SESIÓN DE LABORATORIO 10
DHCP y seguridad en capa 3 con ACL

Objetivos

- Configurar el servicio DHCP en un router
- Configurar el servicio DNS en un servidor.
- Implementar mecanismos de seguridad en el nivel de red.
- Distinguir entre listas de control de acceso estándar y extendidas.
- Implementar políticas de filtrado de tráfico mediante listas de control de acceso estándar y extendidas.
- Configurar el acceso remoto a los routers por medio de una lista de control de acceso.

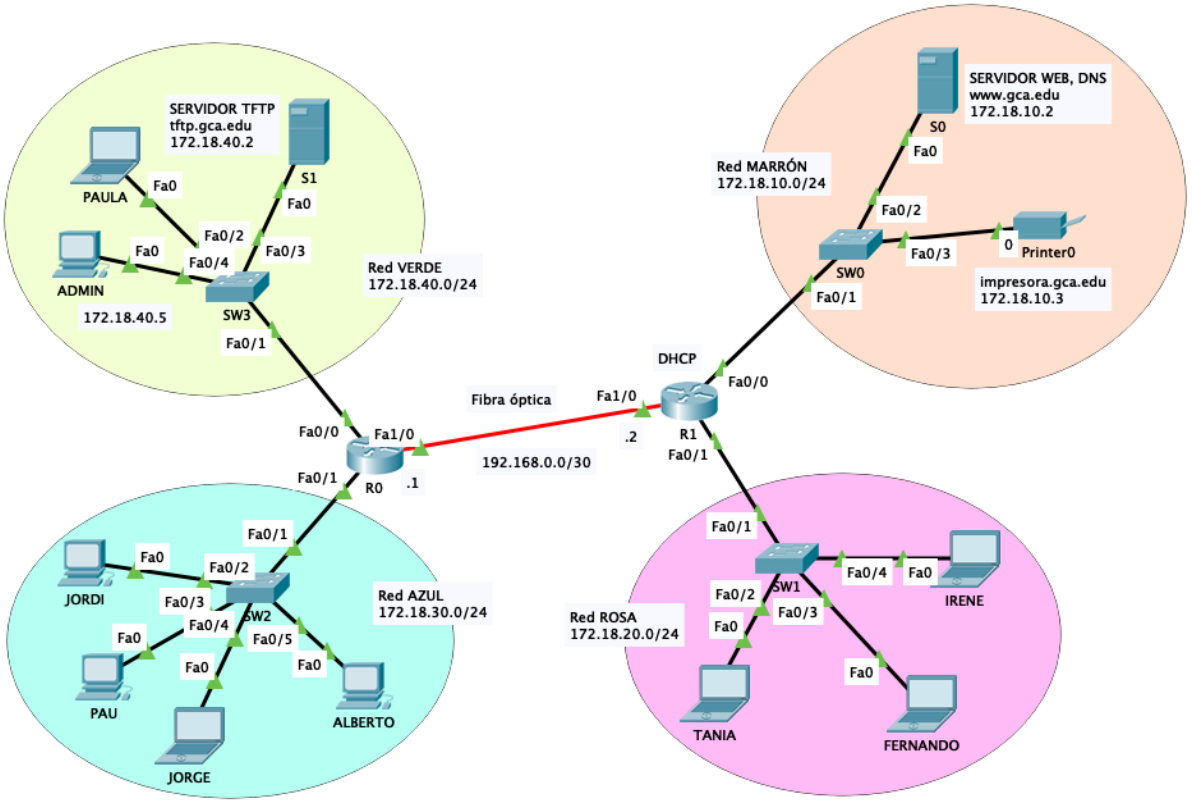
Desarrollo

En esta sesión aprenderemos a configurar servicios como DHCP en un router o DNS en un servidor, así como a utilizar listas de control de acceso (ACL, *Access Control Lists*) como método para el filtrado de tráfico en capa 3 en una red de interconexión. Para ello implementaremos una red corporativa mediante switches Cisco Catalyst 2960 y routers Cisco 2811. Las siguientes imágenes corresponden, respectivamente, a estos dos tipos de dispositivos.

Vamos a considerar la topología de interconexión de una mediana empresa reflejada en la siguiente figura. El ID de red de la empresa es 172.16.0.0/16, es decir, tiene asignada una dirección privada de clase B. El proceso de subnetting ha considerado un total de cuatro subredes:

- 172.18.10.0/24 (red marrón)
- 172.18.20.0/24 (red rosa)
- 172.18.30.0/24 (red azul)
- 172.18.40.0/24 (red verde)

Cada una de estas subredes emplea un switch Catalyst 2960 para conectar los distintos hosts entre sí. Los dos routers 2811 de la topología, R0 y R1, están interconectados mediante la red 192.168.0.0/30 a través de un enlace de fibra óptica. Dado que este modelo de router no tiene conexión óptica hay que instalar una: por ejemplo, se puede seleccionar la tarjeta NM-1FE-FX e incorporarla al router. Recuerda que es necesario apagar el router antes de instalarla.



