parte de la red 192.168.0.0/16, según el RFC 1918.

Su nueva empresa, exitosa, adquiere otra de la competencia, por lo que se debe realizar una fusión. Hasta ahora, la política ha sido seguir agrandando la LAN, agregando hosts a la misma, conectando allí a todos los equipos. La empresa adquirida cuenta con 412 equipos y ocupa un local contiguo.

a) ¿cuál es la nueva dirección de red y máscara que permite conectar a todos los equipos en una única red? ¿qué debería hacer para aplicarla?
b) Describa dos problemas que se experimentan en este tipo redes, y que son argumentos suficientes para modificarla.

Mientras usted está preparando la información y el proyecto para presentar a gerencia, se producen dos nuevas adquisiciones simultáneas, de dos empresas chicas y usted decide cambiar la forma de incorporar estas redes rápidamente a su red corporativa.

c) Describa la forma en la que aplicaría la técnica de NAT para incorporar a estas dos redes a su red principal, cada una con 50 hosts, numeradas como 192.168.0.0/24.
d) Finalmente, usted puede llevar adelante su proyecto de renumeración de la red. Se pide que numere cada una de las redes a definir, sabiendo que los hosts se distribuyen de la siguiente forma: 130 administrativos, 64 directivos, 80 cajas, 260 marketing, 33 contaduría, 18 logística, 70 distribución, 125 diseño, 70 desarrollo, 270 ventas, 7 visitantes. Recuerde que si bien usted dispone de la red 192.168.0.0/16, se desea que la mayor parte de las redes se mantengan dentro del rango original 192.168.84.0/22 y se crezca a redes contiguas. La asignación de rangos innecesariamente grandes es considerado inadecuado. Asigne la dirección de los routers pasarela en la nueva jerarquía de red definida.
e) Ya que va a tener que visitar cada uno de los hosts, ¿qué protocolo, y por qué, habilitaría en los equipos para que de ahora en más ayude a simplificar la configuración?

a)

La nueva cantidad de *hosts* será 615+412=1027, además tenemos la dir. del router y las direcciones reservadas para la red y *broadcast*, un total de 1030 direcciones. Luego, se necesitan $\lceil \frac{\ln(1030)}{\ln(2)} \rceil$ bits de numeración, y por lo tanto el prefijo debe ser de 32-11=21 bits. La nueva dirección de red será 192.168.80.0/21 (máscara 255.255.248.0).
Para aplicar el cambio se deberá cambiar la máscara en el *router* y en cada uno de los *hosts* existentes, y se deberán definir direcciones en el rango para cada uno de los *hosts* nuevos.

b)

En una red moderna, generalmente los dispositivos de red se conectan a *switches*, y por lo tanto el dominio de colisiones no coincide con el dominio de *broadcast;* de no ser así, la cantidad de *hosts* provocaría que las colisiones hicieran casi imposible de utilizar la red. De todas formas, con *switches*, todos los mensajes de *broadcast* igualmente se difunden en toda la subred y afectan a todos los equipos, demandando tiempo de CPU para analizar paquetes que mayoritariamente serán descartados porque son dirigidos hacia otro dispositivo. Esta carga, normalmente atendida por el sistema operativo y no por la tarjeta de red en PCs de escritorio, interrumpe constantemente el procesamiento, afecta la localidad de la ejecución y quita capacidad de procesamiento "productiva" a los hosts.

Otro problema que presenta una red con tantos dispositivos está asociado a las tablas de ARP que deben mantener los *hosts*, así como los *mapeos* de direcciones MAC a puertos en los *switches*. Tablas tan "abultadas" representan *overhead* en las transmisiones.

Otro aspecto importante puede asociarse a la seguridad, pues, cualquier error en la configuración de la red, puede tener impacto en todos los equipos (p.e. un equipo que se configure equívocamente con la dirección del *router*). Cada vez que haya que resolver un problema, la causa puede provenir de la totalidad de la red, y no de sectores.

c)

Se puede colocar cada una de las redes compartiendo una dirección IP libre de la subred 192.168.80.0/21. Asignaría esa dirección IP al *router* NAT que conecta la red de la empresa

adquirida a la red existente, "ocultando" la numeración original. Se debe colocar un *router* NAT para cada red o un *router* que nos permita dos conexiones en NAT.

