

**LISTAS DE CONTROL DE ACCESO (ACL) Y CONTROL DE  
ACCESO BASADO EN EL CONTEXTO (CBAC):  
GENERALIDADES Y GUÍA PRÁCTICA**

**CAMILO ANDRÉS MELÉNDEZ CAMPIS  
JESÚS ANDRÉS TOUS TEJADA**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR  
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA  
PROGRAMA DE INGENIERÍA ELECTRÓNICA  
CARTAGENA DE INDIAS D. T. Y C.**

**2012**

**LISTAS DE CONTROL DE ACCESO (ACL) Y CONTROL DE  
ACCESO BASADO EN EL CONTEXTO (CBAC):  
GENERALIDADES Y GUÍA PRÁCTICA**

**CAMILO ANDRÉS MELÉNDEZ CAMPIS  
JESÚS ANDRÉS TOUS TEJADA**

**Trabajo de monografía presentado como requisito para optar al título de  
Ingeniero Electrónico**

**DIRECTOR  
ING. RICARDO J. ARJONA ANGARITA**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR  
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA  
PROGRAMA DE INGENIERÍA ELECTRÓNICA  
CARTAGENA DE INDIAS D. T. Y C.**

**2012**

**NOTA DE ACEPTACIÓN:**

---

---

---

---

---

**Firma del Presidente del Jurado**

---

**Firma del Jurado**

---

**Firma del Jurado**

Cartagena de Indias D. T. y C., Junio de 2012

Señores

**COMITÉ CURRICULAR**

Facultad de Ingeniería Eléctrica y Electrónica

Universidad Tecnológica de Bolívar

**Respetados señores:**

De la manera más atenta nos dirigimos a ustedes, con el propósito de informarles que la monografía titulada “**LISTAS DE CONTROL DE ACCESO (ACL) Y CONTROL DE ACCESO BASADO EN EL CONTEXTO (CBAC): GENERALIDADES Y GUÍA PRÁCTICA**” ha sido desarrollada conforme a los objetivos establecidos.

Como autores de la monografía consideramos que el trabajo es satisfactorio y solicitamos sea estudiado, evaluado y posteriormente aprobado por ustedes.

En espera de los resultados de dicha evaluación.

Atentamente,

---

Camilo A. Meléndez Campis  
CC No 1.047.428.459  
de Cartagena

---

Jesús Andrés Tous Tejada  
CC No 1.143.354.394  
de Cartagena

Cartagena de Indias D. T. y C., Junio de 2012

Señores

**COMITÉ CURRICULAR**

Facultad de Ingeniería Eléctrica y Electrónica

Universidad Tecnológica de Bolívar

Cordial Saludo.

A través de la presente me permito poner en consideración para su respectiva evaluación, la monografía titulada **“LISTAS DE CONTROL DE ACCESO (ACL) Y CONTROL DE ACCESO BASADO EN EL CONTEXTO (CBAC): GENERALIDADES Y GUÍA PRÁCTICA”**, la cual fue realizada por los estudiantes CAMILO ANDRES MELENDEZ CAMPIS y JESÚS ANDRÉS TOUS TEJADA, a quienes asesoré en su ejecución.

Atentamente;

---

RICARDO J. ARJONA ANGARITA

Asesor de Monografía

## **AUTORIZACIÓN**

Cartagena de Indias D. T. y C., Junio de 2012

Yo, **CAMILO ANDRES MELENDEZ CAMPIS**, identificado con cedula de ciudadanía No 1.047.428.459 de Cartagena, autorizo a la **UNIVERSIDAD TECNOLÓGICA DE BOLIVAR**, para hacer uso de mi monografía y publicarlo en el catalogo en línea de la biblioteca

Atentamente;

---

CAMILO ANDRES MELENDEZ CAMPIS  
CC No 1.047.428.459 de Cartagena

## **AUTORIZACIÓN**

Cartagena de Indias D. T. y C., Junio de 2012

Yo, **JESÚS ANDRÉS TOUS TEJADA**, identificado con cedula de ciudadanía No 1.143.354.394 de Cartagena, autorizo a la **UNIVERSIDAD TECNOLÓGICA DE BOLIVAR**, para hacer uso de mi monografía y publicarlo en el catalogo en línea de la biblioteca

Atentamente;

---

JESÚS ANDRÉS TOUS TEJADA  
CC No 1.143.354.394 de Cartagena

## LISTA DE FIGURAS

**Figura 1.** Aplicación de ACL

**Figura 2.** Ejemplo de configuración de una lista de acceso reflexiva.

**Figura 3.** Funcionamiento del CBAC

**Figura 4.** Funcionamiento del CBAC

**Figura 5.** Un host IP utiliza los bits de código SYN y ACK para llevar a cabo la conexión de tres vías TCP.

**Figura 6.** Ejemplo: firewall de dos interface

**Figura 7.** Esquema de red

**Figura 8.** Esquema de red

**Figura 9.** Ventana de configuración DNS

**Figura 10.** Datos del DNS

**Figura 11.** Configuración Usuarios Email en el servidor

**Figura 12.** Ventana de configuración email

**Figura 13.** Montaje implementado de las dos primeras guías prácticas.

**Figura 14.** *Router* Cisco serie 2800

**Figura 15.** *Switch* D-Link DES-1008D



## LISTA DE TABLAS

**Tabla 1.** Ejemplo de ACL con máscara

**Tabla 2.** Resumen de las ACL

**Tabla 3.** Resumen de ACL

**Tabla 4.** Número de las listas de acceso Cisco IOS

**Tabla 5.** Operación de las ACL en referencia al modelo OSI

**Tabla 6.** Los filtros CBC basados en las capas OSI 5 y 7.

**Tabla 7.** Familia de comandos show ip inspect

**Tabla 8.** Direcciones IP interfaces routers

**Tabla 9.** Direcciones IP Hosts

**Tabla 10.** Datos de configuración ACL

**Tabla 11.** Datos ubicación ACL

**Tabla 12.** Comandos ACL caso 1

**Tabla 13.** Comandos ACL caso 2

**Tabla 14.** Direcciones IP interfaces routers

**Tabla 15.** Direcciones IP Hosts

**Tabla 16.** Datos para configurar el servicio de email en los host

**Tabla 17.** Datos de configuración ACL

**Tabla 18.** Comandos ACL extendida

**Tabla 19.** Datos de configuración ACL extendida

## TABLA DE CONTENIDO

<i>Introducción</i>	11
<i>Objetivos</i>	12
1.0 Listas de control de acceso	13
2.0 Uso de máscaras en las ACL	15
3.0 Resumen de las ACL	16
4.0 Procesamiento de las ACL	19
5.0 Aplicación de las ACL	20
6.0 Edición de las ACL	22
7.0 Reparación de las ACL	23
8.0 Tipos de ACL	25
8.1 ACL estándar	26
8.2 ACL extendidas	28
8.3 ACL reflexivas	32
8.4 CBAC	35
8.4.1 Funcionamiento del CBAC	38
8.4.2 Protocolos soportados por el CBAC	41
8.4.3 Configuración del CBAC	44
8.4.3.1 Paso 1: Establecer pistas y alertas de auditoría	44
8.4.3.2 Paso 2: Establecer interrupciones y umbrales globales	45
8.4.3.3 Paso 3: Definición de la asignación de puesto	46
8.4.3.4 Paso 4: Definición de las reglas de inspección	47
8.4.3.5 Paso 5: Aplicación de la reglas de inspección y de las ACL a las interfaces del <i>router</i>	48
8.4.3.6 Paso 6: Prueba y verificación	52
Guía Práctica 1: Configuración de ACL estándar empleando Packet Tracer	54
Guía Práctica 2: Configuración de ACL extendida utilizando Packet Tracer	61
Guía Práctica 3: Configuración de CBAC empleando Packet Tracer	73

## INTRODUCCIÓN

A medida que crece el uso y la importancia de las actividades empresariales a través de internet, las aplicaciones y los servicios basados en las redes representan mayores riesgos para la información de los individuos y de las empresas. Muchas veces la prisa por conectarse provoca que la seguridad de la red se vea comprometida. La información es un bien de suma importancia, sin la protección o la seguridad adecuada de la red, muchos individuos, empresas y gobiernos ponen en riesgo la confidencialidad de su información.

Los *routers* y *switches* soportan una gran variedad de servicios de red que permiten a los usuarios conectarse a la misma, algunos de estos servicios pueden restringirse o desactivarse, lo que mejora la seguridad sin que la operación de la red se vea afectada, sin embargo aunque esto representa un nivel básico de aseguramiento de red, lo cierto es que, muchos administradores de red ni siquiera aplican este procedimiento, el cual debería ser una práctica común.

Es necesario que los administradores de red manejen los conceptos básicos de seguridad de redes, y que estén al tanto de que en aras de conseguir una mayor seguridad, además de desactivar algunos servicios, también pueden filtrar paquetes en el tráfico de entrada y el de salida mediante ACL (Listas de Control de Acceso), lo que permitirá a los administradores reducir una gran cantidad de amenazas a la red sin que el tráfico productivo se vea afectado.

## OBJETIVOS

### OBJETIVO GENERAL

Elaborar guías prácticas de estudio para estudiantes de ingeniería inclinados hacia el área de las comunicaciones a cerca de los conceptos básicos de seguridad de redes y en especial de la utilización de *routers* para asegurar la red mediante es uso de listas de control de acceso (ACL) y control de acceso basado en el contexto (CBAC).que facilite la comprensión, aprendizaje y aplicación de estos conceptos.

### OBJETIVOS ESPECIFICOS

- Elaborar guías prácticas para la configuración de listas de acceso estándar y extendidas utilizando Packet Tracer™, de manera que facilite la familiarización y aprendizaje de los temas a tratar de la manera más clara y rápida posible.
- Desarrollar metodologías para la configuración de listas de control de acceso basado en contexto (CBAC) utilizando Packet Tracer™ haciendo énfasis en los conceptos básicos acerca de las listas de acceso y su aplicación en la resolución de problemas.

## 1.0 Listas de control de acceso y CBAC

Las ACL se utilizan para filtrar y asegurar el tráfico de las redes. Las ACL filtran el tráfico de la red controlando si los paquetes enrutados o conmutados se han enviado o bloqueado en la interfaz. Estos paquetes son examinados para determinar cómo deben manipularse en función de los criterios establecidos por la ACL.

CBAC proporciona un mayor nivel de seguridad debido a que examina el tráfico de las capa 3 y superiores. El CBAC se utiliza además de las ACL. Los paquetes que entran en el *firewall* sólo son inspeccionados por el CBAC si primero pasan la ACL de entrada de la interfaz. Si la ACL rechaza un paquete, éste simplemente se descarta y no es inspeccionado por el CBAC.

Antes de entrar en los detalles relacionados con el procesamiento y la configuración de las ACL, es necesario conocer los tipos de ACL más comunes:

- **ACL estándar.** Es el tipo de ACL más antiguo, y data de la versión 8.3 del software Cisco IOS. Este tipo de ACL controla el tráfico comparando la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL.
- **ACL extendidas.** Aparecieron en la versión 8.3 del software Cisco IOS. Controlan el tráfico comparando las direcciones de origen y de destino de los paquetes IP con las direcciones configuradas en la ACL.
- **ACL dinámicas (lock-and-key).** Aparecieron en la versión 11.1 del software Cisco IOS. Esta característica depende de Telnet, la autenticación (local o remota) y las ACL extendidas. La configuración *lock-and-key* empieza con la aplicación de una ACL extendida para bloquear el tráfico acerca del *router*. Los usuarios que quieren atravesar el *router* son bloqueados por la ACL

extendida hasta que hacen *telnet al router* y son autenticados. Después se cierra la conexión telnet y la ACL extendida existente permitirá tráfico durante un breve periodo de tiempo en particular (son posibles las interrupciones ociosas y absolutas).

- **ACL Ip con nombre.** Aparecieron en la versión 11.2 del software Cisco IOS. Permite asignar nombres en lugar de números a las ACL estándar y extendidas.
- **ACL reflexivas.** Aparecieron en la versión 11.3 del software Cisco IOS. Permiten el filtrado de los paquetes IP en función de la información de la sesión de capa superior. Generalmente se usan para permitir el tráfico saliente y para limitar el entrante en respuesta a las sesiones originadas dentro del *router*.
- **Control de acceso basado en contexto (CBAC).** Apareció con la versión 12.0.2.T del software Cisco IOS y requiere el Cisco IOS *firewall*. El CBAC inspeccionará el tráfico que viaja a través del *firewall* para descubrir y administrar la información de estado para las sesiones de los protocolos de control de la transmisión (TCP) y de datagrama de usuario (UDP). Esa información de estado se utiliza para crear aperturas temporales en las listas de acceso del *firewall*.

Cada tipo de ACL filtra el tráfico de la red controlando si los paquetes enrutados o conmutados fueron enviados o bloqueados en el *router* o en la interfaz del *switch*. El *router* o el *switch* examinan cada uno de los paquetes para determinar si debe enviarlo o rechazarlo, basándose en los criterios especificados en la ACL. Dichos criterios pueden ser la dirección de origen del tráfico, la dirección de destino del mismo, o el protocolo de capa superior. Una ACL se construye en dos simples pasos:

- **Paso 1.** Crear una ACL.
- **Paso 2.** Aplicar la ACL.

Finalmente, además de definir orígenes y destinos ACL, puede definir puertos, tipos de mensaje ICMP (Internet Control Message Protocol, Protocolo de Mensajes de Control en Internet) y otros parámetros.

## **2.0 USO DE MÁSCARAS EN LAS ACL**

Las máscaras se utilizan con las direcciones IP en las ACL para especificar lo que debe permitirse y lo que debe rechazarse.

