Capítulo 6

LISTAS DE ACCESO IP ESTÁNDAR

Una lista de control de acceso (Access Control List o ACL) es el método utilizado para comparar patrones de información de los diferentes protocolos de la arquitectura TCP/IP. Hay varias situaciones en la que se puede necesitar realizar esta comparación, por ejemplo, para limitar el acceso a una subred por razones de seguridad o para limitar el tamaño de las tablas de enrutamiento de un encaminador por razones de desempeño. Las listas de control de acceso se pueden aplicar de diferentes maneras. Cuando una ACL se aplica a una interfaz, dicha ACL puede diseñarse para que se acepten o rechacen datagramas IP entrantes o salientes de la misma, la aceptación o rechazo de los paquetes se puede basar en los diferentes campos de los protocolos TCP/IP. Cuando una ACL se aplica a un protocolo de enrutamiento (como RIP u OSPF), ejecutándose en un encaminador, ésta puede evitar que el encaminador envíe información de una ruta en particular. El propósito de este capítulo es presentar la lista de control de acceso IP estándar, que es una de las formas más básica de las ACL.

Objetivo

Al finalizar esta unidad, el estudiante estará en capacidad de:

- Conocer los diferentes tipos de listas de acceso y el rango de números asignados a estas.
- Entender el procesamiento “top-down” de las listas de acceso.
- Conocer qué es una negación implícita.
- Usar los comandos de las listas de acceso.
- Usar la máscara comodín (wildcard mask) en las listas de acceso.
- Crear una lista de acceso IP estándar numerada.

- Configurar filtros de tráfico utilizando listas de acceso IP estándar numeradas.
- Activar una lista de acceso sobre una interfaz.
- Verificar la operación de las listas de acceso.

Procedimiento

Controlando el acceso IP

Las listas de control de acceso son una de las características más versátiles de los encaminadores en general, las listas de acceso pueden realizar, entre otras, las siguientes funciones:

Filtrar tráfico

- Filtrar paquetes que intentan pasar a través del encaminador.
- Restringir acceso VTY (telnet) al encaminador.
- Filtrar información de enrutamiento intercambiada por los encaminadores.
- Activar llamadas telefónicas con DDR (Dial-on-demand routing).
- Priorizar tráfico de la red de área amplia con *priotity queuing* y *custom queuing*.

Aunque la anterior lista de funciones puede seguir creciendo, el alcance de este capítulo se concentra en el primer ítem (el filtrado del tráfico TCP/IP que atraviesa un encaminador).

En términos generales, una lista de acceso consiste en un conjunto de comandos de filtro que se agrupan bajo un mismo número (el número escogido para la lista de acceso). Estos comandos definen a cuáles paquetes se les permite o se les niega el paso. Las listas de acceso se crean bajo el modo de configuración global. Para activar la lista de acceso, la cual contiene los comandos de filtrado, ésta se debe aplicar sobre un objeto físico o lógico. Por ejemplo, si se desea filtrar el tráfico que atraviesa a un encaminador, se debe aplicar la lista a una interfaz física del mismo.

Cuando se aplica una lista de acceso a una interfaz, hay dos opciones posibles:

Inbound (in): prueba solamente el tráfico que trata de entrar por la interfaz en cuestión. Con esta opción, los paquetes que entran por una interfaz son comparados inmediatamente con las sentencias de la lista antes de ser conmutados a una interfaz de salida (antes de utilizar la tabla de enrutamiento).

Outbound (out): prueba solamente el tráfico que trata de salir por la interfaz en cuestión. Con esta opción, a los paquetes que hayan sido admitidos por el encaminador (mediante otra interfaz) y conmutados hacia la interfaz de salida se les aplicará la lista de acceso antes de permitirles dejar la interfaz de salida (después de haber utilizado la tabla de enrutamiento).

Específicamente, las listas de acceso IP pueden ser usadas para controlar el flujo de datagramas IP a través de las interfaces del encaminador. Después de aplicar una ACL –en el sentido de entrada o de salida de la interfaz–, ésta puede permitir o negar el paso de los datagramas IP que entran o que salen de la interfaz, es decir, antes o después de ejecutarse el procesamiento de decisión de enrutamiento. Una lista de acceso es una colección secuencial de condiciones que se aplican a las direcciones IP de un datagrama IP o a los protocolos de capa superior a IP, esto se hace con el propósito de permitir o negar el flujo de tráfico de acuerdo a los patrones que se definan en la lista.