El servidor S0, cuya dirección IP es estática: 172.18.10.2 (red marrón) tiene activados dos servicios:

1. Aloja la página web de la empresa, www.gca.edu.
2. Actúa como servidor de nombres de dominio (DNS, Domain Name Server).

Por su parte, el servidor S1 de la red verde tiene activado el servicio TFTP para almacenar una copia de seguridad de los ficheros de configuración `startup-config` de ambos routers. Su dirección IP se configura igualmente de manera estática: 172.18.40.2. Finalmente, la dirección IP de la impresora de la red marrón también se va a configurar de forma estática: 172.18.10.3, de igual forma que el ordenador de la administradora de red, ADMIN, con dirección IP 172.18.40.5.

Recuérdese que en los casos en que la configuración IP del host se hace de forma estática es necesario especificar cuatro parámetros:

1. La propia dirección IP
2. La máscara de red
3. La dirección IP de la puerta de enlace (gateway, imprescindible si se quiere establecer comunicación con otras redes).
4. La dirección IP del servidor de nombres de dominio (opcional pero muy recomendable en la práctica).

De los cuatro parámetros solamente los dos primeros son necesarios. Los otros dos son opcionales: el primero sirve para conectar con otras redes y el segundo para traducir nombres a direcciones IP.

Diseño de la topología básica

Configuración de los routers y switches

Para implementar la topología de interconexión seguiremos las siguientes pautas. En primer lugar dispondremos los dos routers, instalaremos una tarjeta NM-1FE-FX en cada uno de ellos y procederemos a interconectarlos mediante un enlace de fibra óptica. Para instalar la tarjeta es necesario apagar previamente el router, tal como se haría en la realidad. En este momento es recomendable también cambiar el nombre establecido por defecto de cada router mediante el comando `hostname` (R0 y R1).

A continuación dispondremos los cuatro switches, los conectaremos a los routers mediante cables rectos y les asignaremos un nombre a cada uno de ellos mediante el comando `hostname` (SW0, SW1, SW2 y SW3). Una vez conectados los switches procederemos a disponer el resto de hosts: los dos servidores, S0 y S1, la impresora y los ordenadores personales.

Una vez tenemos dispuestos todos los elementos de la red (routers, switches, hosts y enlaces) procederemos a la configuración propiamente dicha de la red de interconexión. Comenzaremos por la conexión entre los dos routers: hay que asignar la dirección IP de las interfaces de fibra óptica (Fa1/0) y después habilitarlas. Veamos cómo hacer todo esto en el router R0:

```
Router#configure terminal
Router(config)#hostname R0
R0(config)#interface fastEthernet 1/0
R0(config-if)#ip address 192.168.0.1 255.255.255.252
R0(config-if)#no shutdown
R0(config-if)#exit
```

Es bastante común usar una máscara de red /30 para los enlaces entre routers porque de esta manera se ajusta perfectamente el número de direcciones IP: los dos bits de hosts se reparten entre los valores 00 (ID de red), 01 y 10 (direcciones IP de los extremos) y 11 (broadcast). Es decir, 192.168.0.0 para el ID de red, 192.168.0.1 y 192.168.0.2 como direcciones de los routers, y finalmente 192.168.0.3 para la dirección de broadcast.

Después pasaremos a configurar las dos interfaces de cada router correspondientes al resto de redes (Fa0/0 y Fa0/1). Para estas interfaces hay que asignar la dirección más baja del rango (.1), dirección que corresponderá a la puerta de enlace de cada subred. Por ejemplo, la dirección de la interfaz Fa0/0 de R0 es 172.18.40.1 y la dirección de su interfaz Fa0/1 es 172.18.30.1. Por ejemplo, para Fa0/1 en R0 tendremos:

```
R0(config)#interface fastEthernet 0/1
R0(config-if)#ip address 172.18.30.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#exit
```

En estos momentos los routers son capaces de actualizar sus tablas de encaminamiento con las redes que tienen directamente conectadas. Sin embargo, hará falta incorporar a estas tablas la información de enrutamiento necesaria para conectar entre sí las redes verde y azul con las redes marrón y rosa. Esto se puede hacer mediante los protocolos de enrutamiento dinámico como OSPF o RIP-2, por ejemplo, que sería la opción más recomendable, o bien lo podemos hacer, en este contexto específico, con una ruta estática por defecto (*gateway of last resort*):

```
R0#configure terminal
R0(config)#ip route 0.0.0.0 0.0.0.0 Fa1/0
```

Esta ruta se representa con el código `S*`. La letra S indica que se trata de una ruta estática (*static*), mientras que el asterisco la identifica como ruta principal. Ello es debido a que podrían configurarse varias rutas por defecto aunque solamente se hará uso de la principal. Cuando el router no consigue encaminar un paquete hacia sus redes conocidas entonces lo envía a través de la interfaz Fa1/0. En el caso del router R1 la configuración de esta ruta por defecto se hace del mismo modo:

```
R1#configure terminal
R1(config)#ip route 0.0.0.0 0.0.0.0 Fa1/0
```

Recuerda que esta configuración de rutas estáticas se lleva a cabo de forma sencilla pero a su vez resulta un método muy poco escalable. En redes de gran tamaño, como hemos dicho, se emplean los protocolos de enrutamiento dinámico, los cuales se encargan de aprender y completar las tablas de rutas de los routers de forma automática.

