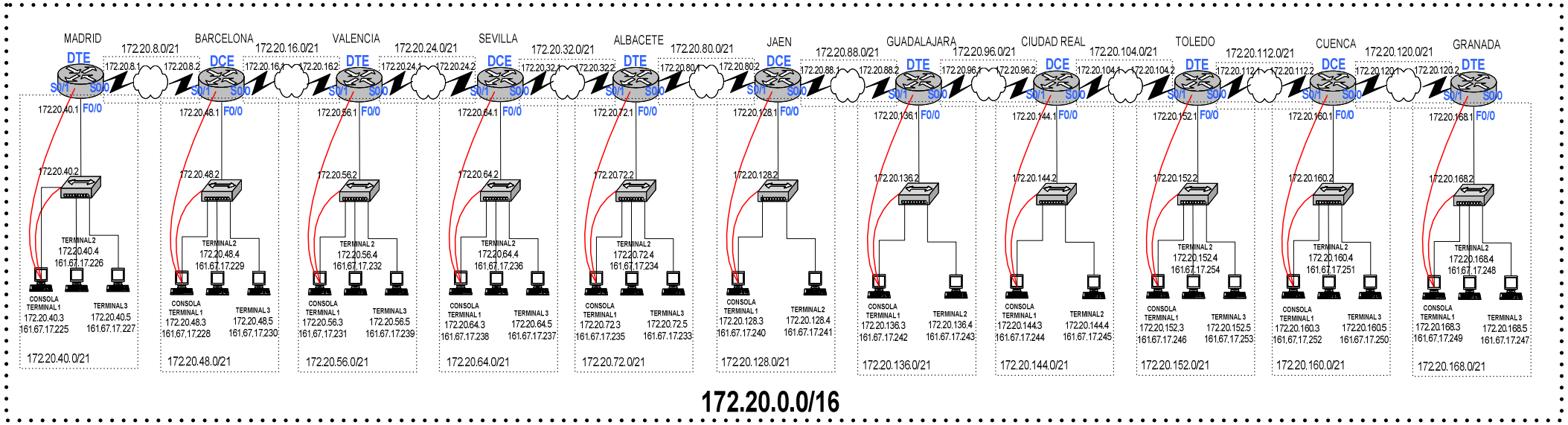
AMPLIACIÓN DE REDES
(2º I.T.I.S.)

PRÁCTICA 4

CONFIGURACIÓN DE ROUTERS: LISTAS DE CONTROL DE ACCESO (ACLs)

Unidad Docente de Redes
Área de Arquitectura y Tecnología
de Computadoras
Departamento de Informática
Universidad de Castilla-La Mancha

TOPOLOGÍA DEL LABORATORIO DE REDES (EPSA)



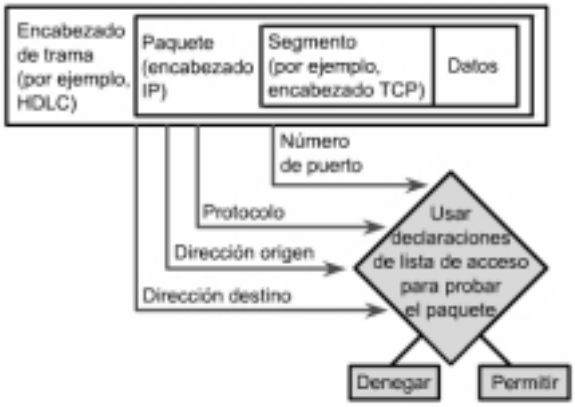
1. Objetivo

El objetivo de esta práctica es que el alumno adquiera los conocimientos prácticos sobre las Listas de Control de Accesos (ACLs) en la configuración de routers. El objetivo final de esta práctica es observar el funcionamiento y la configuración de las mismas, observando sus ventajas en lo referente al filtrado de tráfico que atraviesa un router. Este objetivo se puede desglosar en los siguientes objetivos parciales:

1. Configuración de una ACL IP Estándar
   - Desarrollar una ACL estándar para permitir o denegar tráfico específico
   - Aplicar una ACL IP estándar a una interfaz de router
   - Probar la ACL para determinar si se lograron los resultados deseados
   - Eliminar una ACL de una interfaz de router
   - Eliminar una ACL de un router
2. Configuración de una ACL IP Extendida
   - Desarrollar una ACL IP extendida para permitir o denegar tráfico específico
   - Aplicar una ACL IP extendida a una interfaz de router.
   - Probar la ACL para determinar si se lograron los resultados deseados.
3. Diseñar y planificar una ACL, según requisitos de seguridad específicos.