Lo siguiente no forma parte de la respuesta solicitada. Se incluye con el objetivo de comprender mejor el problema.

Para que esto sea posible, debemos asegurarnos que todos los protocolos utilizados funcionan adecuadamente atrás de un NAT, así como, que no deben generarse conexiones desde la red empresarial, 192.168.80.0/21 a ninguna de las redes 192.168.0.0/24.

d)

Nombremos las redes de la siguiente forma: a) administrativos, b) directivos, c) cajas, d) marketing, e) contaduría, f) logística, g) distribución, h) diseño, i) desarrollo, j) ventas, k) visitantes. La cantidad de bits requeridos para numerar cada red son: a) 8; b) 7; c) 7; d) 9; e) 6; f) 5; g) 7; h) 7; i) 7; j) 9; k)4. La totalidad de direcciones que podemos asignar con estas redes son: $2x2^9+2^8+5x2^7+2^6+2^5+2^4=2032$ hosts, que pueden ser representados por $\lceil \frac{\ln(2032)}{\ln(2)} \rceil$ =11 bits. Las 11 redes pueden ser numeradas de la siguiente forma con 11 bits:

	#	bit										
red	bits	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
d)	9	0	0									
j)	9	0	1									
a)	8	1	0	0								
b)	7	1	0	1	0							
c)	7	1	0	1	1							
g)	7	1	1	0	0							
h)	7	1	1	0	1							
i)	7	1	1	1	0							
e)	6	1	1	1	1	0						
f)	5	1	1	1	1	1	0					
k)	4	1	1	1	1	1	1	0				

Tomando los 21 bits del prefijo de la red 192.168.80.0/21 tenemos:

	#	bit																															Dirección de red
red	bits	**32**	**31**	**30**	**29**	**28**	**27**	**26**	**25**	**24**	**23**	**22**	**21**	**20**	**19**	**18**	**17**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
d)	9	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	0	0										192 168 80 0 / 23
j)	9	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	0	1										192 168 82 0 / 23
a)	8	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	0	0									192 168 84 0 / 24
b)	7	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	0	1	0								192 168 85 0 / 25
c)	7	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	0	1	1								192 168 85 128 / 25
g)	7	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	1	0	0								192 168 86 0 / 25
h)	7	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	1	0	1								192 168 86 128 / 25
i)	7	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	1	1	0								192 168 87 0 / 25
e)	6	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	1	1	1	0							192 168 87 128 / 26
f)	5	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	1	1	1	1	0						192 168 87 192 / 27
k)	4	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	1	1	1	1	1	0					192 168 87 224 / 28

Como podemos ver, la totalidad de las redes se asignaron dentro de la red 192.168.80.0/21 definida luego de la primer extensión.

Por simplicidad, definimos los routers como los hosts con número 1 (uno) de cada red. Por consiguiente sus direcciones son:

router de la red	Dirección de red			
d)	192	168	80	1
j)	192	168	82	1
a)	192	168	84	1
b)	192	168	85	1
c)	192	168	85	129
g)	192	168	86	1
h)	192	168	86	129
i)	192	168	87	1
e)	192	168	87	129
f)	192	168	87	193
k)	192	168	87	225

e)
DHCP, Dynamic Host Configuration Protocol. Luego de habilitado nos permite hacer rediseños a la red, y en vez de necesitar recorrer cada uno de los *hosts* para realizar cambios en la configuración, solamente requerimos hacer los cambios en el servidor de DHCP. Luego, cuando los *leases* expiren y el equipo obtenga una nueva configuración, tendrá la nueva dirección de red que deseemos. De esta forma, las tareas de administración y gestión de la red se ven simplificadas.