La Tabla 6.1 indica los diferentes tipos de listas de acceso numeradas y los correspondientes números que pueden ser utilizados como identificadores de la lista.

Tabla 6.1. Tipos de listas de control de acceso numeradas, identificadas por un número

Tipo de lista de acceso	Rango numérico
ACL IP estándar	1-99
ACL IP extendida	100-199
ACL Ethernet Type Code	200-299
ACL Decnet estándar y extendida	300-399
ACL XNS estándar	400-499
ACL XNS extendida	500-599
ACL Appletalk estándar y extendida	600-699
ACL 48 bit MAC address	700-799
ACL IPX estándar	800-899
ACL IPX extendida	900-999
ACL IPX SAP	1000-1099
ACL 48 bit MAC address extendida	1100-1199
ACL IP estándar, rango expandido	1300-1999
ACL IP extendida, rango expandido	2000-2699
ACL SS7 (voz)	2700-2999

Existen dos clases de listas de control de acceso IP numeradas: la estándar y la extendida. Las listas de acceso IP estándar permiten o niegan el paso de los datagramas IP, basándose solamente en la dirección origen de

los mismos (y probablemente en la dirección destino). Las ACL estándar no tienen en cuenta el tipo de protocolo (TCP, UDP e ICMP, por ejemplo) ni el tipo de aplicación que se transporta (como telnet, e-mail, ftp o web). Asimismo, le dan igual trato a todo el tráfico dentro de una misma pila (suite) de protocolos.

En contraste, las listas de control de acceso IP extendidas proporcionan una mayor granularidad cuando se toman decisiones de filtrado. Con estas listas se pueden filtrar datagramas IP con base en: la dirección IP origen, la dirección IP destino, el protocolo especifico (TCP, UDP, ICMP), los números de puerto (el puerto 23 para telnet o el puerto 25 para e-mail en aplicaciones TCP/IP), la información que contenga el protocolo (como los mensajes ICMP echo request e ICMP echo reply) y otros patrones.

Los encaminadors Cisco soportan listas de acceso IP estándar (más simples) y listas de acceso IP extendidas (más complejas y versátiles). Es importante resaltar que en la interfaz, en un mismo sentido (de entrada o de salida), solamente se puede asociar una lista de acceso en un instante dado. Una vez creada una lista de acceso, ésta se puede aplicar a varias interfaces. El rango de valores que se pueden usar para definir una lista de acceso IP estándar está entre 1 y 99.

Es de notar que el uso de las listas de acceso IP demandan un sobrecosto computacional (overhead) del procesador; esto se debe a que para cada datagrama IP procesado es necesario comparar uno o más de sus campos con cada sentencia en la lista hasta encontrar una coincidencia. Por esta razón, las listas de acceso deben usarse solamente en caso de ser estrictamente necesarias.

Las listas de acceso son procesadas desde arriba hacia abajo (top-down); esto significa que el(los) campo(s) de interés del datagrama IP se comparará(n) con la primera sentencia de la lista, y, si se presenta una coincidencia (un match) entre el contenido del datagrama IP y la(s) condición(es) de la sentencia, se aplicará la acción que se haya definido en la sentencia. Cuando se presenta una coincidencia hay dos posibles acciones que se pueden ejecutar en el datagrama IP (la acción específica se define previamente en la sentencia con la cual se buscó la coincidencia), éstas son:

- Permit: permite el paso o reenvío del datagrama IP.
- Deny: descarta el datagrama IP.

Si se presenta una coincidencia en una sentencia, las siguientes sentencias no serán procesadas. Si no se presenta una coincidencia, el encaminador procederá a hacer una comparación con la siguiente sentencia de la lista.

Entonces, el orden de las sentencias de la lista de acceso es muy importante: las sentencias más específicas deberán colocarse al inicio de la lista y las más generales deberán ir al final.

Cuando se crea una lista de control de acceso, ésta conservará estrictamente el orden en que sean digitadas las sentencias (mediante comandos). El orden que se le de a las sentencias es muy importante debido a que, cuando el encaminador procesa un datagrama IP, busca coincidencias en las sentencias de la lista y se detiene en la búsqueda cuando encuentra la primera coincidencia. Por lo tanto, la definición y creación de la lista debe hacerse de lo específico a lo general.