2. ¿Qué es una ACL?

Una ACL es una colección secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior. Los routers proporcionan capacidades de filtrado de tráfico a través de las **listas de control de acceso (ACL)**. En esta práctica, conocerá las ACL estándar y extendidas como medio de controlar el tráfico de red y de qué manera se usan las ACL como parte de una solución de seguridad (cortafuegos).



Las ACL son listas de instrucciones que se aplican a una interfaz del router. Estas listas indican al router qué tipos de paquetes se deben aceptar y qué tipos de paquetes se deben denegar. La aceptación y rechazo se pueden basar en ciertas especificaciones, como dirección origen, dirección destino y número de puerto. Cualquier tráfico que pasa por la interfaz debe cumplir ciertas condiciones que forman parte de la ACL. Las ACL se pueden crear para todos los protocolos enrutados de red, como IP e IPX, para filtrar los paquetes a medida que pasan por un router. Es necesario definir una ACL para cada protocolo habilitado en una interfaz si desea controlar el flujo de tráfico para esa interfaz. Por ejemplo, si su interfaz de router estuviera configurada para IP, AppleTalk e IPX, sería necesario definir por lo menos tres ACL. Cada ACLs sobre cada interfaz, actúa en un sentido, distinguiendo tanto sentido de entrada como de salida. Se puede definir diferentes ACLs y luego instalarlas sobre los interfaces del router según convenga al administrador de la red.

Razones para el uso de ACLs

Hay muchas razones para crear ACLs. Por ejemplo, las ACL se pueden usar para:

- Limitar el tráfico de red y mejorar el rendimiento de la red. Por ejemplo, las ACL pueden designar ciertos paquetes para que un router los procese antes de procesar otro tipo de tráfico, según el protocolo. Esto se denomina colocación en cola, que asegura que los routers no procesarán paquetes que no son necesarios. Como resultado, la colocación en cola limita el tráfico de red y reduce la congestión.

- Brindar control de flujo de tráfico. Por ejemplo, las ACL pueden restringir o reducir el contenido de las actualizaciones de enrutamiento. Estas restricciones se usan para limitar la propagación de la información acerca de redes específicas por toda la red.

- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le deniega el acceso a dicha red. Si no se configuran ACL en su router, todos los paquetes que pasan a través del router supuestamente tendrían acceso permitido a todas las partes de la red.

- Se debe decidir qué tipos de tráfico se envían o bloquean en las interfaces del router. Por ejemplo, se puede permitir que se enrute el tráfico de correo electrónico, pero bloquear al mismo tiempo todo el tráfico de telnet.

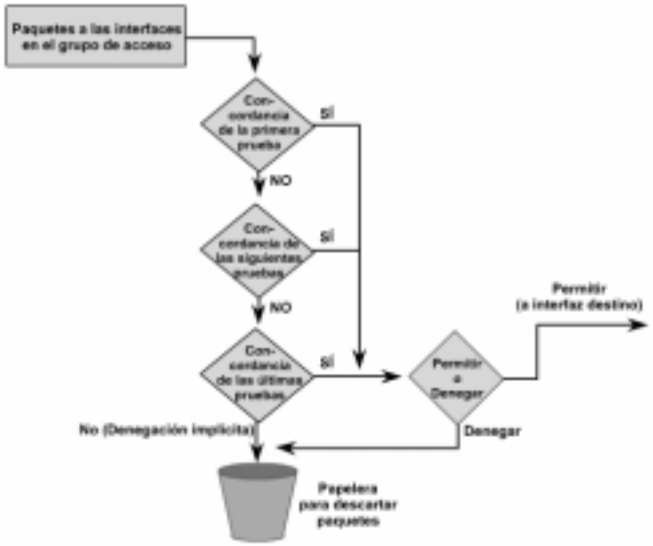
3. Funcionamiento de las ACLs

Una ACL es un grupo de sentencias que define cómo los paquetes:

- Entran a las interfaces de entrada
- Se reenvían a través del router
- Salen de las interfaces de salida del router

El principio del proceso de comunicaciones es el mismo, ya sea que las ACL se usen o no. Cuando un paquete entra en una interfaz, el router verifica si un paquete es enrutable o puenteable. Ahora, el router verifica si la interfaz de entrada tiene una ACL. Si existe, ahora se verifica si el paquete cumple o no las condiciones de la lista. Si el paquete es permitido, entonces se compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino. A continuación, el router verifica si la interfaz destino *tiene* una ACL. Si no la tiene, el paquete puede ser enviado directamente a la interfaz destino.

