

Planificación y Administración de Redes

Listas de Control de Acceso - Cisco



IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Jesús Moreno León
Raúl Ruiz Padilla


j.moreno1@gmail.com

Septiembre 2010

© Jesús Moreno León, Septiembre de 2010

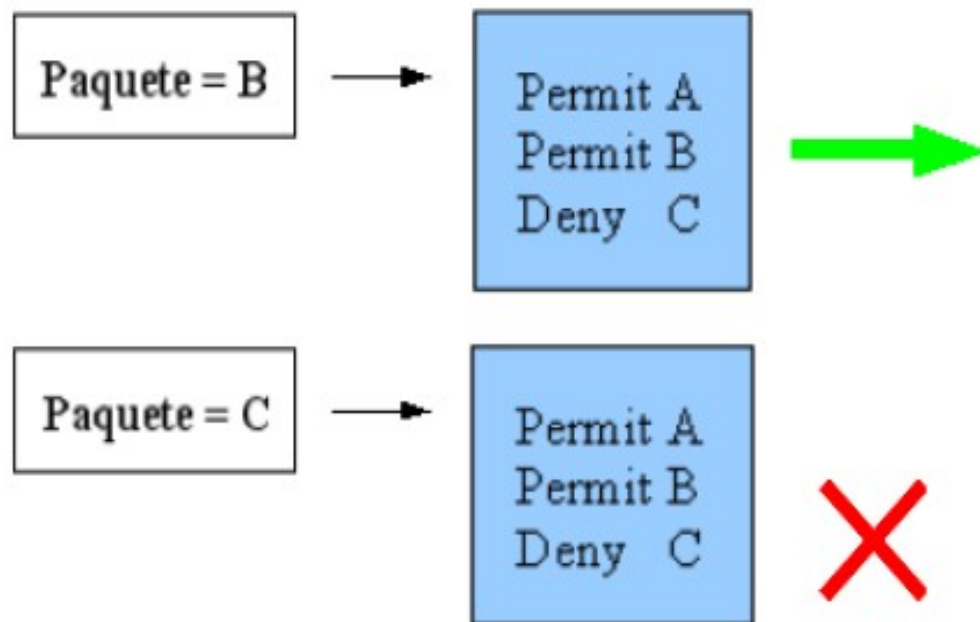
Algunos derechos reservados.
Este artículo se distribuye bajo la licencia
"Reconocimiento-CompartirIgual 3.0 España" de Creative
Commons, disponible en
<http://creativecommons.org/licenses/by-sa/3.0/es/deed.es>

Este documento (o uno muy similar)
está disponible en (o enlazado desde)
<http://informatica.gonzalonazareno.org>



Introducción

Un listado de control de acceso, ACL, es un listado de declaraciones condicionales (permit o deny) que ayudan a regular el tráfico de datos que entra y sale de un router



Introducción

Para comprender mejor su funcionamiento podemos imaginarnos un ACL como si fuera un guardia de seguridad de una discoteca.

Los dueños establecen los criterios que debe cumplir un potencial cliente para poder pasar a la sala.

Cada vez que alguien llega a la puerta, el portero lo evalúa:

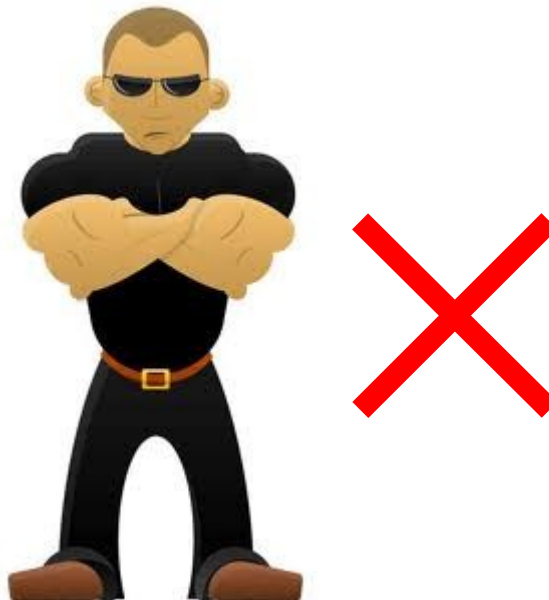
- si cumple los criterios → pasa
- si no los cumple → no pasa



