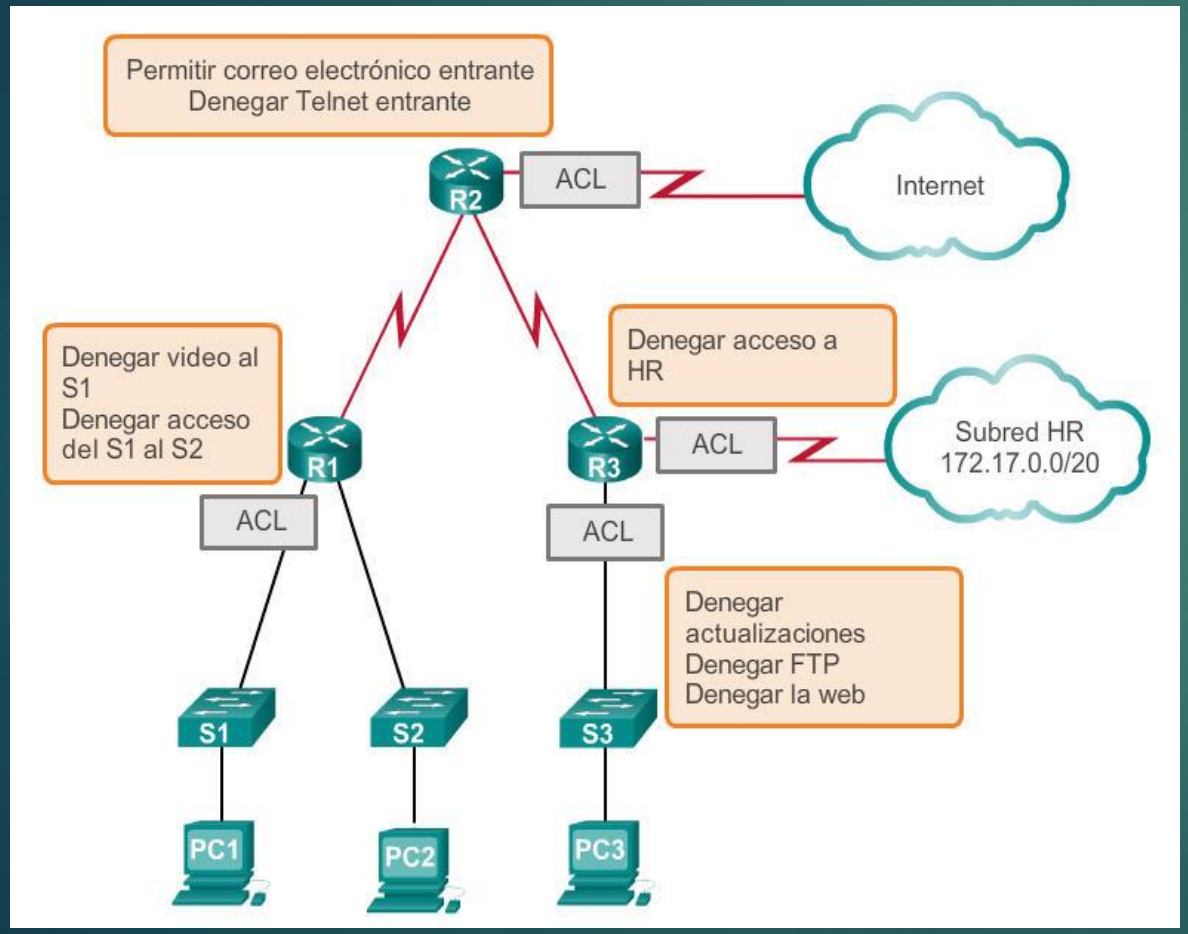
ACL (LISTA DE CONTROL DE ACCESO)

¿Qué es una ACL?



Una ACL es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Las ACL son una de las características del software IOS de Cisco más utilizadas.

FUNCIONES

- Limitar el tráfico de la red para aumentar su rendimiento. Por ejemplo, si la política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que bloqueen el tráfico de video. Esto reduciría considerablemente la carga de la red y aumentaría su rendimiento.
- Proporcionar control del flujo de tráfico. Las ACL pueden restringir la entrega de actualizaciones de routing. Si no se requieren actualizaciones debido a las condiciones de la red, se preserva ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro host acceda a la misma área. Por ejemplo, se puede restringir el acceso a la red de Recursos Humanos a los usuarios autorizados.
- Filtrar el tráfico según el tipo de tráfico. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.
- Filtrar a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos, como FTP o HTTP.