Las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si las sentencias de la ACL no se verifican, se impone una sentencia implícita de "denegar cualquiera". Esto significa que, aunque la sentencia "denegar cualquiera" no se vea explícitamente en la última línea de una ACL, está allí.



4. Configuración de las ACLs

Requieren dos pasos básicos. El primer paso es crear una definición de ACL, y el segundo es aplicar la ACL a una interfaz. Las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente, según la configuración. Sólo se permite una ACL por interfaz. Las ACL salientes son generalmente más eficientes que las entrantes, y por lo tanto siempre se prefieren. Un router con una ACL entrante debe verificar cada paquete para ver si cumple con la condición de la ACL antes de conmutar el paquete a una interfaz saliente.

PASO 1: Definir las sentencias que formarán la ACL. Cada una de ellas se define con la siguiente sentencia

Router (config)# **access-list** numero-lista-acceso **{permit | deny}** {condiciones}

PASO 2: Aplicar dicha ACL sobre los interfaces en el sentido deseado con

Router (config-if)# **{protocol} access-group** numero-lista-acceso **{in/out}**

- Las ACL se crean utilizando el modo de configuración global.
- Al configurar las ACL en un router, se debe identificar cada ACL de forma exclusiva, asignando un número a la ACL del protocolo. Cuando se usa un número para identificar una ACL, el número debe estar dentro del intervalo específico de números que es válido para el protocolo.

Protocolo	Intervalo
IP	1-99
IP extendido	100-199
AppleTalk	600-699
IPX	800-899
IPX extendido	900-999
Protocolo de publicación de servicio IPX	1000-1099

- Se deben seleccionar y ordenar lógicamente las sentencias que forman la ACL de forma muy cuidadosa. Cada una de estas sentencias debe hacer referencia al mismo nombre o número identificatorio, para relacionar las sentencias a la misma ACL. Se puede establecer cualquier cantidad de sentencias de condición, pero cuanto más sentencias se establezcan, mayor será la dificultad para comprender y administrarla ACL.
- Después de crear una ACL numerada, debe asignarla a una interfaz para poderla usar. Si desea alterar una ACL que contiene sentencias de ACL numeradas, necesita eliminar todas las sentencias en la ACL numerada mediante el comando **no access-list** *numero-lista-acceso*.

5. Mascara de Wildcard

Una máscara wildcard es una cantidad de 32 bits que se divide en cuatro octetos, en la que cada octeto contiene 8 bits. Un bit de máscara wildcard de **0** significa "**verificar el valor de bit correspondiente**" y un bit **1** de una máscara wildcard significa "**no verificar (ignorar) el valor de bit correspondiente**". Una máscara wildcard se compara con una dirección IP. Los números uno y cero se usan para identificar cómo tratar los bits de la dirección IP correspondientes. Las ACL usan máscaras wildcard para identificar una sola o múltiples direcciones para las pruebas de aprobar o rechazar. Aunque ambas son cantidades de 32 bits, las máscaras wildcard y las máscaras de subred IP operan de manera diferente.

Digamos que desea verificar una dirección IP para verificar la existencia de subredes que se pueden permitir o denegar. Supongamos que la dirección IP es una dirección Clase B (es decir, que los primeros dos octetos son el número de red) con 8 bits de división en subredes (el tercer octeto es para las subredes). Es necesario usar bits de máscara wildcard IP para permitir todos los paquetes desde cualquier host en las subredes 172.30.16.0 a 172.30.31.0. La figura muestra un ejemplo de cómo usar la máscara wildcard para hacer esto. Para empezar, la máscara wildcard verifica los primeros dos octetos (172.30), utilizando los bits de cero correspondientes en la máscara wildcard. Como no interesan las direcciones de host individuales (un identificador de host no tiene .00 al final de la dirección), la máscara wildcard ignora el octeto final, utilizando los bits unos correspondientes en la máscara wildcard.

En el tercer octeto, la máscara wildcard es 15 (00001111), y la dirección IP es 16 (00010000). Los primeros cuatro ceros en la máscara wildcard indican al router que debe comparar los primeros cuatro bits de la dirección IP (0001). Como los últimos cuatro bits se ignoran, todos los números dentro del intervalo de 16 (00010000) a 31 (00011111) coinciden porque comienzan con el patrón 0001. Para los cuatro bits finales (menos significativos) en este octeto, la máscara wildcard ignora el valor porque en estas posiciones, el valor de la dirección puede ser cero o uno binarios, y los bits wildcard correspondientes son unos. En este ejemplo, la dirección 172.30.16.0 con la máscara wildcard 0.0.15.255 coincide con las subredes 172.30.16.0 a 172.30.31.0. La máscara wildcard no coincide con ninguna otra subred.