Introducción



Introducción



Listas de Control de Acceso

- Las declaraciones se leen **EN ORDEN**. Si un paquete no cumple con la condición de la primera declaración pasa a compararse con la siguiente...
- No pueden existir dos listados de acceso asociados a la misma interfaz y al mismo protocolo
- Podemos asociar un mismo listado de acceso a varias interfaces



Listas de Control de Acceso

- Máscaras comodín
 - Se utilizan para decirle al router cuántos bits de la dirección del listado tienen que coincidir con los de la dirección del paquete analizado para que se cumpla la condición
 - Los bits que quiero que se comprueben se ponen a 0
 - Los que NO se ponen a 1
 - Ejemplos:
 - Permit 172.16.0.0 0.0.255.255
 - Deny 192.168.1.0 0.0.0.255
 - Permit 200.15.14.122 0.0.0.0 (host)
 - Permit any



Listas de Control de Acceso

- Para construir un ACL tenemos que escribir nuestras declaraciones:

```
router(config)#access-list ZZ permit|deny X.X.X.X Y.Y.Y.Y
```

ZZ: número de listado (de 1 a 99)

X.X.X.X: dirección IP

Y.Y.Y.Y: máscara comodín (wildcard mask)

- Si queremos que dos declaraciones pertenezcan al mismo ACL tenemos que asignarles el mismo número de listado

Listas de Control de Acceso

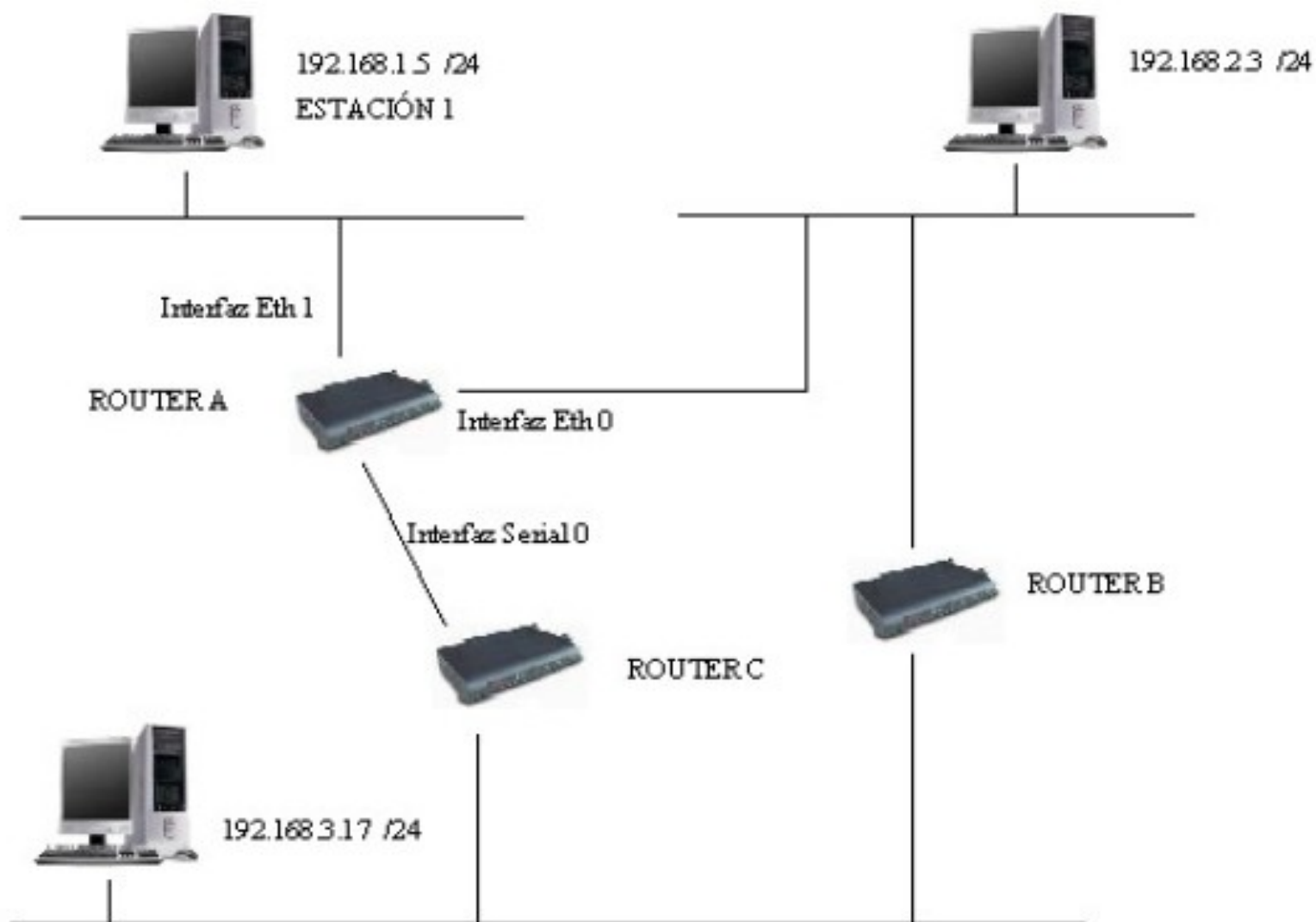
- Tenemos que asignar la ACL a la interfaz (o las interfaces) del router que corresponda, indicando si se aplica al tráfico de entrada o salida

```
Router(config-if)#ip access-group XX in|out
```