Para ilustrar lo anterior, a modo de comparación se aborda el funcionamiento de las listas 80 y 90 definidas a continuación y con las cuales se persigue el objetivo de dejar pasar todo el tráfico proveniente de los equipos de la red 172.16.0.0/16, excepto que este tráfico se origine en el equipo con dirección 172.16.0.1/16, en cuyo caso se descartará.

Lista 80:

1. Permitir todo el tráfico proveniente de los equipos de la red 172.16.0.0/16
2. Negar todo el tráfico proveniente del dispositivo de red con la dirección 172.16.0.1/16

Lista 90:

1. Negar todo el tráfico proveniente del dispositivo de red con la dirección 172.16.0.1/16
2. Permitir todo el tráfico proveniente de los equipos de la red 172.16.0.0/16

Cuando un datagrama IP enviado por el equipo 172.16.0.1/16 enfrente la lista 80, se presentará una coincidencia en la primera entrada de dicha lista (el equipo pertenece a la red 172.16.0.0/16) y, por lo tanto, se aplicará la acción de reenvío del datagrama; como resultado, la lista 80 no cumplirá la función deseada.

Cuando un datagrama IP enviado por el equipo 172.16.0.1/16 enfrente la lista 90, se presentará una coincidencia en la primera entrada de dicha lista (el equipo es el 172.16.0.1/16) y, por lo tanto, se aplicará la acción de descartar el datagrama; como resultado, la lista 90 cumplirá la función deseada. Para los otros equipos de la red 172.16.0.0/16, la coincidencia se presentará en la segunda entrada de la lista 90, la cual permitirá su reenvío.

Negación implícita

Hay una condición especial en la lista de acceso que no ha sido discutida: ¿qué pasa si ante la llegada de un paquete (datagrama IP) se procesan todas las entradas (sentencias) de una lista, pero no se presenta una coincidencia? La respuesta es que el encaminador descartará todo paquete al cual no se le presente una coincidencia. Este proceso se conoce como negación implícita (*deny implicit*). Las listas de acceso tienen una sentencia imaginaria (escondida ante nuestros ojos y ubicada al final de la lista) que descartará todo el tráfico al que no se le presente una coincidencia en alguna de las sentencias anteriores de la lista. Entonces, desde una perspectiva de sentido común, cada lista de acceso deberá tener al menos una sentencia con una acción *permit*, de otra manera, todo el tráfico será descartado.

A continuación se presentan las sugerencias y los aspectos a tener en cuenta en la definición y creación de las listas de acceso:

- El orden de las sentencias en las listas de acceso es importante.
- Las sentencias más restrictivas deben colocarse al inicio de la lista y las más generales, al final.
- El procesamiento de una lista de acceso es top-down –desde la primera hacia la última sentencia– hasta que se encuentre una coincidencia.
- Hay una negación implícita al final de cada lista que descarta todo el tráfico que no fue explícitamente permitido en las sentencias anteriores de la lista.
- Se puede tener una lista de acceso por protocolo, por interfaz, por dirección (in/out), en otras palabras, no se pueden tener dos listas de acceso IP aplicadas en la salida de la misma interfaz.
- Cada lista de acceso es diferenciada por un número y varios protocolos tienen un rango de números reservados para su uso.
- Nunca aplique una lista de acceso vacía a una interfaz; por defecto, las listas de acceso vacías dejan pasar todo el tráfico por una interfaz, pero, tan pronto como se cree la primera sentencia de la lista, la negación implícita de la lista descartará todo el tráfico que no haya sido definido en dicha sentencia.
- El encaminador no puede filtrar el tráfico con una lista de acceso cuando éste se origina dentro del mismo encaminador.

Por las condiciones anteriores se puede concluir que las listas de acceso son difíciles de entender y de implementar, no son un tema simple y pueden, fácilmente, causar problemas.

Comandos para la configuración de listas de acceso IP estándar

En esta sección se cubrirán los aspectos básicos para la configuración de una lista de acceso IP estándar y los ejemplos específicos para la creación de filtros de tráfico TCP/IP.