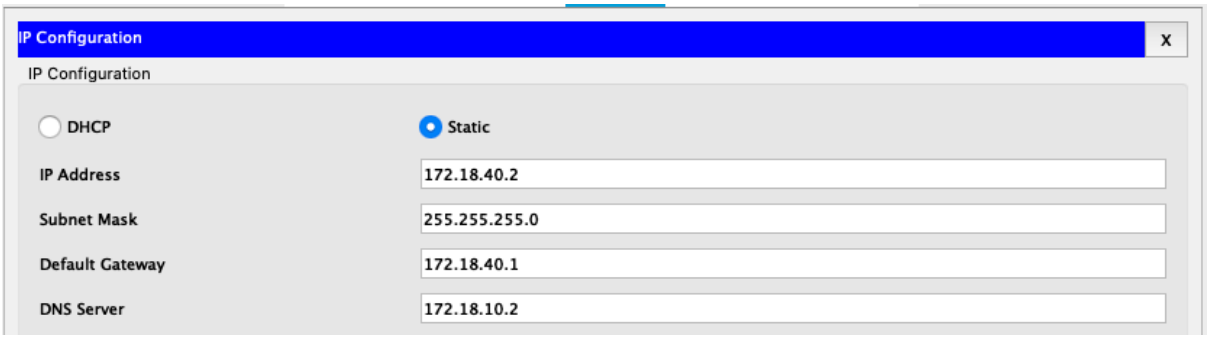
Después de configurar el encaminamiento en los routers hay que comprobar que las tablas de encaminamiento son correctas. Por ejemplo, en el caso del router R1 tendremos:

```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.18.0.0/24 is subnetted, 2 subnets
C       172.18.10.0 is directly connected, FastEthernet0/0
C       172.18.20.0 is directly connected, FastEthernet0/1
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, FastEthernet1/0
S*   0.0.0.0/0 is directly connected, FastEthernet1/0
```

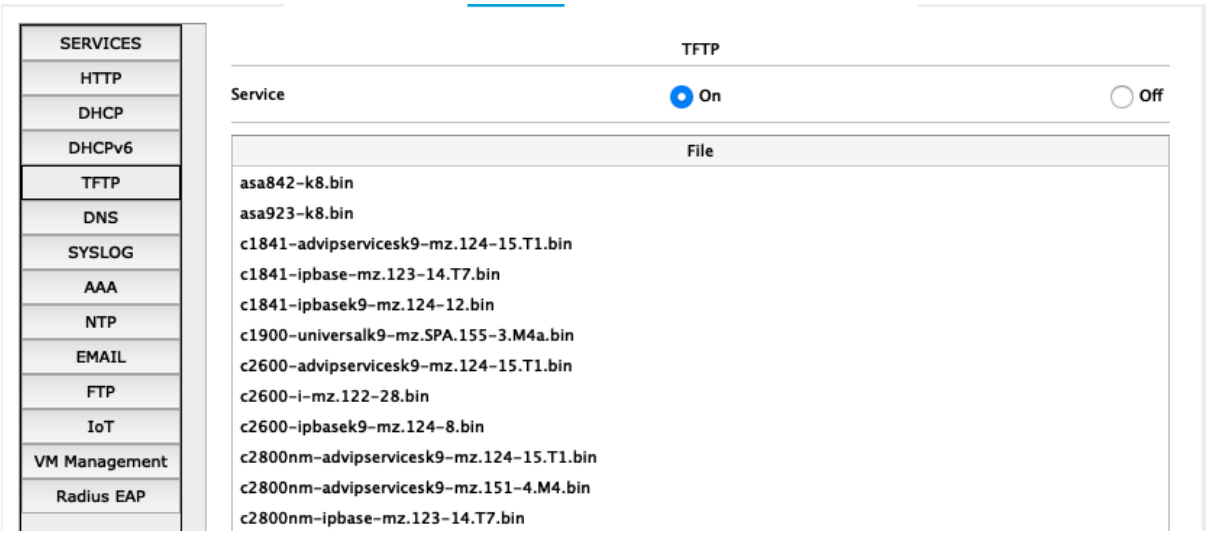
Configuración de direcciones IP estáticas y servicios web y DNS

En este momento ya tenemos los routers dispuestos para encaminar paquetes entre las diferentes subredes. Ahora es el momento de configurar los hosts que tienen direcciones IP estáticas y que no serán asignadas a través del protocolo DHCP. En particular, configuraremos los servidores S0 y S1, la impresora y también el ordenador personal ADMIN. En todos los casos hay que indicar cuatro parámetros: dirección IP, máscara de red, dirección IP de la puerta de enlace y dirección IP del servidor de nombres de dominio.