Cuando el valor de una máscara se divide en código binario, compuesto por unos y ceros, el resultado determina los bits de las direcciones que deben tenerse en cuenta a la hora de procesar el tráfico. Un 0 indica que los bits de la dirección requieren una coincidencia exacta para ser tenidos en consideración. Un 1 en la máscara indica que debe ignorarse el bit correspondiente de la dirección.

Teniendo en cuenta la Tabla 1, suponga que todo el tráfico que empieza con 10.1.1 debe ser coincidente para que el tráfico sea procesado. Basándose en la máscara binaria, puede ver que los primeros tres conjuntos, u octetos, deben coincidir exactamente con la dirección de red binaria dada. Los últimos conjuntos de números son ignorados (.11111111). Por tanto, todo el tráfico que empieza con una dirección de origen 10.1.1 coincidirá por que el último octeto es ignorado. Con esta máscara se procesarán las direcciones de red 10.1.1.1 a 10.1.1.255 (10.1.1.x).

La máscara inversa ACL también se puede determinar sustrayendo la máscara normal de 255.255.255.255. En el siguiente ejemplo, la máscara inversa queda determinada por la dirección de red 172.16.1.0 con una máscara normal de 255.255.255.0.

**Tabla 1.** Ejemplo de ACL con máscara

Parte de dirección de red/host	Valor
Dirección de red (tráfico que se procesará)	10.1.1.0
Máscara <i>wildcard</i>	0.0.0.255
Dirección de red (binaria)	00001010.00000001.00000001.00000000
Máscara (binaria)	00000000.00000000.00000000.11111111

Así se determina la máscara inversa ACL:

**255.255.255.255**

**255.255.255.0** (máscara normal)

**0.0.0.255** (máscara inversa)

### 3.0 RESUMEN DE LAS ACL

Las máscaras de subred también se pueden representar por medio de una notación de longitud fija. Por ejemplo, 192.168.10.0/24 representa 192.168.10.0 255.255.255.0. Otros ejemplos de notaciones abreviadas son las siguientes:

- El origen/*wildcard* de origen de 0.0.0.0/255.255.255.255 significa “cualquiera”.
- El origen/*wildcard* de 10.1.1.2 / 0.0.0.0 es lo mismo que “*host* 10.1.1.2”

¿Cómo se puede resumir un intervalo de redes en una sola red con el fin de optimizar la ACL?. Considere las siguientes direcciones:



- 192.168.32.0/24
- 192.168.33.0/24
- 192.168.34.0/24
- 192.168.35.0/24
- 192.168.36.0/24
- 192.168.37.0/24
- 192.168.38.0/24
- 192.168.39.0/24

Los primeros dos octetos y el último octeto son iguales en todas la redes. Lo que sigue es una explicación de cómo pueden resumirse todos los octetos en una sola red.

Como muestra la Tabla 2, el tercer octeto de las redes anteriores puede escribirse de acuerdo con la posición del bit del octeto y el valor de dirección de cada bit.

**Tabla 2.** Resumen de las ACL

Decimal	128	64	32	16	8	4	2	1
32	0	0	1	0	0	0	0	0
33	0	0	1	0	0	0	0	1
34	0	0	1	0	0	0	1	0
35	0	0	1	0	0	0	1	1
36	0	0	1	0	0	1	0	0
37	0	0	1	0	0	1	0	1
38	0	0	1	0	0	1	1	0
39	0	0	1	0	0	1	1	1

Como los primeros cinco bits coinciden, las ocho redes se pueden resumir en una sola red: 192.168.32.0/21 ó 192.168.32.0 255.255.248.0. Las ocho posibles combinaciones de los tres bits menos de orden inferior son

relevantes para los intervalos de red en cuestión. El siguiente comando define una ACL que permite esta red. Al sustraer 255.255.248.0, una máscara normal, de 255.255.255.255 se obtiene 0.0.7.255. La sintaxis de esta configuración es la siguiente:

```
access-list acl_permit ip 192.168.32.0 0.0.7.255
```

Como otro ejemplo, considere el siguiente conjunto de redes:

- 192.168.146.0/24
- 192.168.147.0/24
- 192.168.148.0/24
- 192.168.149.0/24

Los primeros dos octetos y el último son idénticos en todas las redes. El tercer octeto del conjunto de redes se puede escribir como se muestra en la Tabla 3, de acuerdo con la posición del bit en el octeto y el valor de dirección de cada bit.

**Tabla 3.** Resumen de ACL

Decimal	128	64	32	16	8	4	2	1
146	1	0	0	1	0	0	1	0
147	1	0	0	1	0	0	1	1
148	1	0	0	1	0	1	0	0
149	1	0	0	1	0	1	0	1

A diferencia del conjunto de direcciones de red del ejemplo anterior, estas redes no pueden resumirse en una sola red; en cambio, ocuparán un mínimo de dos redes.

- Para las redes 192.168.146.x y 192.168.147.x, todos los bits coinciden excepto el último, que puede ignorarse. Puede escribirse como 192.168.146.0/23 ó 192.168.146.0 255.255.254.0.
- Para las redes 192.168.148.x y 192.168.149.x, todos los bits coinciden excepto el último, que puede ignorarse. Puede escribirse como 192.168.148.0/23 ó 192.168.148.0 255.255.254.0.

El siguiente código define una ACL resumida para las redes anteriores:

```
access-list 10 permit ip 192.168.146.0 0.0.1.255  
access-list 10 permit ip 192.168.148.0 0.0.1.255
```

## 4.0 PROCESAMIENTO DE LAS ACL

Para que las ACL funcionen con eficacia, deben planificarse de forma lógica. La clave para crear las ACL óptimas está en un entendimiento sólido de cómo se procesan las ACL. Esta sección explica en detalle el procesamiento de las ACL.

Las ACL son procesadas en el orden en que son introducidas en la lista ACL. Por ello, los administradores deben colocar las entradas más frecuentemente utilizadas en la parte superior de la lista. Al hacerlo así, se reduce el tiempo de procesamiento y es más eficaz la administración del *router*.

Además todas las ACL incluyen una sentencia *deny* implícita para el tráfico no permitido. Una ACL de una sola entrada, únicamente con una entrada *deny*, tiene como efecto debido a la sentencia *deny* implícita. En la ACL 101 la sentencia *deny all* es implícita y en la ACL 102 se define explícitamente la sentencia *deny all*:

```
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 102 deny ip any any
```

El siguiente ejemplo ilustra la importancia de la colocación adecuada de las ACL. En este caso, es suficiente con la última entrada. Las tres primeras no son necesarias por que tcp incluye Telnet, e IP incluye TCP, UDP e ICMP.

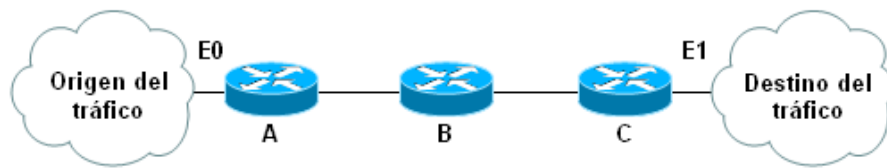
```
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

## 5.0 APLICACIÓN DE LAS ACL

Las ACL pueden definirse sin aplicarlas. Para crear una ACL operativa y activa, la ACL debe aplicarse a la interfaz del *router*.

Las ACL extendidas permiten que el administrador de la red permita o deniegue el tráfico que fluye desde un puerto o unas direcciones IP específicas hasta un puerto o direcciones IP de destinos dados. Esta capacidad permite al administrador de la red ser mucho más específico en lo referente al tráfico que puede pasar por la red.

Las ACL extendidas deben aplicarse a la interfaz más cercana al origen del tráfico. Para bloquear el tráfico de un origen hacia un destino específico, aplique una ACL entrante a E0 del *router* A en lugar de una lista saliente a E1 del *router* C, como se muestra en la figura:



**Figura 1.** Aplicación de ACL

El tráfico del router puede compararse con un viaje internacional. Pongamos por caso que un oficial de aduanas quiera impedir que ciertos pasajeros tomen un vuelo desde Frankfurt, Alemania (el origen), con destino a París, Francia (el destino). La detención podría efectuarse en el aeropuerto de Frankfurt, a modo de bloqueo de salida, o en el aeropuerto de París, como bloqueo de entrada. En este caso es mejor que el bloqueo se efectúe en el aeropuerto de Frankfurt para ahorrar recursos. Al igual que ocurren en un viaje internacional, es mejor que un router autorice o rechace el tráfico lo más cerca posible del origen.

A continuación tiene unas definiciones simplificadas de “saliente” y “entrante”:

- **Salida.** Tráfico que ya ha atravesado el router y está abandonando la interfaz. El origen sería el lugar donde el tráfico ya ha estado; a saber, el otro lado del router. El destino es donde va.
- **Entrada.** Tráfico que está llegando a la interfaz y que pasará por el router. El origen sería el lugar donde el tráfico ya ha estado. El destino es a donde va; a saber, el otro lado del router.

Una vez determinado el tipo de ACL que debe definirse, el siguiente paso es determinar la ACL que debe aplicarse. Como se explicó anteriormente, una ACL puede definirse sin que se aplique. No se procesará tráfico mientras no se aplique una ACL a la interfaz. Como muestra el siguiente

ejemplo, con el comando ***ip access-group***, se aplica una lista de acceso a una interfaz.

**Router# configure Terminal**

**Enter configuration commands, one per line. End with CNTL/Z.**

**Router(config)# interface E0**

**Router(config)# ip access-group 101 in**

**Router(config)# ^Z**

## **6.0 EDICIÓN DE LAS ACL**

La edición o modificación de una ACL requiere una atención especial. Por ejemplo, si el administrador borrara una línea específica de una ACL numerada existente, se borraría la ACL entera. Y cualesquiera condiciones adicionales que hicieran los administradores se anotarían al final de la ACL. Para modificar las ACL numeradas, copie la configuración del router en un servidor TFTP (Trivial File Transfer Protocol, Protocolo Trivial de Transferencia de Archivos) en un editor de texto, como, por ejemplo, el Bloc de notas; a continuación, introduzca los cambios y copie la configuración de nuevo en el router.

En un entorno de producción, la modificación de cualquier ACL podría afectar a la seguridad del router durante el proceso de edición. El uso del Bloc de notas, es una estrategia más segura para modificar las listas de acceso.

Para cambiar o eliminar una ACL de una interfaz, utilice la siguiente sintaxis:

**interface *interfaz***

**no ip access-group # in | out**

Para eliminar una ACL, el usuario debe entrar en el modo de configuración y escribir no delante del comando **access-group**, como se muestra en el siguiente ejemplo:

```
router# configure Terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# interface E0
router(config-if)# no ip access-group 101 in
router(config-if)# ip access-group 102 in
router(config-if)# ^Z
```

## 7.0 REPARACIÓN DE LAS ACL

Si se detecta que se está rechazando demasiado tráfico, estudie la lógica de la ACL o intente definir y aplicar una lista adicional más amplia. El comando **show ip access-lists** proporciona una cuenta de paquetes mostrando la entrada ACL que está en uso.

Con la palabra clave *log* al final de las entradas ACL individuales se muestra el número de ACL y si el paquete fue autorizado o rechazado, además de la información específica del puerto, como se ve a continuación:

```
access-list 101 permit ip any host 10.2.6.6 log
access-list 101 permit ip host 10.2.6.6 any log
```

Para ver el registro, utilice el comando **show logging**. Recuerde que puede configurar los mensajes de registro para ser enviados al buffer local o a un servidor *syslog*.

Los siguientes pasos explican el proceso de depuración. Antes de empezar, no olvide comprobar si existen otras ACL. Si encuentra alguna, bórrrela. Además, asegúrese de que está desactivada la conmutación rápida. La conmutación rápida es una característica que permite un

rendimiento mayor mediante la conmutación de un paquete utilizando una caché creada por la transferencia de paquete inicial. Los *routers* ofrecen el mejor rendimiento en la transferencia de paquetes cuando la conmutación rápida está activada. La conmutación rápida está activada de forma predeterminada en todas las interfaces que soportan este tipo de conmutación. Debe tener un cuidado extremo a la hora de depurar un sistema con mucho tráfico.

Si se necesita la depuración de una ACL, puede hacerse, pero asegurándose de que el proceso y el tráfico fluyen. Para implementar la depuración a nivel de paquete, siga estos pasos:

**Paso 1.** Capture los datos deseados utilizando el comando ***access-list***. En el siguiente ejemplo, la captura de datos se establece para la dirección de destino 10.2.6.6 o la dirección de origen 10.2.6.6.

```
access-list 101 permit ip any host 10.2.6.6
access-list 101 permit ip host 10.2.6.6 any
```

**Paso 2.** Desactive la conmutación rápida en las interfaces implicadas. Si la conmutación rápida no está desactivada sólo verá el primer paquete.