Tareas a realizar

Configurar parámetros de entrada en la lista

Para crear una lista de acceso IP estándar se usa el comando de configuración global *access-list*.

R1(config)# ***access-list*** "ACL#" **permit | deny** "condiciones"

Antes de la versión 11.2 del IOS, el usuario tenía que asignar un número a la lista de acceso (ACL#), este número identifica de manera única a la lista de acceso y agrupa las sentencias hacia una sola entidad. No obstante, a partir de la versión 11.2, se pueden dar nombres en lugar de números para usar listas de acceso con nombres o "named access-list".

Para agrupar las sentencias en la lista de acceso se debe usar el mismo número (ACL#) en todas las sentencias que constituyan la lista de acceso. Las "condiciones" en la lista de acceso definen lo que deberá coincidir al comparar el contenido del datagrama IP para ejecutar la acción de permitir o negar.

Para IP se tiene la siguiente sintaxis:

R1(config)# *access-list* access-list-number {permit | deny} source [wildcard-mask] log

Descripción de los campos que acompañan al comando *access-list*:

- ***Accest-list-number***: un número en el rango de 1 hasta 99 para identificar la lista a la cual pertenecen las entradas.
- ***Pemit/deny***: indica la acción que ejecutará la entrada, en el sentido de permitir o bloquear el tráfico proveniente de la dirección especificada.
- ***Source***: identifica la dirección IP origen.
- ***Wildcard-mask***: "máscara de comodín", identifica cuáles bits del campo de dirección deben tenerse en cuenta. Los bits que tengan 0 en cualquier posición deben examinarse estrictamente y los bits que tengan 1 en cualquier posición no deben examinarse (don´t care); si dicho valor se omite, éste toma por defecto el valor 0.0.0.0

Activar la lista sobre una interfaz

La lista de acceso, por sí misma, no hace nada; una vez se crea la lista, ésta se debe activar sobre una interfaz con la finalidad de que el encaminador empiece a filtrar el tráfico sobre dicha interfaz.

La sintaxis, en general, para asociar una lista de acceso a una interfaz, es la siguiente:

```
R1(config)# interface fastethernet 0/0
R1(config-if)# "protocol" access-group "ACL#" in | out
```

El parámetro "*protocol*" es el protocolo que la lista de acceso filtrará, tal como IP, IPX, Appletalk, etc. Los parámetros "*in*" y "*out*" se refieren a la dirección de filtrado.

La sintaxis para asociar una lista de acceso IP estándar a una interfaz es:

```
R1(config)# interface fastethernet 0/0
R1(config-if)# ip access-group access-list-number {in | out}
```

En la línea anterior, el comando *ip access-group* asocia una lista existente a la interfaz FastEthernet 0/0. Solo se permite una lista de acceso por protocolo para cada interfaz.

Descripción de los campos del comando *ip access-group*:

Access-list-number: indica el número que identifica la lista a ser asociada a la interfaz.

In/out: selecciona si la lista de acceso será aplicada a los paquetes que estén entrando o saliendo de la interfaz; al no especificar nada, el valor por defecto es "*out*" (en versiones posteriores a la 12.x del IOS hay que especificarlo).

Ejemplo 1. Permitiendo el tráfico de una dirección de red

La siguiente lista de acceso permite que solamente el tráfico proveniente de la red 172.16.0.0/16 sea despachado (reenviado) por las interfaces Ethernet 0 y Ethernet 1 del encaminador Router de la Figura 6.1, el tráfico de otras fuentes será bloqueado.

Figura 6.1 Encaminador que permite el paso solamente de datagramas IP con la dirección origen de la red 172.16.0.0/16

Router(config)# *access-list* 1 permit 172.16.0.0 0.0.255.255 [primera entrada]

Siempre hay una última entrada creada por el sistema, ésta no es visible en la lista y su función es implícitamente negar el resto de condiciones que no se hayan cumplido. Similar a la siguiente línea.

access-list 1 deny 0.0.0.0 255.255.255.255 [última entrada] (equivalente a *access-list* 1 deny any)

Router(config)# *interface* ethernet 0
Router(config-if)# *ip access-group* 1 out

Router(config)# *interface* ethernet 1
Router(config-if)# *ip access-group* 1 out