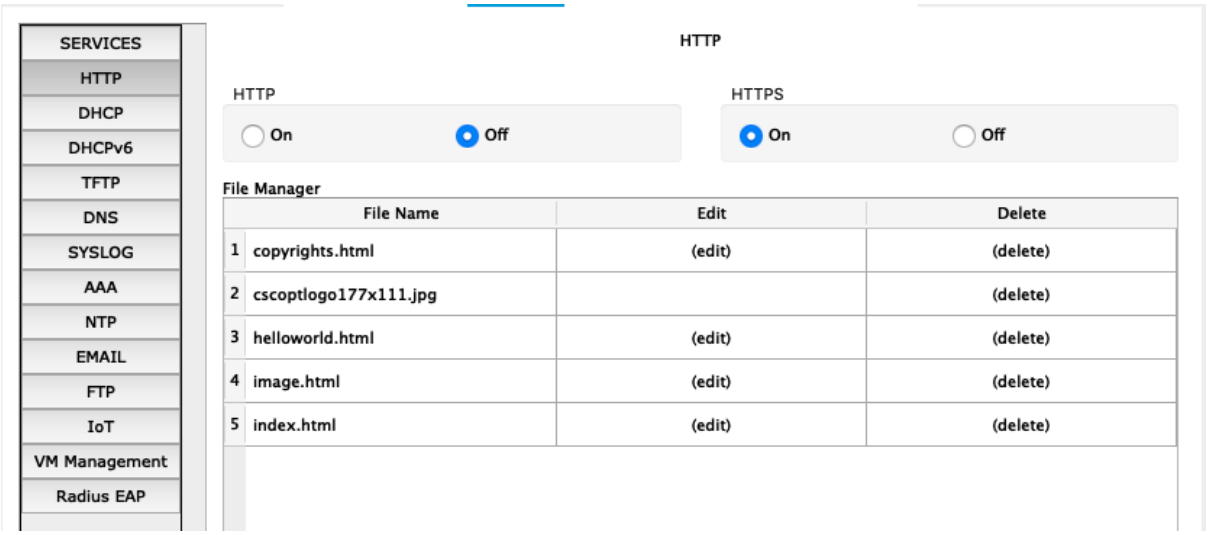
Por ejemplo, la configuración IP del servidor S1 será:



Una vez establecida la configuración completa de la capa de red en estos hosts hay que activar los servicios en los servidores. En el caso del servidor S1 hay que cerciorarse de que el servicio TFTP está activo (es la opción por defecto):

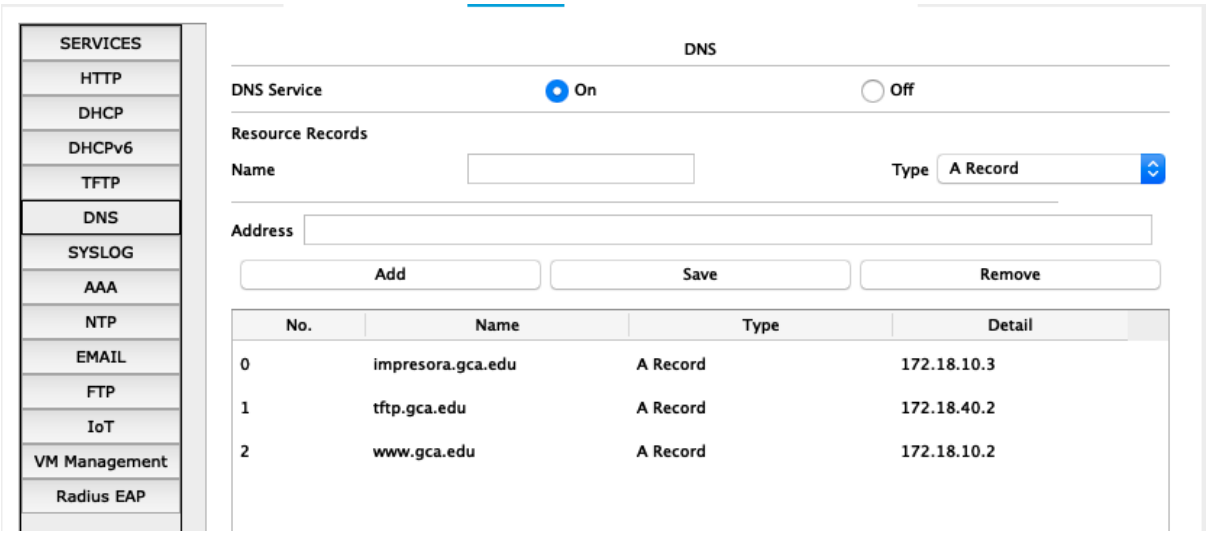


Por otro lado, en el caso del servidor S0 es necesario comprobar que el servicio web también está activo (opción por defecto). De los dos protocolos posibles, es recomendable desactivar el servicio HTTP y dejar únicamente el servicio HTTPS, que es una opción mucho más segura:



Como se puede ver en la imagen anterior, el simulador también nos permite, a través del administrador de archivos (File Manager), editar el contenido de las páginas web almacenadas en el servidor y, si es necesario, adaptarlas a nuestras necesidades.