```
config-if
no ip route-cache
```

**Paso 3.** Para visualizar la salida del comando ***debug*** y los mensajes de error del sistema de la terminal y la sesión actuales, ejecute el comando ***terminal monitor*** en el modo autorizado (enable).

**Paso 4.** Inicie el proceso de depuración con el comando ***debug ip packet 101*** o ***debug ip packet 101 detail***. El ejemplo a continuación muestra una salida de ejemplo de la lista de acceso ***debug ip packet 101***



**Paso 5.** Para detener el procesote depuración, ejecute el comando no *debug all* en el modo autorizado, y el comando de configuración *interface*.

**Paso 6.** Vuelva a activar la conmutación rápida:

**config interface**

**ip route-cache**

El siguiente ejemplo ofrece una salida de ejemplo del comando ***debug ip packet***. La salida muestra dos tipos de mensajes que este comando puede producir: La primera línea de la salida describe un paquete IP que el router envía, y la tercera línea de la salida describe un paquete que es rechazado.

**IP packet debbuging i son**

**IP: s=10.2.6.6 (Ethernet0), d=172.69.1.6 (Serial2), g=172.69.16.2, forward**

**IP: s=172.69.1.57 (Serial2), d=10.2.6.6 (Serial2), g=172.69.16.2, forward**

**IP: s=172.69.1.57 (Serial2), d=10.36.125.2 (Ethernet1), g=172.69.16.2, access denied**

## 8.0 TIPOS DE ACL

Hay muchos tipos de ACL para filtrar el tráfico:

- ACL estándar
- ACL extendidas
- ACL IP con nombre.
- Entradas de ACL IP comentadas
- ACL reflexivas
- ACL basadas en el tiempo utilizando intervalos de tiempo.
- *Proxy* de autenticación.
- ACL turbo.
- ACL basadas en el contexto
- ACL distribuidas basadas en el tiempo.
- ACL criptográficas (*crypto*)

- La tabla siguiente proporciona el estándar de numeración de las listas de acceso en función de sus tipos.

**Tabla 4.** Número de las listas de acceso Cisco IOS

Listas de acceso	Descripción del número
1 a 99	Lista de acceso IP estándar
100 a 199	Lista de acceso IP extendida
200 a 299	Lista de acceso de protocolo de tipo código
300 a 399	Lista de acceso DECnet
400 a 499	Lista de acceso estándar XNS
500 a 599	Liste de acceso extendida XNS
600 a 699	Lista de acceso AppleTalk
700 a 799	Lista de acceso de dirección MAC de 48 bits
800 a 899	Lista de acceso estándar IPX
900 a 999	Lista de acceso extendida IPX
1000 a 1099	Lista de acceso IPX SAP
1100 a 1199	Lista de acceso de dirección MAC de 48 bits extendida
1200 a 1299	Lista de acceso de dirección resumida IPX
1300 a 1999	Lista de acceso estándar IP(intervalo expandido)
2000 a 2699	Lista de acceso extendida IP (intervalo expandido)

## 8.1 ACL estándar

La ACL estándar es el tipo de ACL más antiguo. Las ACL estándar controlan el tráfico comparando la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL. El formato de una ACL estándar es el siguiente:

```
access-list número-lista-acceso { permit | deny } { host / origen wildcard-origen / any }
```

En todas las versiones del software, el parámetro *número-lista-acceso* puede ser cualquier número de 1 a 99. En la versión 12.0.1 del software

Cisco IOS, las ACL estándar empiezan utilizando números adicionales de 1300 a 1999. Estos números adicionales se denominan ACL IP expandidas. La versión 11.2 del software Cisco IOS añadió la capacidad de utilizar un nombre de la lista en las ACL estándar.

En las primeras versiones del software, el valor predeterminado era lo “saliente” en caso de no especificar la palabra clave *out* o *in*. En las versiones posteriores del software debía especificarse la dirección. Recuerde que una configuración *origen/wildcard*-origen de 0.0.0.0 255.255.255.255 también puede escribirse como *any*. El *wildcard* puede omitirse si se compone únicamente de ceros. Por tanto, 10.1.1.2 0.0.0.0 es lo mismo que *host* 10.1.1.2.

La sintaxis para aplicar una ACL a una interfaz es la siguiente:

```
router(config)# interface interfaz número  
router(config-if)# ip access-group número { in | out }
```

El ejemplo siguiente muestra el uso de una ACL estándar para bloquear todo el tráfico excepto el que procede de 10.1.1.x.

```
router(config)# access-list 1 permit 10.1.1.0 0.0.0.255  
router(config-if)# ip address 10.1.1.1 255.255.255.0  
router(config-if)# ip access-group 1 in
```

Por su parte el ejemplo a continuación muestra la creación de una lista de acceso estándar y su aplicación a la interfaz del tráfico de Internet entrante. La lista de acceso rechaza todo el tráfico entrante de Internet que contiene una dirección de origen de las direcciones de la RFC 1918<sup>1</sup> reservadas conocidas y permite cualquier otro tráfico procedente de Internet hasta el campus corporativo.

```
router(config)# access-list 9 deny 127.0.0.0 0.255.255.255
```

---

<sup>1</sup> La RFC 1918 es la norma que rige el espacio de direcciones IP para una red privada en particular.

```
router(config)# access-list 9 deny 10.0.0.0 0.255.255.255
router(config)# access-list 9 deny 172.16.0.0 0.240.255.255
router(config)# access-list 9 deny 192.168.0.0 0.0.255.255
router(config)# access-list 9 permit any
```

**!Apply the access-list 9 to the incoming Internet interface**

```
router(config)# interface Serial 0/0
router(config-if)# description to the internet
router(config-if)# ip address 161.71.73.33 255.255.255.248
router(config-if)# ip access-group 9 in
```

## 8.2 ACL extendidas

Las ACL extendidas controlan el tráfico comparando las direcciones de origen y destino de los paquetes IP con las direcciones configuradas en la ACL. Para las listas de acceso extendidas IP pueden definirse varios protocolos bien conocidos. El formato de comando de las ACL extendidas es el siguiente:

Para IP:

```
access-list número-lista-acceso { dynamic nombre-dinámico [ timeout minutos ] }
{ deny | permit } ip origen wildcard-origen destino wildcard-destino. [ precedente
precedence ] [ tos tos ] [ log | entrada-registro ] [ time-range nombre-intervalo-
tiempo ]
```

Para ICMP:

```
access-list número-lista-acceso { dynamic nombre-dinámico [ timeout minutos ] }
{ deny | permit } icmp origen wildcard-origen destino wildcard-destino. [
precedente precedence ] [ tos tos ] [ log | entrada-registro ] [ time-range nombre-
intervalo-tiempo ]
```

Para TCP:

```
access-list número-lista-acceso { dynamic nombre-dinámico [ timeout minutos ] }  
{ deny | permit } tcp source source-wildcard [ operator [port] ] destination  
destination-wildcard [ operator [port] ] [ established ] [ precedence precedence ] [ tos  
tos ] [ log | log-input ] [ time-range nombre-intervalo-tiempo ]
```

Las ACL extendidas se utilizan con frecuencia para probar condiciones porque proporcionan una gama de control más amplia que las ACL estándar. Una ACL extendida puede utilizarse para permitir el tráfico web y rechazar el tráfico FTP o Telnet procedente de las redes que no son de la empresa. Las ACL extendidas comprueban tanto la dirección de origen como de destino del paquete. También pueden comprobar protocolos específicos, número de puerto y otros parámetros. Los paquetes pueden permitirse o rechazarse basándose en el lugar donde se originaron o en su destino. Una vez definida la ACL, debe aplicarse a la interfaz, entrante o saliente, de la siguiente forma:

```
Interface interfaz número  
ip access-group { número | nombre } { in | out }
```

Utilice la siguiente sintaxis de commando para configurar *lock-and-key* con autenticación, como se muestra la siguiente sintaxis de comando:

```
username nombre-usuario password contraseña  
interface interfaz  
ip Access-group { número | nombre } { in | out }
```

La ACL de una sola entrada en el comando se añadirá dinámicamente a la ACL existente después de la autenticación, como se muestra en la siguiente sintaxis de comando:

```

access-list número-lista-acceso dynamic nombre { permit | deny } [ protocolo ] {
origen wildcard-destino | any} [precedence precedencia ] [tos tos] [established]
[log | entrada-registro] [operador puerto-destino | destino puerto]
line vty interval_línea
login local

```

El ejemplo siguiente muestra una ACL *lock-and-key* (dinámica) básica. Después de que el usuario de 10.1.1.2 realice una conexión Telnet a 10.1.1.1, se aplica la ACL dinámica. La conexión se cierra entonces y el usuario puede ir a la red 172.16.1.x.

```

username test password 0 test
!--- 10 (minutos) es la interrupcion por inactividad
username tst autocommand Access-enable host timeout 10
interface Ethernet 0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
access-list 101 permit tcp any host 10.1.1.1 eq telnet
!--- 15(minutos) es la interrupción absoluta
access-list 101 dynamic testlist timeout 15 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255
line vty 0 4
login local

```

¿Cuándo es adecuado utilizar *lock-and-key*? Dos escenarios generales garantizan una configuración ACL general:

- El permiso es necesario para un usuario, o grupo de usuarios, a fin de acceder con seguridad a un *host* de una red protegida vía Internet. *Lock-and-key* autentica al usuario y después permite un acceso limitado a través del *router firewall*, pero sólo para el *host* o subred de esa persona, y sólo por un periodo de tiempo finito.
- Ciertos usuarios de una red remota tienen que acceder a un *host* de la red corporativa protegido por un *firewall*. *Lock-and-key* requiere que los usuarios se autenticuen antes de permitirles el acceso a los *host* protegidos.

Los siguientes pasos resumen el funcionamiento de *lock-and-key*:

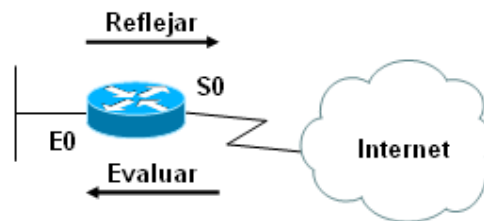
1. Un usuario abre una sesión Telnet a un *router firewall* configurado para *lock-and-key*. El usuario conecta vía uno de los vtys del *router*.
2. El usuario Cisco IOS recibe el paquete Telnet, abre una sesión Telnet, solicita al usuario un nombre de usuario y una contraseña, y lleva a cabo el proceso de autenticación. La autenticación puede realizarla el *router* o un servidor de control del acceso como, por ejemplo, TACAS+ (Terminal Access Controller Access Control System Plus, Sistema de control de acceso al controlador de acceso al terminal) o RADIUS ( Remote Authentication Dial-In User Service, servicio de usuario con acceso remoto por marcación).
3. Cuando un usuario pasa la autenticación, se le desconecta de la sesión Telnet, y el software crea una entrada temporal en la lista de acceso dinámica. Dependiendo de la configuración, esa entrada temporal puede limitar el intervalo de redes al que el usuario tiene acceso temporal.
4. El usuario intercambia datos a través del agujero en el *firewall*.
5. El IOS borra la entrada de la lista de acceso temporal cuando se alcanza una interrupción configurada o cuando el administrador del sistema la borra manualmente. La interrupción configurada puede ser por inactividad o absoluta. La entrada de la lista de acceso temporal no se elimina automáticamente cuando el usuario termina una sesión, permanece hasta que se alcanza la interrupción o hasta que el administrado del sistema la borra.

Las versiones del software Cisco IOS anteriores a la 11.1 no son compatibles con las listas de acceso dinámicas. Por tanto si utiliza un archivo de configuración que incluye una lista de acceso dinámica con

alguna de esas versiones antiguas, la lista de acceso resultante no se interpretará correctamente, lo que podría provocar graves problemas de seguridad.

### 8.3 ACL reflexivas

Las ACL reflexivas (véase Figura 2) permiten que se filtren los paquetes IP en base a la información de sesión de la capa superior. En esta figura, puede colocarse una ACL reflexiva en la interfaz externa (S0) de RTA de modo que pueda evaluarse el tráfico entrante antes de que entre al *router*.



**Figura 2.** Ejemplo de configuración de una lista de acceso reflexiva.

Un requisito común del filtrado es permitir el tráfico IP para las sesiones originadas dentro de la red, pero rechazar el tráfico IP para las sesiones originadas en el exterior de la red. Mediante el uso de ACL extendidas básicas, los administradores pueden aproximar el filtrado de la sesión utilizando la palabra clave *established* con el comando *permit*. Dicha palabra clave filtra los paquetes TCP basándose en si están establecidos los bits ACK o RST. Este método de utilizar la palabra clave *established* sólo está disponible para el protocolo ICMP, los administradores tendrían que permitir todo el tráfico entrante o definir todos los pares de direcciones origen/destino *host/puerto* aceptables posibles para cada protocolo.



Las ACL reflexivas son mucho más adecuadas para el verdadero filtrado de la sesión. Una vez configurada una ACL reflexiva, se activa cuando una sesión de capa superior IP nueva, como TCP o UDP, se inicia desde el interior de la red con un paquete que viaja a la red exterior, como muestra la siguiente sintaxis de comando:

```
router(config)# interface interfaz numero
router(config-if)# ip access-group { número | nombre }{ in | out }
router(config-if)#ip access-list extended nombre
router(config-ext-nacl)# permit protocolo any any reflect nombre [ timeout
segundos]

router(config)# ip access-list extended nombre
router(config-ext-nacl)# evaluate nombre
```

Cuando se activa, la ACL reflexiva genera una entrada temporal nueva. Esta entrada permite que el tráfico entre la red siempre y cuando forme parte de la sesión. Pero no permitirá la entrada en la red del tráfico que no es parte de la sesión. El criterio del filtro está basado en los bits ACK y RST, además de en las direcciones de origen y destino y los números de puerto. El filtrado de la sesión utiliza filtros temporales que se eliminan cuando la sesión termina. Esta acción limita a una franja de tiempo más pequeña la posibilidad de sufrir el ataque de un pirata informático.

Las entradas ACL reflexivas temporales (ACE) se eliminan al final de la sesión. Para las sesiones TCP, la entrada se elimina 5 segundos después de que se hayan detectado dos bits FIN establecidos, o inmediatamente después de una coincidencia de un paquete TCP con el bit RST establecido. Dos bits FIN establecidos en una sesión indican que esa sesión está a punto de terminar. La ventana de cinco segundos permite un cierre de sesión más amigable. Un bit RST indica un cierre brusco de la sesión. De forma alternativa, la entrada temporal se elimina una vez no se detecten paquetes de la sesión durante un periodo de tiempo configurable. Es lo que se conoce como periodo de inactividad.

Para UDP y otros protocolos sin conexión, el final de una sesión UDP se determina de forma distinta que en el caso del final de una sesión TCP. Como se considera que UDP es sin conexión, no existe información de seguimiento de la sesión incrustada en los paquetes. Por tanto, se considera que el final de una sesión se produce cuando no se detectan paquetes de la sesión durante el periodo de tiempo de inactividad.

Hay dos restricciones al uso de las listas de acceso reflexivas:

- Las listas de acceso reflexivas sólo se pueden definir con las lista de acceso IP con nombre extendidas. Los administradores no pueden definir listas de acceso reflexivas con las listas de acceso IP con nombre numeradas o estándar, o con otras listas de acceso de protocolo.
- Las listas de acceso reflexivas no funcionan con algunas aplicaciones que utilizan números de puerto que cambian durante una sesión. Si los números de puerto de un paquete de retorno son diferentes que los del paquete originario, el paquete de retorno será rechazado, incluso si el paquete forma parte realmente de la misma sesión. FTP, una aplicación basada en TCP, es un ejemplo de aplicación con números de puerto cambiantes.

Con las listas de acceso reflexivas, si una solicitud FTP se inicia desde el interior de una red, la solicitud no se completará. En cambio, la red debe utilizar FTP pasivo en esta situación.

## 8.4 Control de acceso basado en contexto (CBAC)

El control de acceso basado en el contexto (CBAC) examina el tráfico que viaja a través del *firewall* para descubrir y administrar la información de estado para las sesiones TCP y UDP. Esta información de estado se utiliza para crear aperturas temporales en las listas de acceso del *firewall*. Estas aperturas se crean configurando listas *ip inspect* en la dirección del flujo del tráfico para permitir el tráfico de retorno y las conexiones de datos adicionales para las sesiones admisibles. Las sesiones admisibles son las sesiones originadas en el interior de una red protegida.

La sintaxis de CBAC es la siguiente:

```
ip inspect name nombre-inspección protocolo [ timeout segundos ]
```

El ejemplo 3.17 muestra el uso de CBAC para inspeccionar el tráfico saliente. La ACL 111 extendida normalmente bloquearía el tráfico de retorno, al contrario que ICMP, sin apertura de huecos CBAC para dicho tráfico.