Nota: Una entrada en la lista con "permit o deny" puede parar el tráfico de información de los algoritmos de enrutamiento cuyo destino sea de difusión (broadcast); para solucionar dicho problema es necesario adicionar explícitamente la siguiente entrada, la cual permitirá el tráfico de broadcast:

ip access-list 1 permit *255.255.255.255 0.0.0.0*

Ejemplo 2. Negando tráfico de un host específico

La siguiente lista de acceso está diseñada para bloquear el tráfico de la dirección específica 172.16.4.20 del host de la Figura 6.2 y, al mismo tiempo, permitir el resto de tráfico sobre la interfaz Ethernet 0.

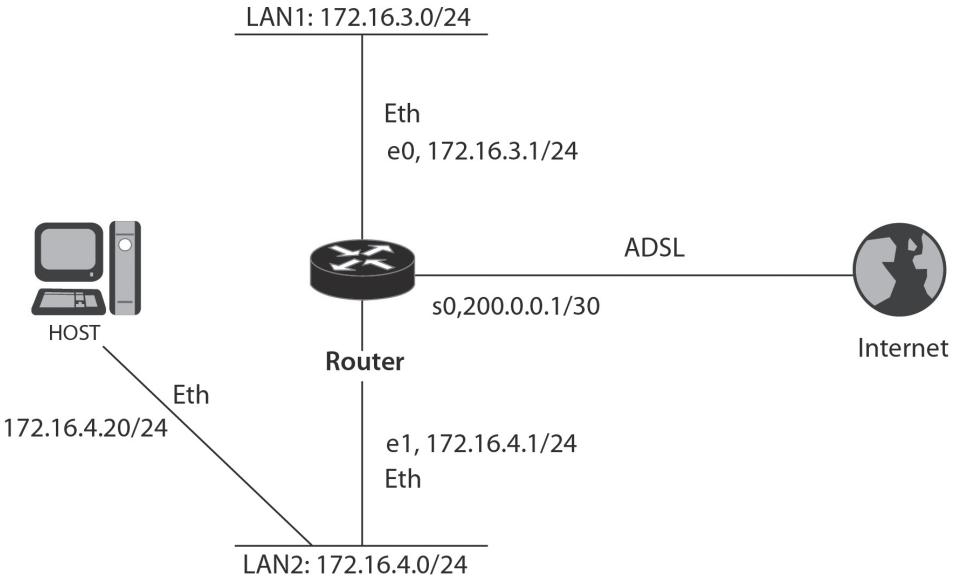

Figura 6.2 Encaminador que permite sobre la interfaz e0 todos los datagramas IP, excepto los que tengan dirección origen 172.16.4.20

Router(config)# *access-list* 2 deny 172.16.4.20 0.0.0.0 [primera entrada]
Router(config)# *access-list* 2 permit 0.0.0.0 255.255.255.255 [segunda entrada]
(Permite todo el tráfico incluyendo el de broadcast)

Router(config)# *interface* ethernet 0
Router(config-if)# *ip access-group* 2

Ejemplo 3. Negando tráfico de una subred

Esta lista de acceso está diseñada para bloquear el tráfico proveniente de la subred 172.16.4.0 y permitir que el resto del tráfico sea despachado.

Router(config)# *access-list* 3 deny 172.16.4.0 0.0.0.255 [primera entrada]
Router(config)# *access-list* 3 permit 0.0.0.0 255.255.255.255 [segunda entrada]

Router(config)# *interface* ethernet 0
Router(config-if)# *ip access-group* 3 out