CONVERSACION TCP

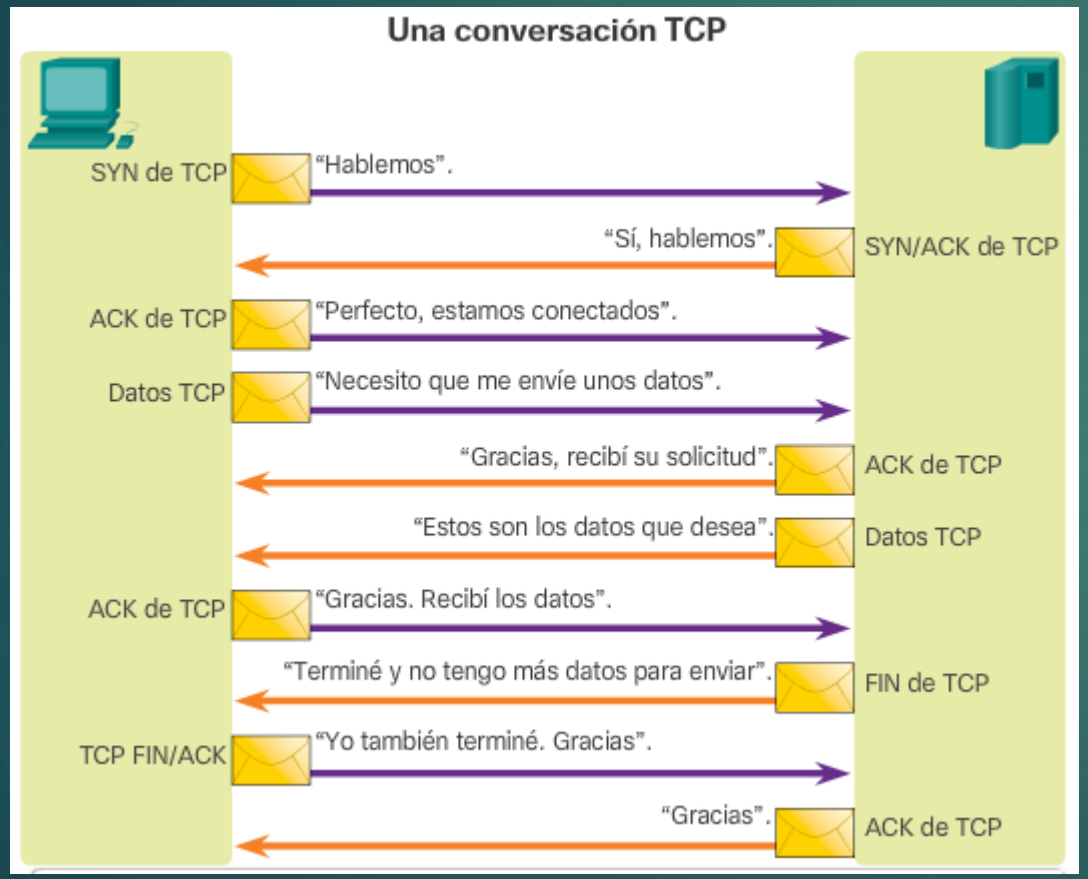
FILTRADO DE PAQUETES

PROPOSITO

FILTRADO DE PAQUETES CONT.

FUNCIONAMIENTO DE LAS ACL

CONVERSACION TCP



Las ACL permiten a los administradores controlar el tráfico hacia y desde la red. Este control puede ser tan simple como permitir o denegar el tráfico según las direcciones de red o tan complejo como controlar el tráfico de la red según el puerto TCP solicitado

Los segmentos TCP se marcan con indicadores que denotan su objetivo: la sesión comienza (se sincroniza) con un indicador SYN, el indicador ACK es un acuse de recibo de un segmento esperado, y un indicador FIN finaliza la sesión. Un indicador SYN/ACK confirma que la transferencia está sincronizada. Los segmentos de datos TCP incluyen el protocolo del nivel más alto necesario para dirigir los datos de aplicación a la aplicación correcta.