Trabajar con representaciones decimales de bits wildcard binarios puede ser una tarea muy tediosa. Para los usos más comunes de las máscaras wildcard, se pueden usar abreviaturas. Estas abreviaturas reducen la cantidad de cosas que hay que escribir cuando se configuran condiciones de prueba de direcciones. Si especificamos que cualquiera cumple la sentencia pondríamos como dirección IP 0.0.0.0 y de máscara todo 1's para que se ignore (255.255.255.255), por tanto la palabra **any** sustituye a 0.0.0.0 255.255.255.255. Por ejemplo, en lugar de usar esto:

Router(config)# **access-list** 1 permit 0.0.0.0 255.255.255.255

se puede usar esto:

Router(config)# **access-list** 1 permit any

Si especificamos una dirección IP determinada, daremos la dirección y luego la máscara de todo 0's, que se simplifica con la palabra **host**. Por ejemplo, en lugar de usar esto:

Router(config)# **access-list** 1 permit 172.30.16.29 0.0.0.0

se puede usar esto:

Router(config)# **access-list** 1 permit host 172.30.16.29

6. ACL Estándar

Las ACL estándar verifican **solo la dirección origen de los paquetes** que se deben enrutar. Se deben usar las ACL estándar cuando se desea bloquear todo el tráfico de una red, permitir todo el tráfico desde una red específica o denegar conjuntos de protocolo. El resultado permite o deniega el resultado para todo un conjunto de protocolos, según las direcciones de red, subred y host. Las ACL estándar, aunque son más fáciles de crear, proporcionan menor control sobre el tráfico de red.

Como hemos aprendido, se usa la versión estándar del comando de configuración global **access-list** para definir una ACL estándar con un número. La sintaxis completa del comando es

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

Se usa la forma **no** de este comando para eliminar una ACL estándar. Esta es la sintaxis:

Router(config)# **no access-list** access-list-number

donde **log** permite registrar los incidentes (msg: nº ACL, si el paquete ha sido permitido o denegado, dirección origen y el número de paquetes)

EJEMPLO 1: la ACL sólo permite que se envíe el tráfico desde la red origen 172.16.0.0. El tráfico que no es de 172.16.0.0 se bloquea. También se muestra en el ejemplo cómo el comando **ip access-group 1 out** agrupa la ACL y la aplica a una interfaz saliente.

Router(config)# access-list 1 permit 172.16.0.0 0.0.255.255

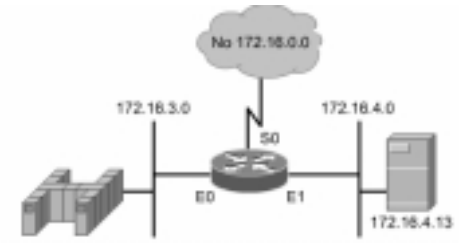
(*access-list 1 deny any* está implícito)

Router(config)# interface f 0/0

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

Router(config-if)# interface f 0/1

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



EJEMPLO 2: ACL para bloquear el tráfico proveniente de una dirección específica, 172.16.4.13, y para permitir que todo el tráfico restante sea enviado en la interfaz Ethernet 0. El primer comando **access-list** usa el parámetro deny para denegar el tráfico del host identificado. La máscara de dirección 0.0.0.0 en esta línea requiere que en la prueba coincidan todos los bits. Esta condición también se puede escribir empleando la palabra clave ***host***. En el segundo comando **access-list** la combinación de máscara wildcard / dirección IP 0.0.0.0 255.255.255.255 identifica el tráfico de cualquier origen. Esta combinación también se puede escribir utilizando la palabra clave **any**. Cualquier paquete que no coincida con la primera línea de la ACL coincidirá con la segunda y se enviará.

Router(config)# access-list 1 deny 172.16.4.13 0.0.0.0

(o bien, access-list 1 deny host 172.16.4.13)

Router(config)# access-list 1 permit 0.0.0.0 255.255.255.255

(o bien, access-list 1 permit any)

(*access-list 1 deny any* está implícito)

Router(config)# interface f 0/0

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

EJEMPLO 3: ACL está diseñada para bloquear el tráfico desde una subred específica, 172.16.4.0, y para permitir que el resto del tráfico sea enviado

Router(config)# access-list 1 deny 172.16.4.0 0.0.0.255

Router(config)# access-list 1 permit any

(*access-list 1 deny any* está implícito)

```
Router(config)# interface f 0/0
Router(config-if)# ip access-group 1 out
```

En esta práctica de laboratorio se trabaja con listas de control de acceso estándar (ACL) para regular el tráfico que se permite pasar a través de un router según el origen, ya sea un host específico (normalmente una estación de trabajo o servidor) o una red completa (cualquier host o servidor en esa red). Una ACL estándar es una herramienta simple y efectiva para controlar qué paquetes pueden pasar a través de un router desde una red a otra. Las ACL estándar son una forma básica de control con capacidades limitadas. Pueden filtrar (permitir o denegar) paquetes que salen de o entran a una interfaz de router utilizando sólo la dirección IP de la red o host origen. Por lo tanto, **se deben aplicar cerca de la dirección destino**, ya que dicha dirección no se puede especificar.