En el caso del servidor S0 hay que activar el servicio DNS (está desactivado por defecto) e incluir los nombres de dominio que se van a emplear en la corporación (`www.gca.edu`, `impresora.gca.edu` y `tftp.gca.edu`):



Finalmente, también es interesante configurar en los routers la dirección del servidor de nombres de dominio, ya que desde su CLI es posible hacer uso de un comando `ping` más completo que el disponible en los hosts. Para ello hay que ejecutar el comando `ip name-server` en el modo de configuración global. De este modo, se puede usar la dirección IP del host o bien su nombre de dominio:

```
R1#configure terminal
R1(config)#ip name-server 172.18.10.2
R1(config)#exit
R1#ping impresora.gca.edu

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.10.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Comprobación de la conectividad

En este momento ya se puede comprobar por medio del comando `ping` que hay conectividad entre los hosts que tienen asignada la configuración IP de forma estática. Uno de los errores más comunes que impiden la conectividad suele estar en la especificación de la puerta de enlace en el host.

Router como servidor DHCP

Un aspecto importante en cualquier red es la manera en la que los hosts obtienen la configuración para acceder a ella. Esta configuración, como hemos visto ya, está formada por una dirección IP, la máscara de red, la puerta de enlace y el o los servidores DNS, estos últimos opcionales pero muy recomendables. En la práctica la configuración manual es difícil de administrar y resulta poco escalable, y es preferible que estos datos de conexión se proporcionen de manera automática mediante el protocolo DHCP (*Dynamic Host Configuration Protocol*). El protocolo DHCP es una opción ideal debido a su facilidad de

administración y servicio centralizado, y se emplea incluso en las redes domésticas más pequeñas.

Normalmente las compañías instalan servidores DHCP dedicados que operan con sistemas operativos como Windows Server o Linux Ubuntu. Sin embargo, los routers Cisco también pueden ser configurados para ofrecer este servicio. Nosotros vamos a configurar el router R1 para que actúe como servidor DHCP de todos los hosts de la topología.

En total el servidor DHCP debe proporcionar la configuración IP a hosts de cuatro redes distintas. En el caso de las redes marrón y verde se van a reservar las 10 primeras direcciones del rango para direcciones estáticas; en las otras dos se podrán asignar direcciones de todo el rango.

Veamos cómo se puede configurar el servicio DHCP para la red marrón:

```
R1#configure terminal
R1(config)#ip dhcp excluded-address 172.18.10.1 172.18.10.10
R1(config)#ip dhcp pool redMarron
R1(config-dhcp)#network 172.18.10.0 255.255.255.0
R1(config-dhcp)#default-router 172.18.10.1
R1(config-dhcp)#dns-server 172.18.10.2
R1(config-dhcp)#lease 1 0 0 (arrendamiento por 24 horas - no funciona)
```

Nótese que, en primer lugar, se especifican las direcciones excluidas del arrendamiento desde el modo de configuración global. Después se crea un pool DHCP denominado `redMarron` que solo es un identificador a nivel local. Una vez creado se entra en un nuevo modo de configuración desde el cual se procede a configurar el resto de parámetros: el ID de la red y su máscara, gracias a los cuales el router calculará de forma automática las direcciones que asignará a los clientes que lo soliciten, la dirección de la puerta de enlace y el o los servidores de nombres de dominio (solamente se ha especificado uno).

El último comando, `lease hours min sec`, establece la vigencia temporal del arrendamiento al host de la configuración IP, pero no está implementado en el simulador, por lo que no hay que emplearlo en esta sesión práctica.

Para la red de color rosa la configuración del servicio DHCP será muy similar al anterior, excepto que en esta red se puede asignar cualquier dirección del rango:

```
R1#configure terminal
R1(config)#ip dhcp pool redRosa
R1(config-dhcp)#network 172.18.20.0 255.255.255.0
R1(config-dhcp)#default-router 172.18.20.1
R1(config-dhcp)#dns-server 172.18.10.2
```

En este momento los hosts de las redes marrón y rosa ya pueden configurarse para obtener su configuración por medio de DHCP, dado que se trata de dos redes conectadas directamente al router R1.

Falta por especificar el servicio DHCP para las redes verde y azul, que no están conectadas directamente al router R1. La configuración se hace de forma similar a los dos casos anteriores:

```
R1#configure terminal
R1(config)#ip dhcp excluded-address 172.18.40.1 172.18.40.10
R1(config)#ip dhcp pool redVerde
R1(config-dhcp)#network 172.18.40.0 255.255.255.0
R1(config-dhcp)#default-router 172.18.40.1
R1(config-dhcp)#dns-server 172.18.10.2
R1(config-dhcp)#exit
R1(config)#ip dhcp pool redAzul
R1(config-dhcp)#network 172.18.30.0 255.255.255.0
R1(config-dhcp)#default-router 172.18.30.1
R1(config-dhcp)#dns-server 172.18.10.2
```

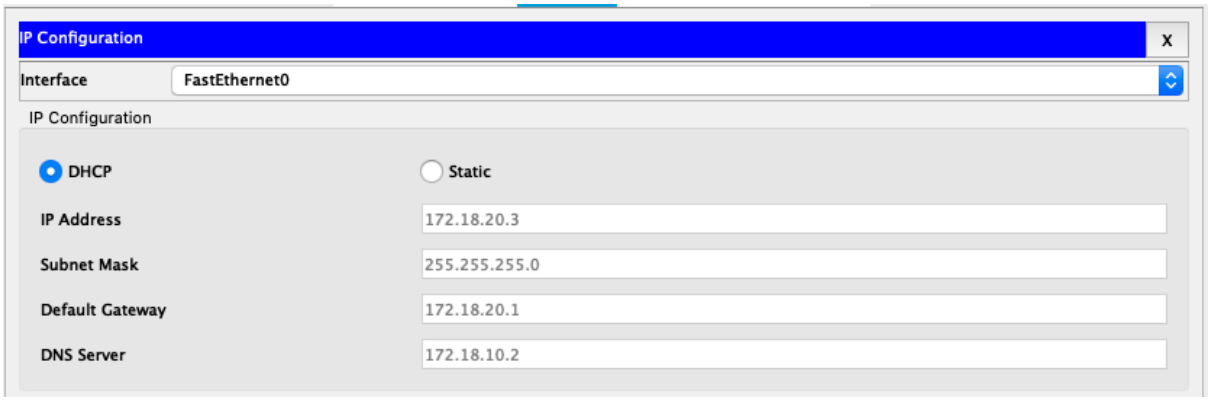
Ahora bien, con esta configuración los hosts de estas redes no pueden obtener su configuración IP porque el servicio DHCP está ubicado en una subred remota. Esto es así porque algunos de los mensajes empleados por el protocolo DHCP (en concreto, DHCPDISCOVER Y DHCPREQUEST) son enviados mediante broadcast y sabemos que los routers no reenvían este tipo de mensajes a través de sus interfaces.

Para resolver este problema se usa la técnica *DHCP relay* en el router R0: los mensajes DHCP de tipo broadcast que reciba deberá redirigirlas al router R1 para que las resuelva. Esto se hace en cada una de las interfaces de R0 donde se recibe el mensaje de broadcast indicando la dirección IP del servidor DHCP (router R0):

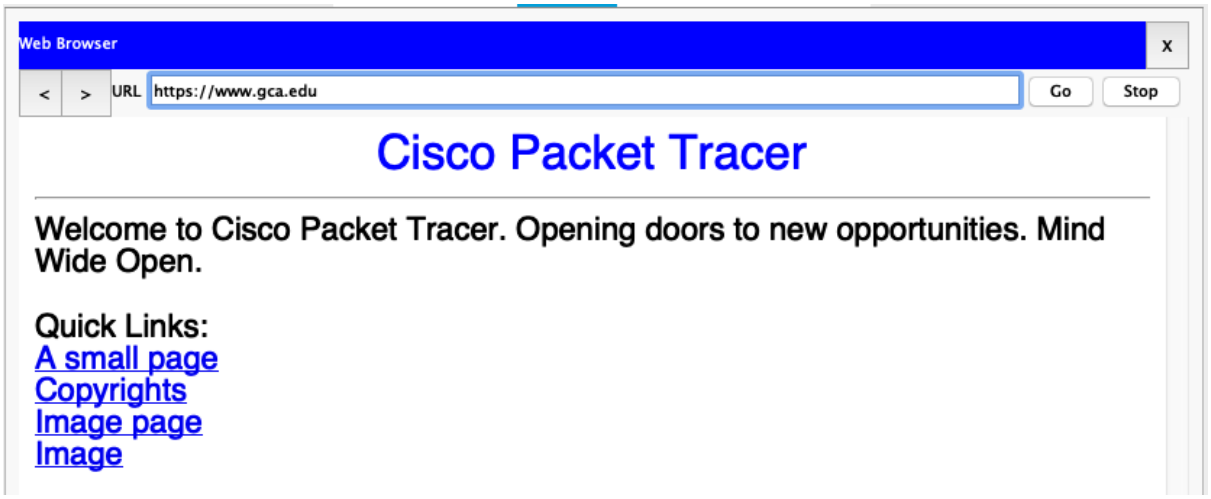
```
R0#configure terminal
R0(config)#interface fastEthernet 0/0
R0(config-if)#ip helper-address 192.168.0.2
R0(config-if)#exit
R0(config)#interface fastEthernet 0/1
R0(config-if)#ip helper-address 192.168.0.2
R0(config-if)#exit
```

Comprobación de la conectividad y acceso a servicios

En estos momentos hay que configurar el resto de hosts para que reciban su configuración IP mediante el protocolo DHCP. Después de observar que la información obtenida por cada host es correcta es necesario comprobar la conectividad de toda la red mediante el comando `ping`. Por ejemplo, los cuatro parámetros de la configuración IP del host FERNANDO obtenidos por DHCP son los siguientes:



También hay que comprobar que se puede hacer uso de los nombres de dominio tanto en los comandos `ping` como en el acceso al servidor web. Por ejemplo, desde el ordenador PAULA se accede satisfactoriamente a la página `www.gca.edu` a través del protocolo HTTPS (no se puede con HTTP):



El comando traceroute

El otro comando, aparte de `ping`, usado para probar la conectividad de una red es `traceroute`. Este comando resulta de gran ayuda para la resolución de incidencias. Mientras que el primero realiza un testeo de extremo a extremo, `traceroute` se encarga de mostrar un listado con el número de saltos que da un paquete desde el origen hasta el destino.

Su modo de operación se basa en el campo TTL (Time To Live) de los paquetes IP y su manejo por parte de los routers. Cada vez que el paquete llega a un router este valor del campo TTL se decrementa; si el resultado es 0 se producen dos acciones: primero, el paquete se descarta, y segundo, se informa al origen de la comunicación que se ha excedido el número de saltos permitido mediante un mensaje ICMP TTL Exceeded.

Bien, pues `traceroute` basa su funcionamiento en este hecho: va enviando, sucesivamente, paquetes con TTL igual a 1, 2, 3, etcétera, hasta que el último llegue a su destino. Cada vez que se recibe un mensaje ICMP TTL Exceeded se muestra en pantalla como uno de los saltos.