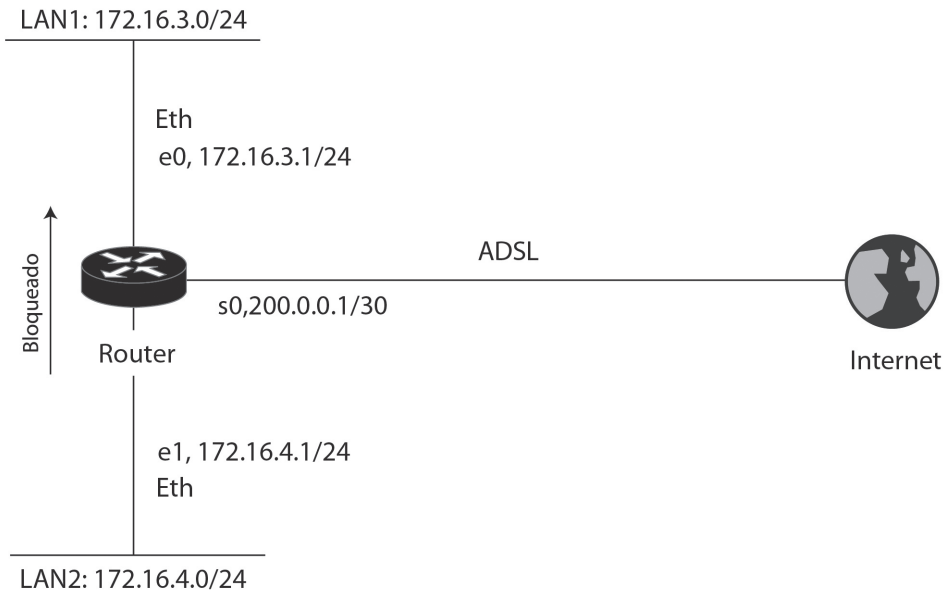

Figura 6.3 Encaminador que permite sobre la interfaz e0 todos los datagramas IP, excepto los que vengan de la red 172.16.4.0/24

Verificando las listas de acceso

El comando *show acces-list* muestra el contenido de las listas de acceso número 2 y 3.

Router# *show access-lists*

```
Standard IP access list 2
    deny 172.16.4.20
    permit 0.0.0.0, wildcard bits 255.255.255.255
Standard IP access list 3
    deny 172.16.4.0, wildcard bits 0.0.0.255
    permit 0.0.0.0, wildcard bits 255.255.255.255
```

El comando *show ip interface* muestra la información IP de las interfaces e indica si éstas se asocian una lista de acceso.

Router# *show ip interface*

```
Serial0 is up, line protocol is up
 Internet address is 192.168.2.1, subnet mask is 255.255.255.0
 Broadcast address is 255.255.255.255
 Address determined by non-volatile memory
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is enabled
 Outgoing access list is 3
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachables are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled
 IP fast switching on the same interface is disabled
 IP SSE switching is disabled
 Router Discovery is disabled
 IP output packet accounting is disabled
 IP access violation accounting is disabled
 TCP/IP header compression is disabled
 Probe proxy name replies are disabled
 Gateway Discovery is disabled
```

Informe

Proponga una red en la que se controle el acceso de un equipo por medio de una lista de acceso estándar, mencione las ventajas y desventajas que se tienen al utilizar una lista de acceso estándar.

Encuentre los errores de la siguiente lista de acceso IP estándar y proponga la lista de acceso IP corregida.

```
Router(config)# access-list 1 permit 192.168.2.1
Router(config)# access-list 1 deny 192.168.2.2
Router(config)# access-list 1 permit 192.168.2.0 0.0.0.255
Router(config)# access-list 1 deny any
Router(config)# interface serial 0/0
Router(config-if)# ip access-group 1 in
```

Encuentre los errores de la siguiente lista de acceso IP estándar y proponga la lista de acceso IP corregida.

```
Router(config)# access-list 2 deny 192.168.2.0
Router(config)# access-list 2 deny 172.20.0.0
Router(config)# access-list 2 permit 192.168.2.1
Router(config)# access-list 2 permit 0.0.0.0 255.255.255.255
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip access-group 1 out
```

Ejercicios de laboratorio

En este ejercicio se requiere configurar una lista de acceso en el Encaminador Router_A para permitir que el telnet a dicho encaminador lo pueda realizar únicamente cualquier equipo que forme parte de la red 192.168.1.0/24. La misma restricción se desea aplicar en los encaminadores Router_B y Router_C.