Otros protocolos enrutados (o enrutables) como IPX o AppleTalk también pueden tener ACL o filtros pero esta práctica de laboratorio se concentra en las ACL IP. Cuando se aplica una ACL IP estándar, ésta filtra (permite o deniega) todo el conjunto de protocolo IP (IP, TCP, SMTP, HTTP, Telnet etc.). Cuando se crean las ACL IP estándar se numeran del 1 al 99.

Estos son los pasos necesarios para usar las ACL de forma efectiva:

- Determinar los requisitos de la ACL (según las necesidades de seguridad, etc.)
- Desarrollar la ACL
- Verificar las sentencias en la ACL
- Aplicar la ACL a una interfaz de router
- Verificar que la ACL se aplique correctamente a la interfaz que se desea
- Verificar que la ACL funcione correctamente

En esta práctica de laboratorio se desarrolla, aplica y prueba una ACL IP estándar. Se realizan dos ejercicios. En el Ejercicio A se deben bloquear paquetes desde un host o red específico/a, impidiendo que accedan a cualquier host u otra red. En el Ejercicio B se bloquea el tráfico desde todos los hosts en una red específica, impidiendo que accedan a cualquier host en una red completa. Realice primero el ejercicio A, una vez acabado elimine la ACL del ejercicio A y realice el ejercicio B.

Ejercicio A: La ACL 1 impide que el tráfico IP desde un host específico (estación de trabajo con dirección IP 172.20.xxx.3, donde xxx es 40,48,56,64, etc, según sea tu red) conectada al switch Fast-Ethernet de la interfaz f0/0 de tu router, alcance tu red vecina hacia la derecha (p. ej., desde 172.20.40.3 no se debe poder alcanzar la subred 172.20.48.0 que cuelga de Barcelona, pero sí el resto de redes).

Ejercicio B: La ACL 2 impide que el tráfico IP desde todos los hosts de tu red alcance tu red vecina hacia la derecha.

Tarea 1. Configuración de una ACL IP Estándar

Paso 0. Borrar las ACLs existentes. Ejecuta el comando ***show access-list*** para comprobar si existe alguna ACL definida. En ese caso, bórralas con el comando ***no access-list <nº>***. Comprueba también si algún interfaz tiene aplicada ninguna ACL con el comando ***show ip interface***. En ese caso, desactívalas empleando el comando ***no ip access-group <nº> in/out***, desde el modo de configuración del interfaz.

Paso 1. Determinar los requisitos de la ACL. ¿Cuál es tráfico (paquetes) que se bloquea (deniega) o se permite, y de qué hosts o redes proviene? Como se usa una ACL IP estándar, sólo se puede filtrar según la dirección origen. Con el ejercicio A, se desea bloquear el tráfico desde la dirección de host 172.20.xxx.3, donde xxx es 40,48,56,64, etc, según sea tu red. Con el Ejercicio B, se desea bloquear el tráfico desde todos los hosts de tu red.

Paso 2. Determinar el lugar (router+interfaz) de aplicación de las ACLs. Como las ACL estándar sólo pueden especificar o verificar direcciones origen, se debe aplicar el filtro lo más cerca posible del destino. ¿A qué router y a qué interfaz se puede aplicar la ACL para cada uno de los ejercicios de ejemplo, A o B? Consulte el diagrama de laboratorio estándar y llene la tabla siguiente con la dirección (o direcciones) IP que se deben bloquear, la red a la cual no deben acceder, el router donde se debe aplicar la ACL, la interfaz a la que se aplicará y si se bloquea la entrada o la salida (IN o OUT)

Ejercicio	Host IP o red que se debe denegar (bloquear)	Red a la que no deben acceder los paquetes	Router donde se debe aplicar la ACL	Interfaz donde se debe aplicar la ACL (S0, S1, E0, etc)	IN o OUT
A (ACL 1)					
B (ACL 2)					