```
R0#traceroute www.gca.edu

Type escape sequence to abort.
Tracing the route to 172.18.10.2

 1   192.168.0.2     0 msec    0 msec    2 msec
 2   172.18.10.2     0 msec    0 msec    0 msec
```

Como se indica en el resultado anterior, la distancia entre el router R0 y el servidor web www.gca.edu es de dos saltos: el que va de R0 a R1 (primera línea) y el que va de R1 al propio servidor (segunda línea). Es importante fijarse en las direcciones IP que identifican cada uno de los saltos: en el caso de los routers, la dirección IP corresponde a la interfaz que recibe el paquete.

Copia de la configuración por TFTP

Una vez comprobada la conectividad de la red hay que copiar, en cada router, el fichero `running-config` (alojado en la memoria RAM) en `startup-config` (alojado en la memoria NVRAM) para evitar así la pérdida de la configuración y asegurarnos de que el router, en caso de apagarse, vuelve a arrancar con la configuración apropiada:

```
R0#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R0#
```

Así mismo, conviene tener una copia de respaldo de este fichero de configuración en el servidor S1 donde hemos activado el servicio TFTP. Por ejemplo, en el caso del router R0 podemos hacer:

```
R0#copy startup-config tftp
Address or name of remote host []? tftp.gca.edu
Destination filename [R0-confg]?

Writing startup-config...Translating "tftp.gca.edu"...!!
[OK - 777 bytes]

777 bytes copied in 0 secs
R0#
```

ACL estándar numerada

Una lista ACL estándar es la solución de seguridad de capa 3 más básica disponible en IOS, ya que basa su filtrado únicamente en el origen de la comunicación, ya sea una dirección IP de un host específico o un ID de red.

Una lista de control de acceso se compone de una serie de sentencias o condiciones que el router agrega a medida que son definidas. Según el orden en que han sido configuradas, la dirección de cada paquete IP es inspeccionada y cotejada con la lista de control de acceso hasta que se produzca la primera coincidencia, en cuyo caso se ejecutará la acción configurada en dicha sentencia, que será denegar o permitir la comunicación.

Un detalle de suma importancia a tener en cuenta es que todas las ACL definen, de manera automática, una denegación implícita (`deny any`) al final de la lista, de forma tal que, si un paquete no satisface ninguno de los filtros configurados, será descartado automáticamente.

La denegación implícita puede evitarse añadiendo de forma manual un comando `permit any` como última entrada de la ACL, aunque por motivos de seguridad resulta una práctica poco o nada recomendable.

Para definir una ACL estándar hay que emplear el comando `access-list` desde el modo de configuración global, dotándolo de un identificador numérico entre 1 y 99, o bien entre 1300 y 1999, que identifica la ACL, seguida de `permit` o `deny`, y a continuación la dirección IP del host o bien el ID de la red afectada por el filtro.

Para configurar una ACL estándar hay que identificar en qué router, interfaz y dirección (`in`, `out`) será aplicada. Las ACL estándar deben configurarse lo más cercanamente posible al **destino** a fin de evitar bloqueos indeseados. Veamos un ejemplo sencillo:

```
Router#configure terminal
Router(config)#access-list 1 permit host 192.168.12.78
Router(config)#access-list 1 deny 192.168.12.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
Router(config)#exit
```

La lista de acceso definida se aplica en la interfaz Fa0/1 del router una vez que el paquete ha sido encaminado. Esta lista permitiría el tráfico del host con IP 192.168.12.78 pero a continuación se bloquea el tráfico de cualquier host perteneciente a la red 192.168.12.0/24. La condición final permite que el resto de paquetes con un origen distinto no sean bloqueados en la interfaz.

Nótese el efecto de la máscara wildcard 0.0.0.255, que representa el valor inverso a la máscara de red. En realidad, los bits de la dirección IP de origen del paquete se analizan de la siguiente manera: los bits a 0 de la máscara se comparan con el ID incluido en la sentencia y en caso de coincidencia se aplica la acción indicada; los bits a 1 de la máscara no son analizados.

Una vez concluida la configuración se puede verificar por medio del comando siguiente:

```
Router#show ip access-lists
Standard IP access list 1
    permit host 192.168.12.78
    deny 192.168.12.0 0.0.0.255
    permit any
```

Aplicación de la ACL estándar número 10

Se pide diseñar las ACL necesarias para impedir cualquier tipo de tráfico entre las redes Azul y Rosa. Hay que tener en cuenta que el tráfico que se pretende bloquear afecta a las dos direcciones posibles entre las dos redes.

En este caso se deben diseñar dos ACL casi idénticas, una por cada router, en la interfaz que conecta a la red para la que vamos a filtrar el tráfico ya que se recomienda que las ACL estándar se sitúen lo más cerca posible del destino. El número de ACL no tiene por qué ser el mismo en ambos routers. El sentido en que se aplica cada ACL es `out`.

```
R1(config)#access-list 10 deny 172.18.30.0 0.0.0.255
R1(config)#access-list 10 permit any
R1(config)#interface fa0/1
R1(config-if)#ip access-group 10 out
R1(config-if)#exit
```

```
R0(config)#access-list 10 deny 172.18.20.0 0.0.0.255
R0(config)#access-list 10 permit any
R0(config)#interface fa0/1
R0(config-if)#ip access-group 10 out
R0(config-if)#exit
```

Después de definir las ACL y aplicarlas en las interfaces correspondientes es aconsejable comprobar tanto el filtrado del tráfico llevado a cabo por las listas de acceso y también que el resto del tráfico que no viaja entre ambas redes se permite.

ACL extendida numerada

Las ACL extendidas son un poco más complejas que las estándar porque nos permiten ajustar el filtrado de tráfico con mayor precisión. En particular, una ACL extendida permite identificar tanto la dirección IP de origen como la IP de destino, así como el protocolo o

puerto utilizado durante la comunicación. Los protocolos más comunes son IP, TCP, UDP o ICMP. El ID de una ACL extendida está comprendida de 100 a 199 o bien entre 2000 y 2699.

A pesar de estas diferencias, las similitudes son muy grandes. Ambas se aplican a nivel de interfaz y en una de las dos direcciones posibles, y también definen un listado de filtros a medida que son configurados para, a posteriori, analizar los paquetes según un orden concreto; cuando haya una coincidencia se aplica la acción determinada en la misma. Así mismo, los dos tipos de listas incorporan un `deny any` final de forma implícita.

Para configurar una ACL extendida hay que identificar en qué router, interfaz y dirección (`in`, `out`) será aplicada. Las ACL extendidas, a diferencia de lo que ocurría con las ACL estándar, deben ser configuradas lo más cerca posible al **origen** a fin de evitar que circulen por la red paquetes que posteriormente serán descartados. Veamos un ejemplo sencillo que intenta controlar el tráfico recibido por un servidor web (el servicio HTTP usa TCP con número de puerto 80):

```
Router#configure terminal
Router(config)#access-list 100 deny tcp 192.168.20.0 0.0.0.255 host 10.10.1.1 eq 80
Router(config)#access-list 100 permit tcp any any eq 80
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#exit
```

El servidor web tiene dirección IP 10.10.1.1. En la lista de acceso anterior se permite el acceso al servicio web a cualquier host que no pertenezca a la red 192.168.20.0/24. Cualquier otro tipo de tráfico, debido al `deny any` implícito del final de la lista, será descartado.

Aplicación de la ACL extendida número 110

Se quiere impedir que los hosts de la red Rosa accedan al servidor web. El número de puerto asociado al servicio HTTPS es el 443. Cualquier otro tráfico deberá permitirse.

```
R1#configure terminal
R1(config)#access-list 110 deny tcp 172.18.20.0 0.0.0.255 host 172.18.10.2 eq 443
R1(config)#access-list 110 permit ip any any
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip access-group 110 out
R1(config-if)#exit
R1(config)#exit
```

Después de aplicar la lista anterior es recomendable comprobar que desde la red Rosa se puede hacer un ping al servidor web puesto que se usa el protocolo ICMP. También es

importante comprobar que se puede acceder al servicio DNS del servidor, dado que este servicio hace uso del protocolo TCP pero en el puerto 53.

Aplicación de la ACL extendida número 120

Se pretende que ningún host de la red verde reciba tráfico ICMP.

```
R0#configure terminal
R0(config)#access-list 120 deny icmp any any
R0(config)#access-list 120 permit ip any any
R0(config)#interface fastEthernet 0/0
R0(config-if)#ip access-group 120 out
R0(config-if)#exit
R0(config)#exit
```

Con esta lista de control de acceso evitamos que cualquier host externo a la red verde pueda hacer un `ping` a uno de sus hosts. La lista se sitúa en la interfaz Fa0/0 del router R0 ya que es el lugar más cercano al destino posible. La segunda condición se establece para evitar la denegación implícita presente al final de toda lista de control de acceso.