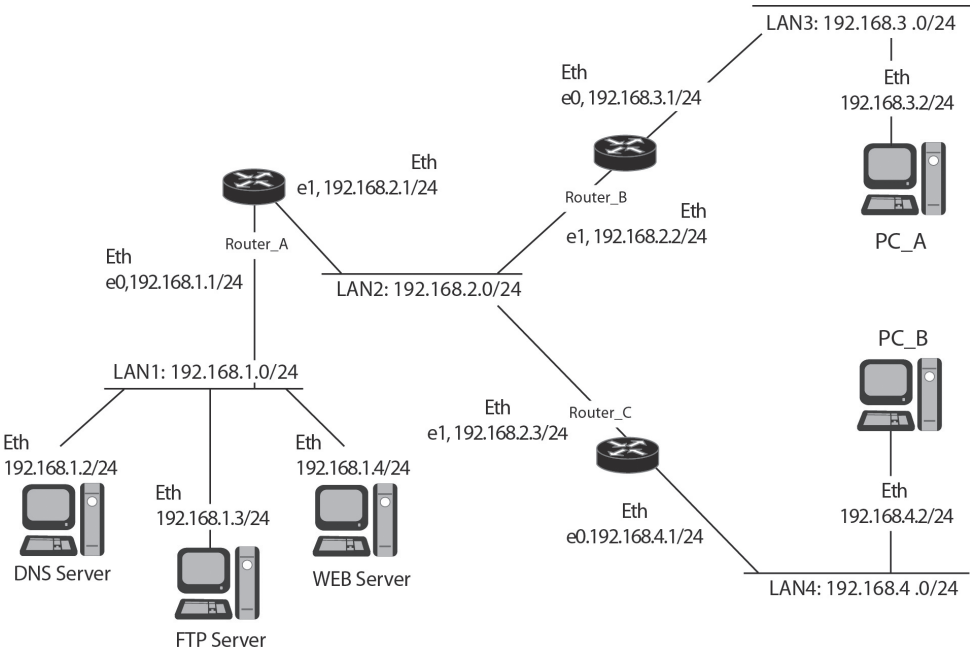

Figura 6.4 Red con listas de acceso

Procedimiento: para cumplir la primera función se debe entrar al encaminador Router_A, crear una lista de acceso IP estándar y aplicarla de la siguiente manera:

Configuración del Encaminador Router_A:

```
Router_A(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router_A(config)# line vty 0 4
Router_A(config-line)# access-class 1 in
```

(La misma configuración se debe aplicar a los encaminadores Router_B y Router_C).

Tareas adicionales: Verificar la configuración de los encaminadores haciendo lo siguiente:

1. Desde los PC intente hacer telnet a los encaminadores.
2. Desde cualquier encaminador, intente hacer telnet hacia otro.
3. Desde un equipo en la red 192.168.1.0/24, intente hacer telnet a los encaminadores.

Sugerencia: se puede usar GNS3 para emular los encaminadores y VPCS (Virtual PC Simulator) para simular los PC; otra posibilitad es usar Packet Tracer.

Información complementaria

Corrección de las entradas de una lista de acceso

Una vez construida una lista de acceso IP estándar, sus entradas no pueden ser borradas ni insertadas (las listas de acceso con nombres facilitan su edición; ver sección "Información complementaria" del capítulo 7). Si se ejecuta el comando *no access-list* para tratar de remover una sola entrada, el encaminador borrará la lista de acceso completa. Asimismo, cada comando que se digite en una lista de acceso será colocado al final de la lista. Para editar una línea de una lista de acceso es mejor visualizarla con el comando *show running-config*, pegarla a un editor de texto, corregirla en el editor de texto, desasociarla de la interfaz, copiarla desde el editor de texto hacia el encaminador y finalmente asociarla a la interfaz.

Máscara comodín (Wildcard mask)

Una máscara comodín no es una máscara de subred, tal como una dirección IP; una máscara comodín tiene una longitud de 32 bits y se usa para verificar sobre cuáles de los 32 bits de una dirección IP debe buscarse una coincidencia o simplemente ignorar dicho bit.

Un 0 en una posición de bit de la máscara comodín significa que se debe buscar coincidencia en el bit de la dirección IP que tenga la misma posición.

Un 1 en una posición de bit de la máscara comodín significa que no se debe buscar coincidencia en el bit de la dirección IP que tenga la misma posición.

Algunas veces a la máscara comodín se le denomina *máscara invertida*; cuando se desea buscar una coincidencia con una dirección de red o de subred, todo lo que se debe hacer para obtener la máscara comodín a partir de la máscara de red es: al valor 255 se le resta el valor decimal de cada octeto (byte) de la máscara de red.