Nota: Recuerde que debe colocar las ACL estándar cerca del destino

Paso 3. Desarrollar la ACL. Definir las sentencias ACL en modo Router(config)#, en el router adecuado segñun la tabla anterior. Las sentencias ACL son aditivas. Cada sentencia se agrega a la ACL. Si hay más de una sentencia en la ACL (lo que es típico) y se desea cambiar una sentencia anterior, se debe borrar la ACL y comenzar de nuevo. En estos ejemplos se bloquean paquetes desde sólo una dirección de host IP o una red. Como las ACL siempre terminan con un "deny any" implícito, si se utilizan una de las sentencias anteriores esto haría que esta lista denegara una sola dirección origen, pero también denegaría implícitamente cualquier otra dirección origen. Nuestro objetivo es sólo denegar el acceso desde un único host, de manera que es necesario agregar una segunda sentencia para permitir todo el tráfico restante.

Paso 4. Verificar las sentencias en la ACL. Utilice el siguiente comando ***show access-list*** *número-lista* para controlar sus sentencias y verificar que todo se haya escrito correctamente. Si desea corregir un error o hacer un cambio en una sentencia existente se debe eliminar la ACL y comenzar de nuevo. ¿Cuántas sentencias hay en la ACL?

Paso 5. Aplicar la ACL a un interfaz del router. Utilice para ello el comando ***ip access-group*** <nº acl> ***in/out***, dentro del modo de configuración del interfaz adecuado.

Paso 6. Verificar si la ACL se aplica a la interfaz correcta. El comando ***show ip interface*** muestra información de interfaz IP e indica si se ha establecido alguna ACL. ¿Cuáles fueron los resultados que demuestran que la ACL se ha aplicado correctamente?

Paso 7. Verificar que la ACL funcione correctamente. Pruebe la ACL intentando enviar paquetes desde el host/red origen que se debe permitir o denegar. Emita varios comandos ***ping*** para probar estas ACL según sea el ejercicio.

7. ACL Extendida

Las ACL extendidas verifican las direcciones origen y destino de los paquetes. También pueden verificar protocolos, números de puerto y otros parámetros específicos. Esto ofrece mayor flexibilidad para describir las verificaciones que debe realizar la ACL. Las ACL extendidas se usan con mayor frecuencia para verificar condiciones porque ofrecen una mayor cantidad de opciones de control que las ACL estándar. Se puede usar una ACL extendida cuando se desea permitir el tráfico de la Web pero denegar el Protocolo de transferencia de archivos (FTP) o Telnet desde las redes que no pertenecen a la empresa. Como las ACL extendidas pueden bloquear el tráfico según la dirección destino, se pueden **ubicar cerca del origen**, lo que ayuda a reducir el tráfico de red. Algunos de los números de puerto más comunes aparecen en la tabla. La forma completa del comando **access-list** de una ACL extendida es:

Decimal	Palabra clave	Descripción	Protocolo
0		Reservado	
1-4		No asignado	
20	FTP-DATOS	FTP (datos)	TCP
21	FTP	FTP	TCP
23	TELNET	Conexión terminal	TCP
25	SMTP	SMTP	TCP
42	NAMESERVER	Servidor de nombre del host	UDP
53	DOMAIN	DNS	TCP/UDP
69	TFTP	TFTP	UDP
70		Gopher	TCP/IP
80	HTTP	WWW	TCP
133-159		No asignado	
160-223		Reservado	
162		FNP	UDP
224-241		No asignado	
242-251		No asignado	

Router(config)# **access-list** access-list-number {**permit** | **deny**} protocol **source** [source-mask **destination** destination-mask operator operand] [established]

Log: para registrar los incidentes (msg: nº ACL, si el paquete ha sido permitido o denegado, dirección origen y el número de paquetes)
proto: ip, tcp, udp, icmp, gre, igrp
operation: lt(less than), gt(greater than), eq (equal), neq (non equal) y
operand: un número de puerto
established: Permite que pase tráfico TCP si el paquete utiliza una conexión establecida (bit ACK activado)

EJEMPLO 1: ACL extendida que bloquea el tráfico de FTP (el servicio FTP emplea el puerto TCP 21).

Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

Router(config)# access-list 101 permit ip 172.16.4.0 0.0.0.255 0.0.0.0 255.255.255.255

(*access-list 1 deny any* está implícito)

Router(config)# interface f 0/0

Router(config-if)# ip access-group 101 out

EJEMPLO 2: ACL que no permite que el tráfico de Telnet (el servicio Telnet emplea el puerto TCP 23) desde 172.16.4.0 se envíe desde la interfaz E0. Se permite todo el tráfico desde cualquier otro origen a cualquier otro destino

Router(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23

Router(config)# access-list 101 permit ip any any

(*access-list 1 deny any* está implícito)

Router(config)# interface f 0/0

Router(config-if)# ip access-group 101 out

En esta práctica de laboratorio se trabaja con las ACL extendidas para regular el tráfico que se permite que pase a través del router, según el origen y el tipo de tráfico. Las ACL son una herramienta importante para controlar qué paquetes, y qué tipo de paquetes pueden pasar a través de un router desde una red a otra. En esta práctica de laboratorio se desarrollará, aplicará y probará una ACL IP extendida. Realice el Ejercicio A y el Ejercicio B que se describen a continuación.

Ejercicio A: Evitar que el tráfico del servicio de **ECHO** (puerto TCP 7) desde un host específico (estación de trabajo con dirección IP 172.20.xxx.3, donde xxx es 40,48,56,64, etc, según sea tu red) conectada al switch Fast-Ethernet de la interfaz f0/0 de tu router, alcance tu red vecina hacia la derecha (p. ej., desde 172.20.40.3 no se debe poder ejecutar el servicio de ECHO frente a un servidor situado en la subred 172.20.48.0 que cuelga de Barcelona, pero sí se debe poder ejecutar frente a un servidor situado en cualquier otra red; además, cualquier otro servicio debe de poder funcionar normalmente).

Ejercicio B: Evitar que el tráfico del servicio **DAYTIME** (puerto TCP 13) desde un host específico (estación de trabajo con dirección IP 172.20.xxx.3, donde xxx es 40,48,56,64, etc, según sea tu red) conectada al switch Fast-Ethernet de la interfaz f0/0 de tu router, alcance tu red vecina hacia la derecha.

Tarea 2. Configuración de una ACL IP Extendida

Paso 1. Determinar los requisitos de la ACL. En particular, decidir en qué router y a qué interfaz debe ser aplicada la ACL. Como ahora se utilizan ACL extendidas y se pueden filtrar la dirección origen y destino, se puede aplicar el filtro lo más cerca posible del origen, lo que ahorra ancho de banda. ¿A qué router y a qué interfaz se puede aplicar la ACL para cada uno de los ejercicios de ejemplo, A o B?

Paso 2. Desarrollar la ACL. Definir las sentencias ACL en modo Router(config)#. Recordad que las sentencias de una misma ACL son aditivas. Cada sentencia se agrega a la ACL. Si hay más de una sentencia en la ACL (lo que es típico) y se desea cambiar una sentencia anterior, se debe borrar la ACL y comenzar de nuevo. En estos ejemplos se bloquean paquetes desde sólo una dirección de host IP o una red. Como las ACL siempre terminan con un "deny any" implícito, si se utilizan una de las sentencias anteriores esto haría que esta lista denegara una sola dirección origen, pero también denegaría implícitamente cualquier otra dirección origen. Nuestro objetivo es sólo denegar el acceso desde un solo host, de manera que es necesario agregar una segunda sentencia para permitir todo el tráfico restante.

Paso 3. Verificar las sentencias en la ACL. Utilice el siguiente comando ***show access-list*** *número-lista* para controlar sus sentencias y verificar que todo se haya escrito correctamente. Si desea corregir un error o hacer un cambio en una sentencia existente se debe eliminar la ACL y comenzar de nuevo. ¿Cuántas sentencias hay en la ACL?

Paso 4 - Aplicar la ACL a una interfaz de router. Se debe recordar que se puede decidir aplicar la ACL a los paquetes entrantes o salientes. A menos que se especifique

IN (entrante), la ACL se aplica sólo a los paquetes OUT (salientes) (IN y OUT siempre se consideran desde fuera del router).

Paso 5. Verificar si la ACL se aplica a la interfaz correcta. El comando **show ip interface** muestra información de interfaz IP e indica si se ha establecido alguna ACL. ¿Cuáles fueron los resultados que demuestran que la ACL se ha aplicado correctamente?.

Paso 6. Verificar que la ACL funcione correctamente. Pruebe la ACL intentando hacer ECHO o DAYTIME desde el host origen que se debe denegar.

8. ACL Nombradas

Las ACL nombradas permiten que las ACL IP estándar y extendidas se identifiquen con una cadena alfanumérica (nombre) en lugar de la representación numérica actual (1 a 199). Las ACL nombradas se pueden usar para eliminar entradas individuales de una ACL específica. Esto permite modificar sus ACL sin eliminarlas y luego reconfigurarlas. Se usan las ACL nombradas cuando:

- Se desea identificar intuitivamente las ACL utilizando un nombre alfanumérico.
- Existen más de 99 ACL simples y 100 extendidas que se deben configurar en un router para un protocolo determinado.