```
ip inspect name myfw ftp timeout 3600  
ip inspect name myfw http timeout 3600  
ip inspect name myfw tcp timeout 3600  
ip inspect name myfw udp timeout 3600  
ip inspect name myfw tftp timeout 3600  
  
interface Ethernet0/1  
    ip address 172.16.1.2 255.255.255.0  
    ip access-group 111 in  
    ip inspect myfw out  
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo  
access-list 111 permit icmp any 10.1.1.0 0.0.0.255
```

Antes de explorar con más profundidad el CBAC, debe tener claro los siguientes conceptos básicos sobre las ACL tradicionales:

- Las ACL terminan con una sentencia *deny any* implícita.
- Si en una interfaz no hay ACL configuradas, se permiten de forma predeterminada todas las conexiones.
- Las ACL proporcionan el filtrado del tráfico en la capa de red utilizando lo siguiente:
  1. Direcciones IP de origen y destino.
  2. Puertos de origen y destino.
- Las ACL pueden utilizarse para implementar un *firewall* de filtrado.
- Las ACL abren puertos permanentes para permitir el tráfico, lo que genera una vulnerabilidad en la seguridad.
- Las ACL no funcionan con aplicaciones que negocian dinámicamente con los puertos.

El CBAC proporciona a los usuarios una protección mejor ante los ataques que las ACL típicas, una lista con los protocolos que soporta, descripciones de las funciones de alerta y seguimiento de las auditorías añadidas, y una lista de las tareas de configuración del CBAC. El CBAC crea aperturas temporales en las listas de acceso de las interfaces del *firewall*. Dichas aperturas se producen cuando el tráfico especificado sale de la red interior a través del *firewall*. El CBAC permite que el tráfico regrese a través del *firewall* sólo si forma parte de la misma sesión que el tráfico original que activó el CBAC cuando salía del *firewall*.

**Tabla 5.** Operación de las ACL en referencia al modelo OSI

Capa	Operaciones ACL
Aplicación (capa 7)	-
Presentación (capa 6)	-
Sesión (capa 5)	-
Transporte (capa 4)	Protocolos: TCP, UDP. ACL extendida: filtros en los protocolos de origen y destino/número de puerto.
Red (capa 3)	Protocolos: IP, ICMP, IGMP ACL estándar: filtros en la dirección IP de origen ACL extendida: filtros en las direcciones IP de origen y destino.
Enlace de datos (capa 2)	Filtrado MAC ACL estándar: filtros en la dirección MAC de origen. ACL extendida: filtros en las direcciones MAC de origen y destino.
Física (capa 1)	-

Como se mencionó anteriormente, en la configuración del CBAC están implicadas las siguientes tareas, que se explicarán a continuación:

**Paso 1.** Establecer las pistas y alertas de auditoría.

**Paso 2.** Establecer las interrupciones globales y los umbrales.

**Paso 3.** Definir la PAM.

**Paso 4.** Definir las reglas de inspección.

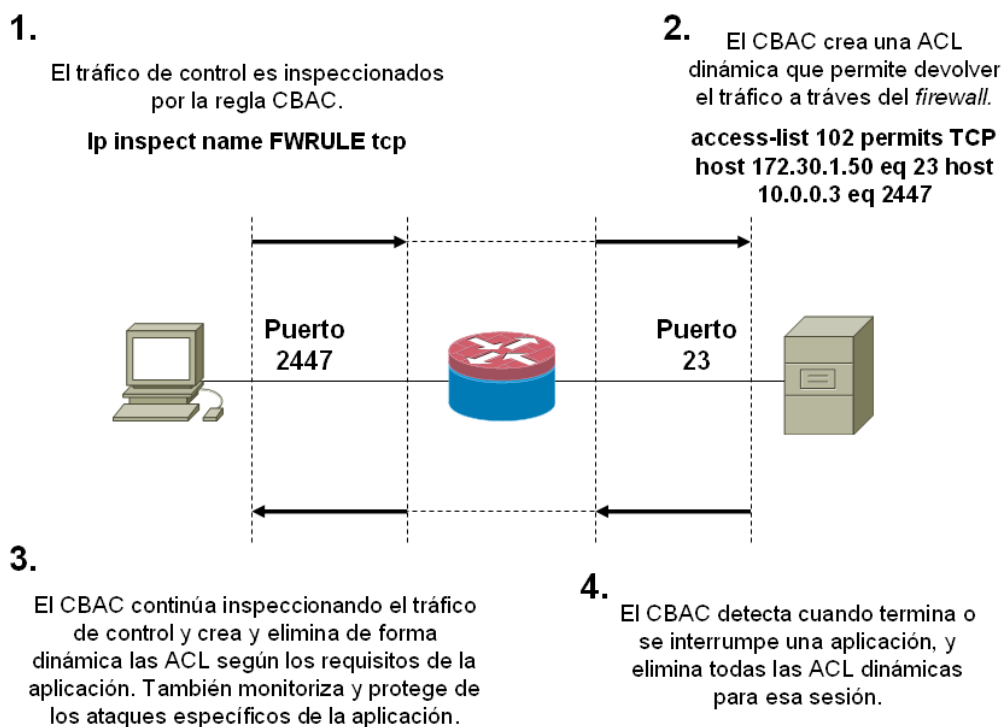
**Paso 5.** Aplicar las reglas de inspección y las ACL a las interfaces.

**Paso 6.** Probar y verificar

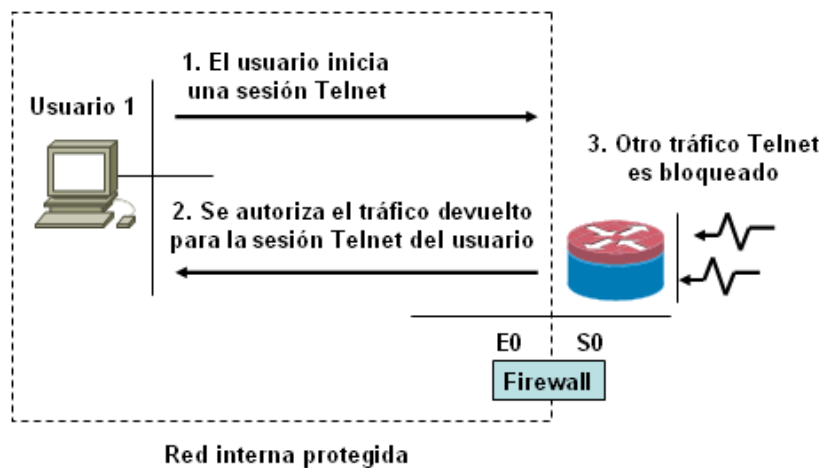
### 8.4.1 Funcionamiento del CBAC

El CBAC especifica los protocolos que se inspeccionarán, así como la interfaz y la dirección de la interfaz, tanto de entrada como de salida, donde se origina la inspección. Únicamente los protocolos especificados serán inspeccionados por el CBAC. Las figuras 3 y 4. Los paquetes que entran en el *firewall* sólo son inspeccionados por el *firewall* si antes pasan la ACL entrante de la interfaz. Si la ACL rechaza un paquete, simplemente se descarta y no es inspeccionado por el CBAC.

El CBAC inspecciona y monitoriza sólo los canales de control de las conexiones. Los canales de datos no son inspeccionados. El software CBAC analiza los comandos y las respuestas FTP. Por ejemplo, durante las sesiones FTP, tanto los canales de control como los de datos (que se crean al transferirse un archivo de datos) son monitorizados en busca de cambios de estado, pero el CBAC sólo inspecciona el canal de control.



**Figura 3.** Funcionamiento del CBAC



**Figura 4.** Funcionamiento del CBAC

La inspección realizada por el CBAC reconoce los comandos específicos de la aplicación, como los comandos SMTP ilegales, en el canal de control, y detecta y previene ciertos ataques a nivel de aplicación. El CBAC rastrea los números de secuencia de todos los paquetes TCP y rechaza los paquetes cuyos números de secuencia no están dentro de los intervalos esperados. Cuando el CBAC sospecha de un ataque, la función de denegación de servicio (DoS) puede llevar a cabo las siguientes acciones:

- Generar mensajes de alerta
- Proteger los recursos del sistema que podrían obstaculizar el rendimiento.
- Bloquear los paquetes de los atacantes sospechosos.

El CBAC utiliza los valores de interrupción y umbral para manipular la información de estado. Utiliza dicha información para ayudar a determinar cuándo han de derivarse las sesiones que se establecen completamente. El establecimiento de valores de interrupción para las sesiones de red ayuda a prevenir los ataques del tipo Dos al liberar recursos del sistema. Estos valores logran este objetivo derivando sesiones después de un

periodo específico de tiempo. El establecimiento de valores de umbral para las sesiones de red ayuda a prevenir los ataques DoS mediante el control del número de sesiones semiabiertas, lo que limita la cantidad de recursos del sistema aplicados a las sesiones semiabiertas. Cuando una sesión es derivada, el CBAC envía un mensaje de reinicio a los dispositivos de ambos extremos (origen y destino) de la sesión. Cuando el sistema se encuentra bajo un ataque DoS y recibe un comando de reinicio, libera o desbloquea los procesos y recursos relacionados con esa sesión incompleta.

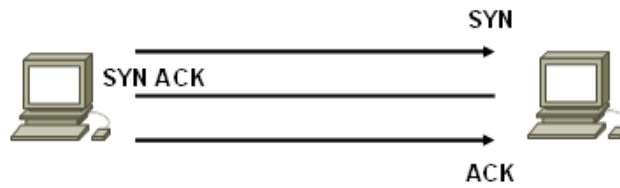
El CBAC proporciona tres umbrales contra los ataques DoS:

- El número total de sesiones TCP o UDP abiertas.
- El número de sesiones semiabiertas basadas en el tiempo.
- El número de sesiones sólo de TCP entreabiertas por *host*.

Si se excede un umbral, el CBAC tiene dos opciones:

- El CBAC envía un mensaje de reinicio a los puntos finales de la sesión semiabierta más antigua, quedando los recursos disponibles para dar servicio a los paquetes recién llegados.
- En el caso de las sesiones sólo TCP entreabiertas, el CBAC bloquea temporalmente todos los paquetes SYN durante el tiempo configurado por el valor de umbral. Cuando el *router* bloquea un paquete SYN, nunca se inicia el establecimiento de conexión de tres vías (véase la Figura 5), lo que impide al *router* utilizar recursos de memoria y procesamiento que son necesarios para las conexiones correctas.





**Figura 5.** Un host IP utiliza los bits de código SYN y ACK para llevar a cabo la conexión de tres vías TCP.

La detección y prevención de ataques DoS requieren la creación de una regla de inspección CBAC, que se aplica a una interfaz. La regla de inspección debe incluir los protocolos que se monitorizarán contra los ataques DoS. Por ejemplo, si en la regla de inspección está activada la inspección de TCP, entonces el CBAC puede rastrear todas las conexiones TCP en busca de los ataques DoS. Si la regla de inspección incluye la inspección del protocolo FTP pero no la inspección de TCP, el CBAC sólo rastrea las conexiones FTP en busca de los ataques DoS.

Una tabla de estado conserva la información de estado de la sesión. Siempre que un paquete es inspeccionado, se actualiza una tabla de estado para incluir la información sobre el estado de la conexión de paquete. Sólo se permitirá el paso de tráfico de retorno por el *firewall* si la tabla de estado contiene información indicando que el paquete pertenece a una sesión admisible. La inspección controla el tráfico que pertenece a una sesión válida y envía el tráfico que no reconoce. Cuando el tráfico de retorno es inspeccionado, se actualiza la información de la tabla de estado cuando es necesario.

#### 8.4.2 Protocolos soportados por el CBAC

Una razón por la que el CBAC es una poderosa herramienta para controlar los flujos de tráfico es que soporta la inspección del tráfico en las capas de sesión y de aplicación del modelo de referencia OSI. Las

siguientes secciones explican la inspección del tráfico en estos dos niveles.

### **Inspección de la capa de sesión**

Puede configurar el CBAC para que inspeccione todas las sesiones TCP, independientemente del protocolo de la capa de aplicación. En ocasiones, este método recibe el nombre de inspección TCP de un solo canal o inspección TCP genérica. También es posible configurar el CBAC para que inspeccione las sesiones UDP, con independencia del protocolo de la capa de aplicación. Este método también se conoce como inspección UDP de un solo canal o inspección UDP genérica.

### **Inspección de los protocolos de la capa de aplicación**

También es posible configurar el CBAC para que inspeccione los protocolos específicos de la capa de aplicación. La siguiente tabla ilustra los protocolos de dicha capa que se pueden configurar para el CBAC.

**Tabla 6.** Los filtros CBC basados en las capas OSI 5 y 7.

Capa OSI	Lo que se puede filtrar
Aplicación	VDOLiveRPC (Sun RPC, no DCE RPC)
	Microsoft RPC
	FTP
	TFTP
	Comandos UNIX R (por ejemplo rlogin, rexec, rsh)
	SMTP
	Java
	SQL*Net
	RSTP
	H.323 (por ejemplo NetMeeting, CUseeMe)
Presentación	-
Sesión	Todas las sesiones TCP, independientemente del protocolo de la capa de aplicación.
	En ocasiones recibe el nombre de inspección TCP de un solo canal o inspección TCP genérica.
	Todas las sesiones UDP, independientemente del protocolo de la capa de aplicación.
	En ocasiones recibe el nombre de inspección UDP de un solo canal o inspección UDP genérica.
Transporte	-
Red	-
Enlace de datos	-
Física	-

Cuando se configura un protocolo para el CBAC, se inspecciona el tráfico de ese protocolo y se guarda la información de estado. En general, se permite a los paquetes regresar y atravesar el *firewall* sólo si pertenecen a una sesión admisible.

## 8.4.3 Configuración del CBAC

### 8.4.3.1 Paso 1: Establecer pistas y alertas de auditoría.

Una característica útil del CBAC es su capacidad de generar alertas y pistas de auditoría, lo que hace más eficaces y efectivas la monitorización y el seguimiento de los eventos de seguridad predefinidos. El proceso de rastreo y alerta de auditoría funciona de la siguiente forma:

1. El CBAC genera alertas y pistas de auditoría en tiempo real en función de los eventos rastreados por el *firewall*.
2. Las funciones mejoradas de rastreo de la auditoría utilizan el *syslog* para rastrear todas las transacciones de la red a la vez que graban las marcas de tiempo, el *host* de origen, el *host* de destino, los puertos utilizados y el número de bytes transmitidos para el informe avanzado basado en la sesión.
3. Las alertas en tiempo real envían mensajes de error *syslog* a las consolas de administración centrales al detectar actividad sospechosa.

Observe que al utilizar las reglas de inspección CBAC puede configurar alertas e información de rastreo de la auditoría sobre una base de protocolo por aplicación. Por ejemplo, para generar información de rastreo de auditoría para el tráfico HTTP, simplemente especifique en la regla CBAC lo que le gustaría hacer en cuanto a cubrir la inspección HTTP. El siguiente ejemplo ilustra el procedimiento:

```
router(config)# ip inspect audit-trail
! Activa el servidor syslog y el registro
router(config)# logging on
router(config)# logging 10.0.0.3
router(config)# ip inspect audit-trail
router(config)#
[no] ip inspect alert-off
```

### 8.4.3.2 Paso 2: Establecer interrupciones y umbrales globales

El CBAC utiliza interrupciones y umbrales para determinar durante cuánto tiempo administrar la información de estado para una sesión y para determinar cuándo derivar sesiones que no se establecen completamente. Estas interrupciones y umbrales se aplican globalmente a todas las sesiones.

Puede utilizar los valores de interrupción y umbral predeterminados o cambiarlos por valores más adecuados a los requisitos de seguridad de la red. Cualquier cambio en los valores de interrupción y umbral debe realizarse antes de continuar con la configuración del CBAC. Tal como se muestra a continuación:

```
router1>enable
password:
password:
Router1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router1(config)#ip inspect tcp synwait-time 30
Router1(config)#ip inspect tcp finwait-time 5
Router1(config)#ip inspect tcp idle-time 3600
Router1(config)#ip inspect udp idle-time 5
Router1(config)#ip inspect dns-timeout 5
Router1(config)#ip inspect max-incomplete high 500
Router1(config)#ip inspect max-incomplete low 400
Router1(config)#ip inspect one-minute high 500
Router1(config)#ip inspect one-minute low 400
Router1(config)#ip inspect tcp max incomplete host 50 block-time 0
Router1(config)#ip ^Z
```

### 8.4.3.3 Paso 3: Definición de la asignación de puerto a la aplicación

Después de completar las dos primeras tareas de configuración del CBAC, debe establecer la asignación de puerto a la aplicación (PAM, Port to Application Mapping).

PAM activa la personalización de los números de puerto TCP o UDP para las aplicaciones o servicios de res. PAM utiliza esta información para soportar entornos de red que ejecutan servicios utilizando puertos que son diferentes de los puertos registrados o bien conocidos asociados a una aplicación.

Con la información de puerto, PAM establece en el *firewall* una tabla de información de asignación de puertos a las aplicaciones. La información de la tabla PAM permite que los servicios soportados por el CBAC se ejecuten en puertos no estándar. Anteriormente, el CBAC se limitaba a inspeccionar el tráfico utilizando únicamente los puertos bien conocidos o registrados asociados a una aplicación. PAM permite a los administradores de redes personalizar el control de acceso a la red en cuanto a servicios y aplicaciones específicas.

PAM también soporta la asignación de un puerto específico del *host* o de la subred, lo que permite la aplicación de PAM a un solo *host* o subred mediante ACL estándar, como lo muestra el siguiente ejemplo:

```
Router1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router1(config)#! Configure Port to Application Mapping
Router1(config)#ip port-map http port 8000
Router1(config)#ip ^Z
```

#### 8.4.3.4 Paso 4: Definición de las reglas de inspección

El CBAC permite la inspección del tráfico en las capas de sesión y aplicación del modelo OSI; sin embargo, para que el CBAC funcione, debe saber qué tráfico debe inspeccionar. Las reglas de inspección se utilizan para definir las aplicaciones que el CBAC inspeccionará. Es preciso definir reglas de inspección para especificar qué tráfico IP, o qué protocolos de la capa de aplicación, deben ser inspeccionados por el CBAC en una interfaz. Normalmente, sólo se define una regla de inspección. La única excepción se podría dar si el CBAC está activado en las dos direcciones en una sola interfaz de *firewall*. En este caso, deben configurarse dos reglas, una para cada dirección.

Una regla de inspección debe especificar cada uno de los protocolos de la capa de aplicación deseados, además de los protocolos TCP o UDP genéricos, si así se desea. La regla de inspección consiste en una serie de sentencias; cada una de ellas enumera un protocolo y especifica el mismo nombre de regla de inspección. Las reglas de inspección también incluyen opciones para controlar los mensajes de rastreo y alerta de auditoría y para comprobar la fragmentación de paquetes IP.

Para definir un conjunto de reglas de inspección, utilice el comando ***ip inspect name*** en el modo de configuración global. Utilice la forma *no* de este comando para eliminar la regla de inspección para un protocolo o eliminar el conjunto entero de reglas de inspección. La sintaxis del comando ***ip inspect name*** es la siguiente:

```
Router(config)# ip inspect name nombre-inspección protocol [ alert { on | off } ] [ audit-trail { on | off } ] [ timeout segundos ]
```

El siguiente ejemplo muestra la configuración de reglas de inspección para los protocolos de aplicación: alertas y pistas de auditoría activadas.

```
Router(config)# ip inspect name FWRULE smtp alert on  
audit-trail timeout 300
```

```
Router(config)# ip inspect name FWRULE ftp alert on  
audit-trail on time out 300
```

#### **8.4.3.5 Paso 5: Aplicación de las reglas de inspección y de las ACL a las interfaces del *router***

Una vez familiarizado con las reglas de inspección y su configuración, debe aprender a aplicarlas a las interfaces del *router*. Ninguna regla de inspección será eficaz hasta que la aplique a una interfaz del *router*. Esta sección se centra en la aplicación de las reglas de inspección a las interfaces interiores y exteriores del *router* y también explica los comandos necesarios para ello. Además, de un ejemplo en el que se ilustran mejor las reglas de inspección; el cual muestra una topología sencilla que tiene un *router* de perímetro con dos interfaces, una hacia la red interna y otra hacia internet.

#### **Aplicación de reglas de inspección y ACL**

Para que el Cisco IOS Firewall sea eficaz, tanto las reglas de inspección como las ACL deben aplicarse estratégicamente a todas las interfaces del *router*. A continuación tiene unas normas generales para aplicar las reglas de inspección y ACL al *router*.

- En la interfaz donde se inicia el tráfico, aplique en la dirección interior la ACL que permita únicamente el tráfico deseado. Aplique en la dirección interior la regla que inspeccione ese tráfico deseado.
- En todas las interfaces, aplique en la dirección anterior la ACL que rechaza o deniega todo el tráfico excepto el tráfico no inspeccionado por el CBAC, como el ICMP.



Para aplicar a una interfaz un conjunto de reglas de inspección, utilice el comando ***ip inspect interface configuration***. Utilice la forma **no** de este comando para eliminar de la interfaz el conjunto de reglas.

La sintaxis del comando *ip inspect* es la siguiente:

```
Router(config)# ip inspect name nombre-inspeccion { in | out }
```

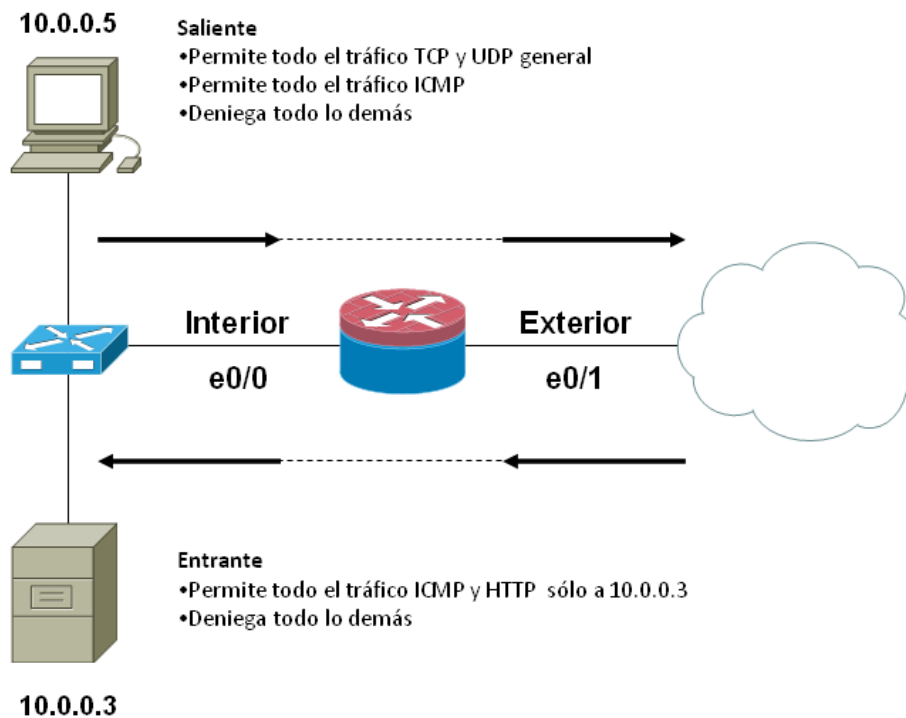
La ejecución de este commando aplica las reglas de inspección indicadas a una interfaz donde:

- *nombre-inspección* hace referencia al conjunto de reglas de inspección.
- *in* aplica las reglas de inspección al tráfico entrante.
- *out* aplica las reglas de inspección al tráfico saliente.

Para aplicar las reglas de inspección a la interfaz e0/0 en una dirección interior, debe configurar lo siguiente:

```
Router(config)# interface e0/0  
Router(config-if)# ip inspect FWRULE in
```

## Firewall de dos interfaces



**Figura 6.** Ejemplo: firewall de dos interfaces.

Para configurar el CBAC con el objetivo de que inspeccione el tráfico TCP y UDP, introduzca lo siguiente:

```
Router(config)# ip inspect name OUTBOUND tcp  
Router(config)# ip inspect name OUTBOUND udp
```

En base a la figura, para permitir el tráfico iniciado en el interior de la red 10.0.0.0, introduzca lo siguiente:

```
Router(config)# access-list 101 permit ip 10.0.0.0 0.0.0.255 any  
Router(config)# access-list 101 deny ip any any
```

Para aplicar una ACL y una regla de inspección a la interfaz interior en una dirección anterior, introduzca lo siguiente:

```
Router(config)# interface e0/0
Router(config-if)# ip inspect OUTBOUND in
Router(config-if)# ip access-group 101 in
```

Para configurar el CBAC a fin de que inspeccione el tráfico TCP, introduzca lo siguiente:

```
Router(config)# ip inspect name INBOUND tcp
```

Para permitir el tráfico ICMP y HTTP iniciado en el exterior al *host* 10.0.0.3, introduzca lo siguiente:

```
Router(config)# access-list 102 permit icmp any host 10.0.0.3
Router(config)# access-list 102 permit icmp tcp host 10.0.0.3 eq www
Router(config)# access-list 102 deny ip any any
```

En referencia a la figura, para aplicar una ACL y una regla de inspección a la interfaz saliente en una dirección interior, introduzca lo siguiente:

```
Router(config)# interface e0/1
Router(config-if)# ip inspect INBOUND in
Router(config-if)# ip access-group in
```

La implementación de la política de seguridad permitirá todo el tráfico saliente TCP y UDP general iniciado en el interior, desde la red 10.0.0.0, para acceder a Internet. Desde la misma red también será permitido el tráfico ICMP. El resto de redes del interior, que no están definidas, deben ser denegadas. Para el tráfico entrante iniciado en el exterior, se permite a todos acceder únicamente como ICMP y http al *host* 10.0.0.3. Cualquier otro tráfico debe ser denegado.

### 8.4.3.6 Paso 6: Prueba y verificación

Los administradores pueden utilizar la familia de comandos **show ip inspect** para probar y verificar una instalación del CBAC. La siguiente tabla muestra estos comandos.

**Tabla 7.** Familia de comandos show ip inspect

Comando	Propósito
<b>show ip inspect name <i>nombre-inspección</i></b>	Muestra una regla de inspección configurada en particular.
<b>show ip inspect config</b>	Muestra la configuración de inspección del CBAC completa.
<b>show ip inspect interfaces</b>	Muestra la configuración de la interfaz respecto a las reglas de inspección y listas de acceso aplicadas.
<b>show ip inspect session [detail]</b>	Muestra las sesiones existentes que el CBAC está rastreando e inspeccionando actualmente.
<b>show ip inspect all</b>	Muestra toda la configuración del CBAC y todas las sesiones existentes que el CBAC está rastreando e inspeccionando actualmente.

La sintaxis del comando **show ip inspect** se muestra en los ejemplos que aparecen a continuación.

Para visualizar las configuraciones del CBAC, las configuraciones de interfaz y las sesiones, utilice los siguientes comandos:

```
Router#  
show ip inspect name nombre-inspección  
show ip inspect config  
show ip inspect interfaces  
show ip inspect session [detail]  
show ip inspect all
```

Está página se dejó intencionalmente en blanco.

**GUIA PRÁCTICA 1**  
**CONFIGURACION DE ACL ESTANDAR EMPLEANDO**  
**PACKET TRACER**

**Objetivos:**

- Planificar y configurar ACL estándar para permitir o denegar tráfico específico.
- Verificar el funcionamiento de las ACL.

**Investigación previa:**

- Configuración básica de un router (dirección IP, interfaces, protocolos).
- ¿Qué es una ACL estándar?
- Configuración de una ACL estándar.

**Requerimientos:**

- Computador con sistema operativo Windows XP o superior
- Software Cisco Packet Tracer versión 5.3.1.

## CASO DE ESTUDIO

### Situación

Una EPS de la ciudad de Cartagena, se encuentra conectada con un puesto de salud de un municipio aledaño como se muestra en la figura 7. La entidad prestadora de salud ha tenido problemas de seguridad desde que se instaló la conexión con el puesto de salud. Por esto se hace necesario implementar unas ACL que permita el control del tráfico.

### Políticas de seguridad

- El host 4 representa el equipo del médico encargado del puesto de salud, el cual debe ser el único autorizado con acceso a la red de la EPS.
- El host 3 representa la parte de contabilidad de la EPS y es necesario limitar el tráfico solo a la red local.

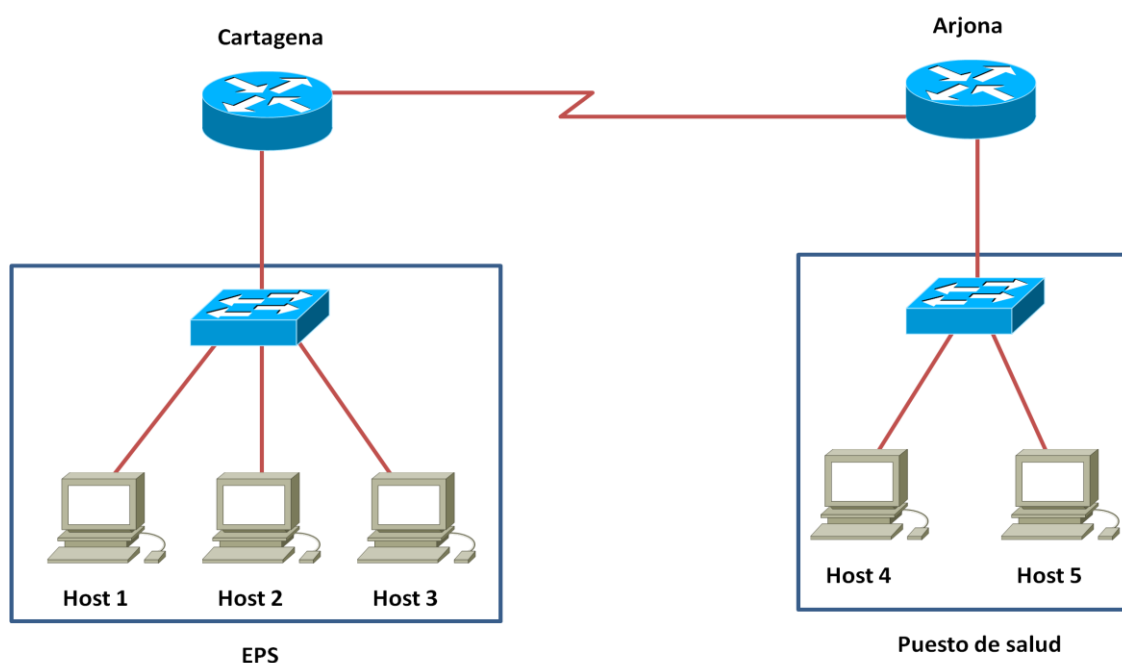


Figura 7. Esquema de la red

### Datos de configuración

La información necesaria para la configuración básica de los routers y los host se muestra consignada en las siguientes tablas:

**Tabla 8. Direcciones IP interfaces routers**

Router	FastEthernet 0/0	Serial 0/0	Tipo de Serial 0/0	Clock
Cartagena	192.184.20.1	200.150.10.1	DCE	56000
Arjona	192.184.50.1	200.150.10.2	DTE	

**Tabla 9. Direcciones IP Hosts**

Host	Dirección IP
1	192.184.20.2/24
2	192.184.20.3/24
3	192.184.20.4/24
4	192.184.50.2/24
5	192.184.50.3/24

### DESARROLLO DE LA PRÁCTICA

- 1) Realizar las interconexiones entre los diferentes elementos de red mostrados en la figura 7. De igual manera debe configurar los equipos de acuerdo a la información suministrada en las tablas 8 y 9.

**Nota:** no olvide configurar el protocolo RIP versión 1 para que se dé una comunicación transparente entre los routers.

- 2) Determinar los requisitos para las ALC, es necesario que tenga claro cuál es la lógica a aplicar para cada caso:



- **Caso 1:** se debe permitir el tráfico del Host 4 a la red de la EPS, pero se menciona que es el único autorizado, por lo que los demás hosts deben tener el tráfico limitado a la red local.
  - **Caso 2:** se debe limitar el tráfico del host 3 solo a la red local, sin afectar el tráfico de los demás equipos de la red.
- 3) Estructurar la lógica a aplicar en las ACL, es muy importante que tenga en cuenta cual es el orden de la lógica a aplicar para cada caso, además cual es la IP del o de los equipos que se encuentran involucrados en la política de seguridad.

- **Caso 1:** deny traffic from host 5  
permit traffic from host 4
- **Caso 2:** deny traffic from host 3  
permit all other traffic

a) Empleando esta lógica es posible estructurar las ACL. En la tabla 10 ingrese los datos de las respectivas ACL.

**Tabla 10. Datos de configuración ACL**

Caso	Descripción	Numero ACL	Permit/Deny	Dirección de origen	Mascara wildcard
1	Detenga el trafico del host 5				
1	Permita el trafico del host 4				
2	Detenga el trafico del host 3				
2	Permita el resto del trafico				

b) ¿Qué sucedería si se cambia el orden de las sentencias en cada ACL?

---

---

c) ¿Por qué es necesario especificar que se debe hacer con el resto del tráfico en cada ACL?

---

---

d) ¿Qué pasaría si no se especifica que hacer con el resto del tráfico en el caso 1?

---

---

Por último en el proceso de estructuración de las ACL, es necesario determinar la correcta ubicación para las listas de acceso en las interfaces de los routers.

**Nota:** Recuerde que las ACL estándar se ubican lo más cerca posible del destino.

e) Observe el diagrama de red mostrado en la figura 7 y seleccione los routers, las interfaces y las direcciones de tráfico (in, out) adecuadas. Ingrese la información en la tabla 11 que se muestra a continuación.

**Tabla 11. Datos ubicación ACL**

Caso	Router	Interfaz	Dirección de tráfico
1			
2			

- 4) Configure las ACL empleando el CLI (Comand Line Interface) en el modo de configuración global del router seleccionado para cada caso teniendo en cuenta la lógica y el orden planteado en el punto anterior:
- **Caso 1:** Para la configuración de esta ACL es necesario emplear los comandos mostrados en la tabla 12, reemplazando las palabras subrayadas por los respectivos valores:

**Tabla 12. Comandos ACL caso 1**

Logica	Comandos
deny traffic from host 5	access-list # deny <u>address</u> <u>wildcard</u>
permit traffic from host 4	access-list # permit <u>address</u> <u>wildcard</u>

- **Caso 2:** Como se menciona anteriormente para la configuración de esta ACL de igual manera es necesario emplear los comandos mostrados en la tabla 13, reemplazando las palabras y simbolos subrayados por los respectivos valores:

**Tabla 13. Comandos ACL caso 2**

Logica	Comandos
deny traffic from host 3	access-list # deny <u>address</u> <u>wildcard</u>
permit all other traffic	access-list # permit <u>address</u> <u>wildcard</u> *

\*En este caso la **address** o dirección de origen y la **wildcard** pueden ser reemplazadas por la palabra “any” ya que involucra al resto de equipos de la red.

- 5) Asigne las ACL previamente configuradas a la interfaz seleccionada para cada caso como se muestra en la tabla 11. Para realizar esto es necesario emplear la siguiente sintaxis en el CLI ( Comand Line Interface) en modo de configuración de interfaces:

```
interface type #/#  
ip access-group # (in/out)
```

- 6) Compruebe que las ACL se han configurado y asignado correctamente:
- a) Compruebe la correcta configuración de la ACL empleando el comando **show access-list** estando en modo de usuario privilegiado, el cual le mostrara toda la información referente a las ACL configuradas y asignadas en el router.
  - b) Verifique la funcionalidad de las ACL a través de el envío de paquetes para comprobar que se permitan o se nieguen los paquetes de acuerdo a las sentencias declaradas por las ACL. Realice este proceso con un ping.

**GUIA PRÁCTICA 2**  
**CONFIGURACION DE ACL EXTENDIDA EMPLEANDO**  
**PACKET TRACER**

**Objetivos:**

- Planificar y configurar ACL extendida para permitir o denegar tráfico específico, a nivel de protocolos y puertos.
- Verificar el funcionamiento de las ACL.

**Investigación previa:**

- Configuración básica de un router (dirección IP, interfaces, protocolos).
- Lista de puertos TCP/UDP
- ¿Qué es una ACL extendida?
- Configuración de una ACL extendida.

**Requerimientos:**

- Computador con sistema operativo Windows XP o superior
- Software Cisco Packet Tracer versión 5.3.1.

## CASO DE ESTUDIO

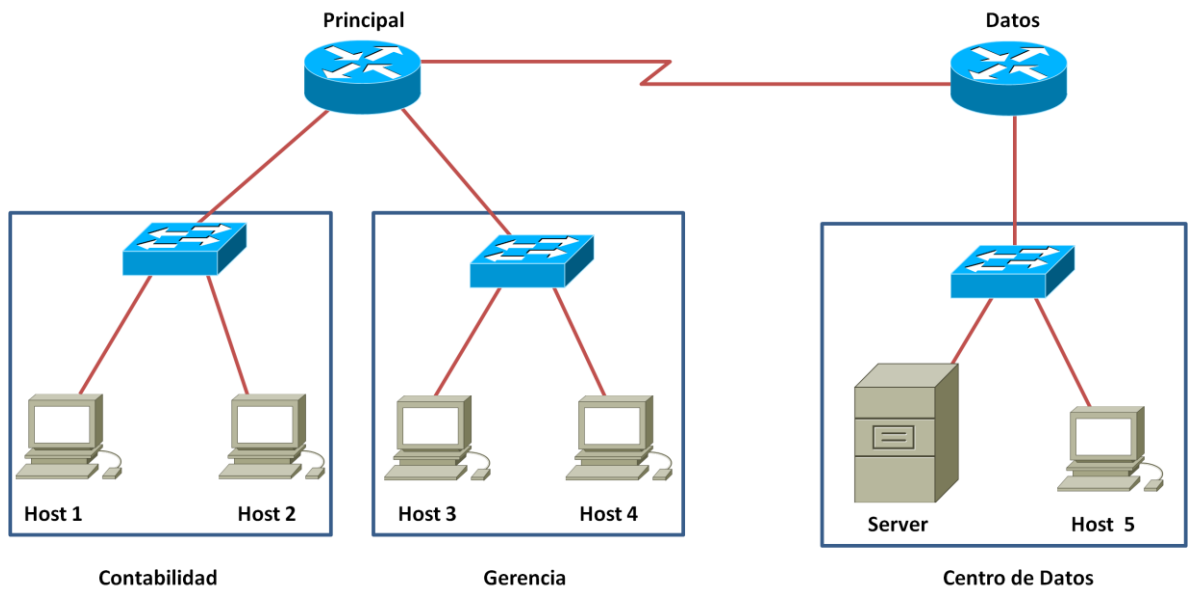
### **Situación**

EL banco de la Republica, presenta el esquema de red mostrado en la figura 8, en el que su red interna está conformada por dos departamentos (contabilidad y gerencia), interconectada con el centro de datos, el cual por seguridad se encuentra ubicado en otra parte de la ciudad y que proporciona acceso al servidor central.

En el banco se han presentado malos manejos de los servicios internos y perdida de información confidencial de cuentas bancarias, Por esta razón se hace necesario implementar unas ACL que permita el control de tráfico específico (protocolo y puerto) teniendo en cuenta el origen y el destino.

### **Políticas de seguridad**

- El host 3 representa el equipo de la secretaria de gerencia, el cual no debe tener acceso a la red del centro de datos, solo se le debe permitir la comunicación entre las redes del router principal.
- La red de contabilidad debe tener únicamente acceso FTP y HTTP al servidor para cargar y descargar información de cuentas bancarias, de igual manera los equipos de la red solo podrán recibir correos electrónicos.



**Figura 8. Esquema de la red**

### Datos de configuración

La información necesaria para la configuración básica de los routers y los host se muestra consignada en las siguientes tablas:

**Tabla 14. Direcciones IP interfaces routers**

Router	FastEthernet 0/0	FastEthernet 0/1	Serial 0/0	Tipo de Serial 0/0	Clock
<b>Principal</b>	192.168.10.1	192.168.20.1	220.150.40.1	DCE	56000
<b>Datos</b>	192.169.40.1	-	220.150.40.2	DTE	

**Tabla 15. Direcciones IP Hosts**

Host	Dirección IP	DNS server
1	192.168.10.2/24	192.169.40.3
2	192.168.10.3/24	
3	192.168.20.2/24	
4	192.168.20.3/24	
5	192.169.40.2/24	
Server	192.169.40.3/24	-

### DESARROLLO DE LA PRÁCTICA

- 1) Realizar las interconexiones entre los diferentes elementos de red mostrados en la figura 8. De igual manera debe configurar los equipos de acuerdo a la información suministrada en las tablas 14 y 15.

**Nota:** no olvide configurar el protocolo RIP versión 1 para que se dé una comunicación transparente entre los routers.

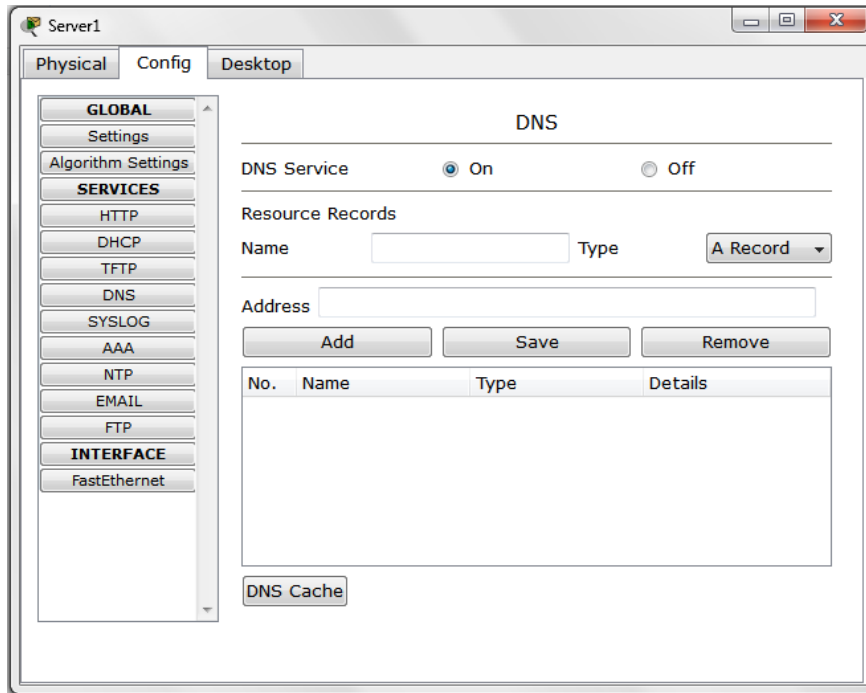
- 2) Configurar el DNS y Mail server:

**Nota:** Es importante mencionar que el objetivo de esta guía no es la configuración de los servicios del servidor, por esta razón no se profundizara demasiado en esto.

Para realizar la configuración se deben seguir los siguientes pasos:

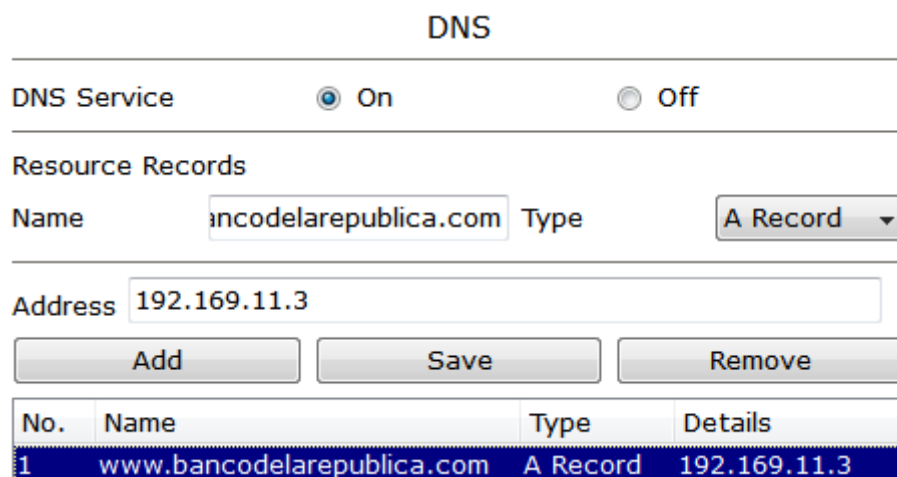
- a) Abrir la interfaz grafica del servidor e ingresar en la pestaña de config y seleccionar el servicio DNS. Seguido de esto debe aparecer una ventana como la que se muestra en la figura 9.





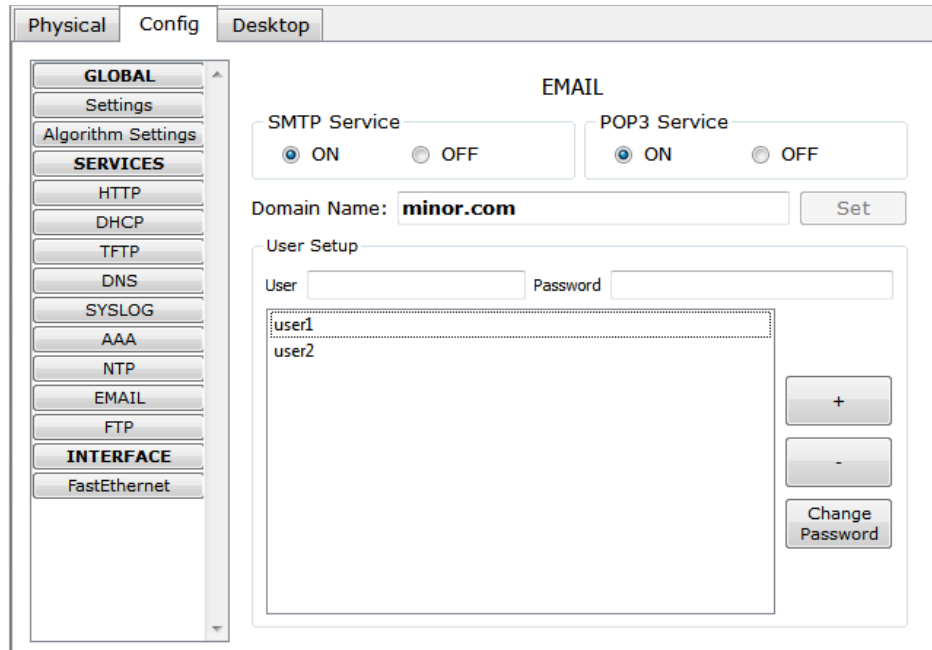
**Figura 9. Ventana de configuración DNS**

- b) Agregar el nombre de la página de internet y la dirección IP del servidor. El nombre de la página es **www.bancodelarepublica.com** la dirección IP del servidor es la mostrada en la tabla 15. Después de agregar los datos verifique que estos aparezcan en la lista en la parte inferior de la ventana como se muestra en la figura 10.



**Figura 10. Datos del DNS**

- c) Agregar el dominio del correo electrónico, el Domain Name para esta práctica es **minor.com**. ingresar el nombre y el password de cada uno de los usuarios del servicio de Email en el servidor como se muestra en la figura 11.



**Figura 11. Configuración Usuarios Email en el servidor**

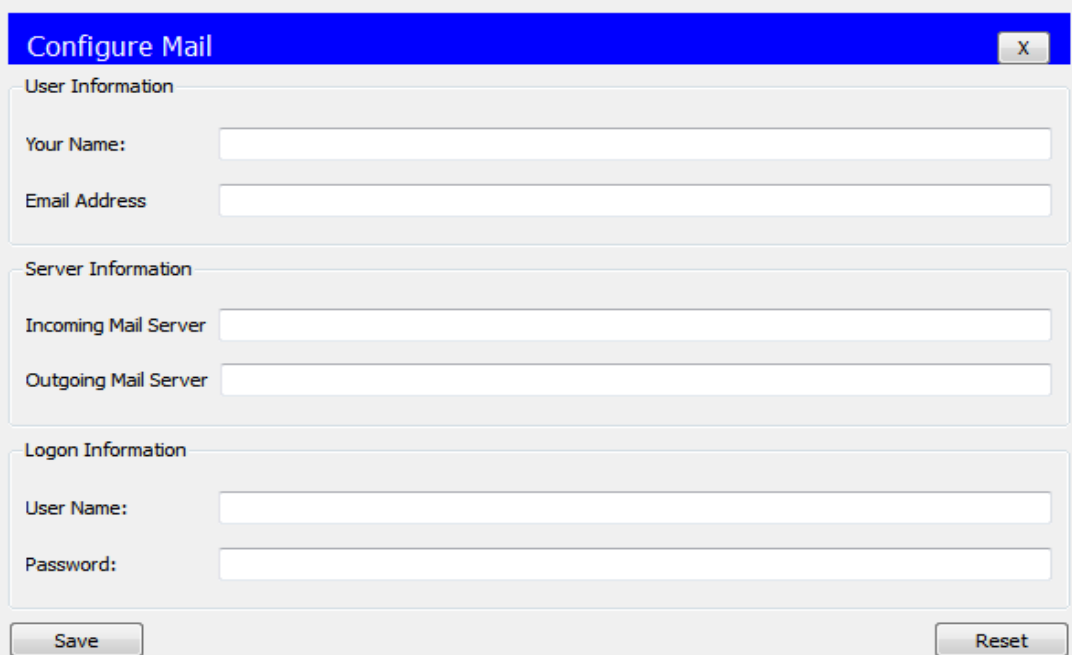
Empleando los campos de name y password de la tabla 16, ingresaremos los usuarios a utilizar este servicio.

**Tabla 16. Datos para configurar el servicio de email en los host**

Host	Name	Email Address	Incoming mail server	Outgoing mail server	Password
1	user1	user1@minor.com			
2	user2	user2@minor.com			
3	user3	user3@minor.com	192.169.40.3	192.169.40.3	cisco*
4	user4	user4@minor.com			
5	user5	user5@minor.com			

\* Para agilizar el desarrollo de la práctica se emplea el mismo password en todos los equipos. Esto no es recomendable hacerlo en aplicaciones reales.

- d) Configurar el servicio email en cada equipo de la red. Abrir la interfaz grafica del PC e ingresar en la pestaña **Desktop**, una vez allí seleccione el servicio **EMail**. Seguido de esto debe aparecer una ventana de configuración como la que se muestra en la figura 12.



The image shows a 'Configure Mail' dialog box with the following fields:

- User Information:**
  - Your Name:
  - Email Address:
- Server Information:**
  - Incoming Mail Server:
  - Outgoing Mail Server:
- Logon Information:**
  - User Name:
  - Password:

Buttons: Save, Reset

**Figura 12. Ventana de configuración email**

Empleando la información consignada en la tabla 16, se debe configurar el servicio.

**Nota:** Este procedimiento se debe realizar con todos los PCs.

- 3) Crear una ACL para restringir el tráfico proveniente del Host 3 hacia la red del centro de datos.
- a) Estructurar la lógica a aplicar en la ACL:
- deny traffic from host 3 to network centro de datos
  - permit all other traffic

Teniendo en cuenta la logica anterior, completa la tabla 17 con los datos necesarios de la ACL.

**Tabla 17. Datos de configuración ACL**

Descripción	Numero ACL	Dirección de origen	Mascara wildcard	Dirección de destino	Mascara wildcard
Detenga el trafico del host 3 a la red del centro de datos					
Permita el resto del trafico					

Teniendo el diagrama de red mostrado en la figura 8, se selecciona el routers, la interfaz y la dirección de tráfico adecuadas. En este caso el router mas cercano al origen es el router **principal**, la interfaz es la **FastEthernet 0/1** y la dirección del trafico es **in** (entrante a la interfaz).

- b)** Configure las ACL empleando el CLI (Comand Line Interface) en el router **principal**. Teniendo en cuenta la lógica y el orden planteado en el punto anterior. Recuerde realizar este procedimiento en el modo de configuración global.

Es necesario emplear los comandos mostrados en la tabla 18, reemplazando las palabras subrayadas por los respectivos valores:

**Tabla 18. Comandos ACL extendida**

Logica	Comandos
deny traffic from host 3 to network centro de datos	access-list # deny ip <u>origin</u> <u>address wildcard destiny</u> <u>address wildcard</u>
permit all other traffic	access-list # permit ip <u>origin</u> <u>address wildcard destiny</u> <u>address wildcard *</u>

\*En este caso la **origin address** o dirección de origen y la **wildcard** pueden ser reemplazadas por la palabra “any”, al igual que la **destiny address** y la **wildcard** ya que involucra al resto de equipos de la red.

- c) Asigne la ACL previamente configurada a la interfaz FastEthernet 0/1. Para realizar esto es necesario emplear la siguiente sintaxis en el CLI ( Comand Line Interface) en modo de configuración de interfaces:

```
interface FastEthernet 0/1
ip access-group # (in/out)
```

- d) Compruebe la correcta configuración de la ACL empleando el comando **show access-list** estando en modo de usuario privilegiado, el cual le mostrara toda la información referente a las ACL configuradas y asignadas en el router.
- e) Verifique la funcionalidad de la ACL a través de el envío de paquetes para comprobar que se permitan o se nieguen los paquetes de acuerdo a las sentencias declaradas por la ACL. Realice este proceso con un ping.

4) Crear una ACL para permitir solo el acceso FTP y HTTP de la red de contabilidad al servidor de la red del centro de datos, y habilitar solo la recepción de correos electrónicos.

a) Estructurar la lógica a aplicar en la ACL:

```
permit traffic HTTP from network contabilidad to server
```

```
permit traffic DNS from network contabilidad to server*
```

```
permit traffic FTP from network contabilidad to server
```

```
permit traffic POP3 from any to any
```

\* Es necesario agregar la sentencia de tráfico DNS, para poder visualizar las páginas a través de los dominios configurados.

Teniendo en cuenta la lógica anterior, completa la tabla 19 con los datos necesarios de la ACL.

**Tabla 19. Datos de configuración ACL extendida**

Descripción	Protocolo	Puerto	Dirección de origen	Máscara wildcard	Dirección de destino	Máscara wildcard
Permita el tráfico de la red de contabilidad al servidor						
Denegar el resto del tráfico						

Teniendo en cuenta el diseño de red de la figura 8, el router mas cercano al origen es el **principal**, la interfaz apropiada es la **FastEthernet 0/0**, y la dirección del trafico es **in** (entrante a la interfaz).

- b)** Configure las ACL empleando el CLI (Comand Line Interface) en el modo de configuración global del router **principal**.

Teniendo en cuenta los siguientes comandos:

```
access-list # (deny/permit) protocol origin address  
wildcard destiny address wildcard eq #
```

**Nota:** Recuerde reemplazar las palabras subrayadas por los valores adecuados

- c)** Asigne la ACL previamente configurada a la interfaz FastEthernet 0/0 como se hizo en la sección c del punto 3.

- d)** Compruebe la correcta configuración de la ACL empleando el comando **show access-list**, el cual le mostrara toda la información referente a las ACL configuradas y asignadas en el router.

- e)** Verifique la funcionalidad de la ACL, para esto realice las siguientes pruebas:

- I. Ingrese desde cualquier terminal de la red de contabilidad al **web browser** e intente acceder a la página **www.bancodelarepublica.com**.

¿Cuál fue el resultado de realizar esta operación?

---

---

II. Haga ping entre el host 4 y cada uno de los host de la red de contabilidad.

¿Se realizó el ping con éxito? Justifique su respuesta

---

---

---

¿Cuál es el mensaje que aparece en la pantalla de **command prompt** al intentar hacer ping a los equipos de la red de contabilidad?

---

---

III. Envié un correo electrónico desde el host 1 hacia el host 4 y viceversa. ¿Fueron recibidos los correos electrónicos? ¿A qué se debe?

---

---

---



**GUIA PRÁCTICA 3**  
**CONFIGURACION DE CBAC EMPLEANDO EL SOFTWARE**  
**CISCO PACKET TRACER**

**Objetivos:**

- Configurar un IOS firewall con CBAC.
- Verificar el funcionamiento de CBAC.

**Investigación previa:**

- Configuración básica de un router (dirección IP, interfaces, protocolos).
- ¿Qué es ACL?, ¿Qué es CBAC?
- Configuración de ACL estándar, extendida y CBAC.

**Requerimientos:**

- Computador con sistema operativo Windows XP o superior
- Software Cisco Packet Tracer versión 5.3.1.

## CASO DE ESTUDIO

### Situación

El laboratorio de comunicaciones del programa de ingeniería electrónica de la UTB se desea conectar al servidor del centro de datos como se muestra en el esquema de red de la figura 13.

Para esto necesita implementar ciertas políticas de seguridad y control en el router del laboratorio para impedir tráfico malicioso procedente de los estudiantes hacia el servidor. Por esto se hace necesario implementar unas ACL que permita el control del tráfico en conjunto con una CBAC para la supervisión e informes de alerta sobre el tráfico.

### Políticas de seguridad

- Bloquear todo el tráfico externo a la red del laboratorio de comunicaciones
- Permitir e inspeccionar el tráfico HTTP, ICMP de la red interna del laboratorio al exterior de la red.

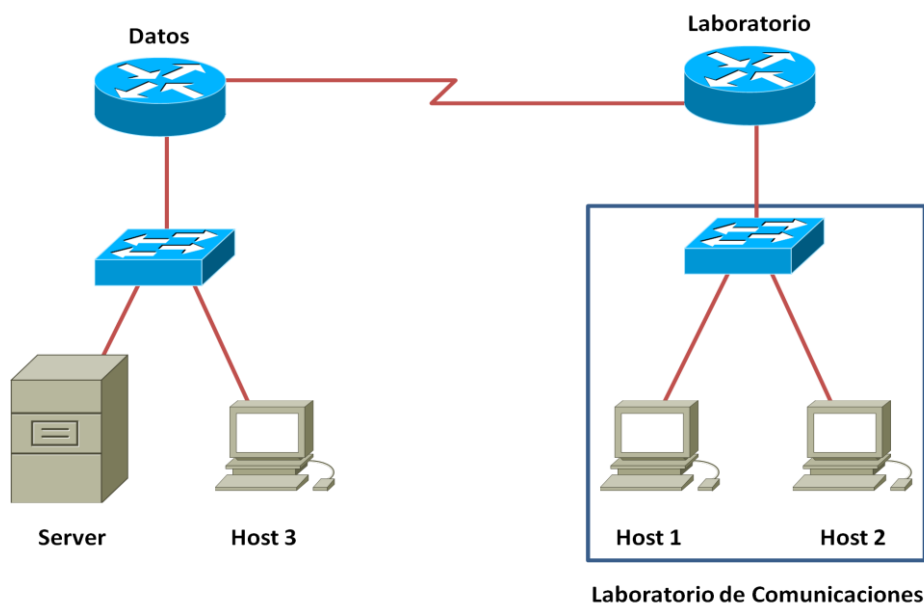


Figura 13. Esquema de la red

## Datos de configuración

La información necesaria para la configuración básica de los routers y los host se muestra consignada en las siguientes tablas:

**Tabla 20. Direcciones IP interfaces routers**

Router	FastEthernet 0/0	Serial 0/0	Tipo de Serial 0/0	Clock
Datos	192.180.10.1	200.140.20.1	DCE	56000
Laboratorio	192.180.20.1	200.140.20.2	DTE	

**Tabla 21. Direcciones IP Hosts**

Host	Dirección IP
1	192.180.20.2/24
2	192.180.20.3/24
3	192.184.10.2/24
Server	192.184.10.3/24

## DESARROLLO DE LA PRÁCTICA

- 1) Realizar las interconexiones entre los diferentes elementos de red mostrados en la figura 13. De igual manera debe configurar los equipos de acuerdo a la información suministrada en las tablas 20 y 21.

**Nota:** no olvide configurar el protocolo RIP versión 1 para que se dé una comunicación transparente entre los routers.

2) Crear una ACL que bloquee el tráfico externo a la red del laboratorio de comunicaciones.

a) Estructurar la lógica a aplicar en la ACL

deny traffic from any to network laboratorio de comunicaciones

Teniendo en cuenta que en el diseño de red de la figura 13, la red externa inicia a partir de la interfaz serial seria, el router mas cercano al origen es el **laboratorio**, la interfaz apropiada es la **serial 0/0/0**, y la dirección del trafico es **in** (entrante a la interfaz).

b) Configure las ACL empleando el CLI (Comand Line Interface) en el modo de configuración global del router **laboratorio**. Teniendo en cuenta los siguientes comandos:

access-list # (deny/permit) protocol origin address  
wildcard destiny address wildcard

**Nota:** Recuerde reemplazar las palabras subrayadas por los valores adecuados

c) Asigne la ACL previamente configurada a la interfaz correspondiente

d) Compruebe la correcta configuración y funcionalidad de la ACL.

**Nota:** emplee un ping para realizar la comprobación de funcionalidad.

3) Crear una CBAC que permita inspeccionar el tráfico HTTP y ICMP de la red del laboratorio hacia el exterior.

a) Crear reglas de inspección para los diferentes protocolos, para esto emplee la siguiente sintaxis en el CLI (Comand Line Interface) en el modo de configuración global:

ip inspect name nombre-inspeccion protocolo

**Nota:** preferiblemente usar un nombre para las reglas de inspección que sea fácil de recordar, se recomienda para el desarrollo de esta práctica usar el nombre **UTB**.

- b) Habilitar las auditorías del tráfico permitido o denegado a través del router. Estas auditorías permiten tener un control del historial de eventos, los cuales son almacenados en el servidor. Para realizar esta operación se debe emplear la siguiente sintaxis:

```
ip inspect audit-trail
```

```
service timestamp debug datetime msec*
```

\*Este comando es empleado para crear una base de tiempo en la que puedan ser registrados los eventos ocurridos, en este caso se toma una base de tiempo en milisegundos.

Es necesario especificar cual la dirección IP del servidor al cual se va a *loggear* para monitorear los eventos ocurridos a través del servicio syslog del servidor. Para ello se emplea la siguiente sintaxis.

```
logging dirección servidor
```

- c) Asignar las reglas de inspección a la interfaz correspondiente. En este caso a la interfaz en la que se implemento la ACL, y la dirección del tráfico debe ser saliente de la interfaz. Empleando la siguiente sintaxis en el CLI (Comand Line Interface) en el modo de configuración de interfaces:

```
interface serial 0/0/0
```

```
ip inspect nombre-inspeccion out
```

- 4) Verificar la configuración y funcionalidad de la CBAC

- a) Compruebe la correcta configuración de las reglas de inspección entrando en modo de usuario privilegiado y empleando el comando **show ip inspect config**, el cual le mostrara toda la información referente a las reglas de inspección configuradas en el router.
- b) Verifique la funcionalidad de la reglas de inspección a través ACLs a través de el envío de paquetes, y el acceso HTTP al servidor.
- I. Ingrese en el CLI (Comand Line Interface) modo de usuario privilegiado e ingrese el comando **show ip inspect sessions**. A continuación ingrese desde cualquier pc de la red del laboratorio de comunicaciones al **web browser** y digite la dirección ip del servidor, y observe el CLI de router.

¿Qué información proporciona el CLI sobre la sesión HTTP del pc?

---

---

---

---

Ahora realice un ping entre el host 1 y el host 3, y viceversa

¿Se realizaron los pings con éxito? Justifique su respuesta

---

---

---

---

¿Qué información proporciona el CLI sobre los pings realizados entre los host?

---

---

---

---

II. Ingrese al la interfaz grafica del servidor y seleccione el servicio **syslog**, el cual le permitirá observar los registros de eventos ocurridos a través de la interfaz en la que se aplico el firewall.

¿Qué información le proporciona el servicio syslog del servidor?

Escriba un evento que haya registrado el servicio

---

---

---

---

## BIBLIOGRAFÍA

Access List Basics. En: Jeff Sedayao. Cisco IOS Access Lists. O'Reilly; 2001. Pág. 22-89.

ACL de *router*. En Cisco. Fundamentos de seguridad de redes. Pearson; 2004; Pág. 147-204.

Cisco Icon Library [diapositivas 2-16]. Cisco; 2011 [36 diapositivas]



## ANEXOS

### Implementación de las guías prácticas

A manera de conclusión del documento, se realizó la implementación de forma exitosa de las dos primeras guías prácticas: Configuración de ACL estándar y extendida utilizando Packet Tracer™, en ambas se obtuvieron los resultados esperados.



**Figura 13.** Montaje implementado de las dos primeras guías prácticas.

Para la realización de las mismas se hizo uso, además de los PC's y conectores necesarios, de los siguientes equipos:

- **Router Cisco serie 2800**



**Figura 14.** Router Cisco serie 2800

- **Switch D-Link DES-1008D**



**Figura 15.** *Switch D-Link DES-1008D*

A partir de la experiencia obtenida durante la implementación de las guías prácticas a continuación se listan algunas recomendaciones a la hora de llevar el contenido de las guías de la simulación a la realidad:

- Los servicios del servidor como HTTP, DNS y email, no se configuran de la misma manera en la que se realiza en el server-PT del software CISCO Packet Tracer™, es necesario la instalación y configuración de programas que permitan la correcta operación de estos servicios, como es el caso del Internet Information Server (IIS) para el funcionamiento del web server, establecer la configuración apropiada a través del panel de control de Windows™ para la configuración del DNS Server, y un programa para el servicio de correo electrónico tal como Microsoft® Outlook.
- Es importante tener en cuenta que a la hora de configurar ACL en un router real no se pueden configurar varias en diferentes interfaces, el router solo permite en estado activo una sola ACL, a diferencia de los *routers* simulados que permiten el uso de diversas ACL en el mismo equipo para efectos académicos; por lo que lo más recomendable es estructurar una buena lógica para aplicar una sola ACL en el lugar más estratégico y con todas las condiciones necesarias para cumplir con las políticas de seguridad y control exigidas.
- Debido a la naturaleza académica de la implementación es probable que durante el montaje y prueba sea necesario encender y apagar los equipos repetidas veces, por lo que se recomienda que, para ahorrar tiempo y evitar errores a la hora de configurar los equipos, constantemente se copie el contenido del *running-config* al *startup-config*.