Ejemplos:

- Para buscar una coincidencia con la subred 255.255.255.0 se requiere una máscara comodín de 0.0.0.255
- Para buscar una coincidencia con la subred 255.255.240.0 se requiere una máscara comodín de 0.0.15.255

Nótese que la máscara comodín se obtiene siempre de tomar el número 255 y restarle el valor que tenga la máscara de red.

Máscaras comodín especiales

La máscara comodín 0.0.0.0 establece que todos los 32 bits de la dirección del paquete deben coincidir con la dirección especificada en la sentencia, por ejemplo, el valor **172.16.1.1 0.0.0.0** representa una condición en la cual, por medio de la máscara comodín, se requiere que la dirección del paquete sea exactamente igual a **172.16.1.1** para que haya una coincidencia. La expresión **172.16.1.1 0.0.0.0** puede ser remplazada en el comando por la expresión **host 172.16.1.1**.

La máscara comodín 255.255.255.255 realiza la función opuesta a la máscara comodín 0.0.0.0. Es decir, con 255.255.255.255 no se requiere coincidencia en ningún bit de la dirección del paquete y, como consecuencia, cualquier dirección en el paquete dará una coincidencia. Normalmente el valor 0.0.0.0 255.255.255.255 sirve en una sentencia para tener una coincidencia, independientemente de la dirección del paquete, pues, aunque obviamente no existen paquetes con una dirección IP de 0.0.0.0, el valor de cualquier dirección que tenga el paquete coincidirá si la máscara comodín fuera 255.255.255.255. La expresión **0.0.0.0 255.255.255.255** puede ser reemplazada en el comando por la expresión **any**.

Problemas

1. Al aplicar una lista de control de acceso como salida en la interfaz de un encaminador (mediante el comando *ip access group número-de-lista out*) se presenta una peculiaridad de la cual se debe estar consciente: el comando no filtra los datagramas IP que se originan en el encaminador mismo. Verifique dicha peculiaridad.
2. Las listas de acceso permiten que sus expresiones o sentencias queden comentadas en el archivo de configuración para aclarar lo que hacen. Verifique esta característica con el siguiente código.

```
R1(config)# ip access-list standard ACL-COMENTADA
R1(config-std-nacl)# remark Impide el paso de uno de los equipos de la red 192.168.1.0
R1(config-std-nacl)# deny host 192.168.1.2
R1(config-std-nacl)# permit 192.168.1.2 0.0.0.255
R1(config-std-nacl)# permit any
R1(config-std-nacl)# end
```

Glosario

Coincidencia (match): se presenta cuando los campos de un datagrama IP (incluido el campo de datos) cumplen las condiciones definidas en una línea de la lista de control de acceso IP.

Host: estación de trabajo, computador, servidor, portátil, impresora que se encuentra conectado(a) como sistema final de una red IP.

Máscara comodín (wildcard mask): cadena de 32 bits, los cuales determinan la posición de los bits de la dirección IP que se deben tener en cuenta (bits del comodín puestos en cero) y de los que no se deben tener en cuenta (bits del comodín puestos en uno). Generalmente, su valor se representa con notación punto decimal, similar a la representación de una dirección IP o a la representación de la máscara de subred.

Pila: es el conjunto de protocolos definidos en la arquitectura TCP/IP. Por ejemplo, los protocolos IP, TCP, UDP, DHCP, etc. son algunos de los que conforman la pila TCP/IP.

Sobrecosto computacional: cualquier procesamiento computacional adicional que se haga por encima del requerido en condiciones normales.

Top-down: procesamiento ordenado y secuencial que se realiza con las sentencias que conforman la lista de control de acceso; siempre se inicia con la primera sentencia y, en caso de no encontrar una coincidencia, se conti-

núa con la siguiente. Este proceso se repite hasta encontrar una coincidencia o hasta llegar al final de la lista.

Bibliografía

BONEY, J. (2005). *Cisco IOS in a Nutshell*. 2nd Ed. Sebastopol, CA: O'Reilly.

DOOLEY, K.; BROWN, I. (2007). *Cisco IOS Cookbook ™*. 2nd Ed. Sebastopol, CA: O'Reilly.

SEDAYAO, J. (2001). *Cisco IOS Access Lists*. Sebastopol, CA: O'Reilly.