Tenga en cuenta lo siguiente antes de implementar las ACL nombradas:

- Las ACL nombradas no son compatibles con las versiones de Cisco IOS anteriores a la versión 11.2.
- No se puede usar el mismo nombre para múltiples ACL. Además, las ACL de diferentes tipos no pueden tener el mismo nombre. Por ejemplo, no es válido especificar una ACL estándar llamada Jorge y una ACL extendida con el mismo nombre.

Para nombrar la ACL, se utiliza el siguiente comando:

Router(config)# **ip access-list** {**standard** | **extended**} nombre

En el modo de configuración de ACL, se especifica una o más condiciones de permitir o denegar. Esto determina si el paquete debe pasar o debe descartarse:

Router(config {std- | ext-}nacl)# **deny | permit** {source [source-wildcard] | **any**}

Se usa la forma **no** de este comando para eliminar una condición de una ACL.

El ejemplo siguiente es una ACL nombrada estándar denominada **Internetfilter**:

ip access-list standard Internetfilter

deny 192.5.34.0 0.0.0.255

permit 128.88.0.0 0.0.255.255

permit 36.0.0.0 0.255.255.255

(Nota: cualquier otro acceso está implícitamente denegado)

Tarea 3. Diseño y planificación de un plan de seguridad

Esta práctica de laboratorio es un ejercicio que simula una situación de la realidad. Se trabaja con múltiples listas de control de acceso extendidas (ACL) para simular la regulación del tráfico al que se permite pasar a través de múltiples routers a varios servidores e Internet. Este es un ejercicio para practicar el análisis de los requisitos de seguridad y diseñar un plan de ACL. Se pueden configurar la mayoría de las ACL en los routers indicados, pero no se pueden probar en realidad algunas de las capacidades de filtrado de las ACL en algunos casos. Por ello, debes desarrollar este plan de seguridad por escrito indicando claramente la configuración de cada ACL, y dónde debe aplicarse (router, interfaz, sentido ***in*** ó ***out***). Entrégaselo al profesor de prácticas en el plazo que te indique.

En esta práctica de laboratorio **se diseña un plan de seguridad** que utiliza múltiples ACL extendidas y determinará dónde se deben aplicar sobre la base de la siguiente configuración de laboratorio estándar. Puede haber más de una respuesta correcta.

Paso 1 - Definir los requisitos de la ACL.

A continuación se suministran los requisitos y algunos supuestos para esta práctica de laboratorio. En general es mejor intentar usar la menor cantidad posible de listas de acceso y tener en cuenta el potencial de crecimiento de la red. En este ejercicio se usan ACL extendidas.

Supongamos que sus servidores empresariales se ubican en la red 172.20.56.0 (desde Valencia).

1. Se debe permitir acceso a través de la Web (protocolo http) a su servidor web 172.20.56.80 para cualquier persona
2. Se debe permitir el acceso a través de DNS a su servidor DNS 172.20.56.53
3. Se debe permitir que el personal docente tenga pleno acceso desde la red 172.20.72.0 a cualquiera de estos servidores.
4. No se debe permitir otro acceso a ningún servidor en la red 172.20.56.0

Suponga que todos los estudiantes se encuentran en la red 172.20.48.0, y se desea controlar el acceso hacia o desde esa red. Supongamos que el router Madrid le pertenece a su ISP y no tiene control sobre él.

1. NO se debe permitir que los estudiantes usen FTP a Internet (¡posibles problemas de virus!)
2. Se debe permitir que los estudiantes tengan cualquier otro tipo de acceso a Internet
3. Se debe permitir que los estudiantes tengan acceso a la red del cuerpo docente 172.20.72.0 para pasar mensajes de correo electrónico (SMTP)
4. Se debe denegar a los estudiantes cualquier otro tipo de acceso a la red del cuerpo docente 172.20.72.0

Paso 2. Desarrollar una o más ACL. Agrupe las sentencias según sus características comunes y la ubicación donde usted considera que se debe aplicar la ACL. Intente crear la menor cantidad posible de ACL y mantener la flexibilidad.

Paso 3. Aplicar y verificar las ACL con los routers del laboratorio (si están disponibles). Puede que no sea posible probar todas las capacidades de filtrado de las ACL, ya que no dispondrá de un servidor HTTP o DNS o acceso a Internet, pero se puede probar la mayor parte del filtrado. Recuerde que sólo se puede aplicar una ACL por protocolo (como IP) por dirección (entrante o saliente (IN or OUT)).