- También podemos asignar una ACL a los puertos telnet

```
Router(config)#line vty 0 4  
Router(config-line)#access-class XX in|out
```

Listas de Control de Acceso



Listas de Control de Acceso

- Vamos a crear un listado para la interfaz serial 0 del router A
- Queremos que sólo los datos que se envíen desde la red de la estación 1 a los nodos de la red 192.168.3.0 puedan utilizar la línea contratada que conecta el router A y el router C
- Nuestro listado rechazará todos los demás paquetes



Listas de Control de Acceso

- Creamos nuestras declaraciones (con el mismo número de listado)

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255  
Router(config)#access-list 1 deny any *
```

* Declaración implícita en todos los ACL

- Asignamos la ACL a la interfaz serial 0 para el tráfico de salida

```
Router(config)#interface serial0  
Router(config-if)#ip access-group 1 out
```

ACLs extendidas

- Las listas de acceso IP estándar sólo verifican la dirección de origen en la cabecera del paquete(Capa 3)
- Las listas de acceso IP extendidas pueden verificar otros muchos elementos, incluidas opciones de la cabecera del segmento(Capa 4), como los números de puerto

```
Router(config)#access-list[nº de lista de acceso][permit|deny][protocol][dirección de origen][mascara comodín][puerto del operador][dirección de destino][mascara de destino][puerto del operador][established][log]
```

Puerto del operador puede ser: `lt` (menor que) `gt` (mayor que) `eq` (igual a) o `neq` (distinto que) y un número de puerto de protocolo.

ACLs extendidas

- Las ACLs extendidas se numeran entre 100 y 199. Ejemplos:

```
Router(config)#access-list 100 deny ip 192.168.1.32  
                0.0.0.0 172.16.2.0. 0.0.0.255  
Router(config)#access-list 100 permit ip any any  
...  
Router(config-if)#access-group 100 out
```

```
Router(config)#access-list 101 deny tcp 192.168.14.0  
                0.0.0.255 any eq 80  
Router(config)#access-list 101 permit ip any any
```

ACLs con nombre

- Desde la versión 11.2 del IOS de Cisco podemos identificar las ACL's con un nombre:

```
Router(config)#ip access-list[standard|extended] [nombre]  
Router(config[std|ext]nacl)#[permit|deny][condiciones de prueba]
```

Ejemplo:

```
Router(config)#ip access-list standard castigados  
Router(config-std-nacl)#deny 192.168.14.0 0.0.0.255  
Router(config-std-nacl)#permit any
```


Bibliografía



GUIA OFICIAL PARA EL
EXAMEN CCNA ICND2
de ODOM, WENDELL

PRENTICE-HALL

Capítulo 6. Listas de control
de acceso IP