Puertos TCP

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Leyenda

Puertos TCP registrados:

1863	MSN Messenger
2000	Cisco SCCP (VoIP)
8008	HTTP alternativo
8080	HTTP alternativo

Puertos TCP bien conocidos:

21	FTP
23	Telnet
25	SMTP
80	HTTP
143	IMAP
194	Internet Relay Chat (IRC)
443	HTTP seguro (HTTPS)

Puertos UDP

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Leyenda

Puertos UDP registrados:

1812	Protocolo de autenticación RADIUS
5004	RTP (protocolo de transporte de voz y video)
5040	SIP (VoIP)

Puertos UDP bien conocidos:

69	TFTP
520	RIP

Puertos TCP/UDP comunes

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Leyenda

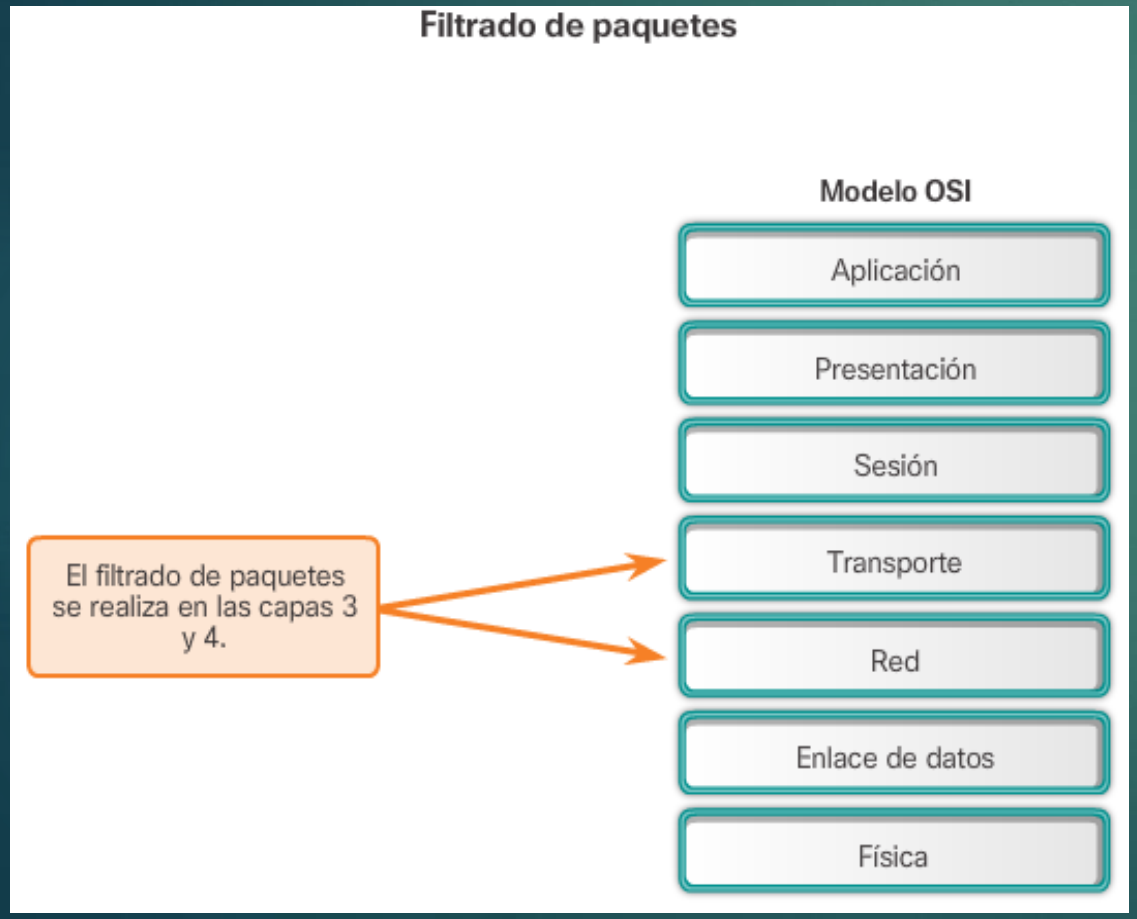
Puertos TCP/UDP registrados comunes:

1433	MS SQL
2948	WAP (MMS)

Puertos TCP/UDP bien conocidos comunes:

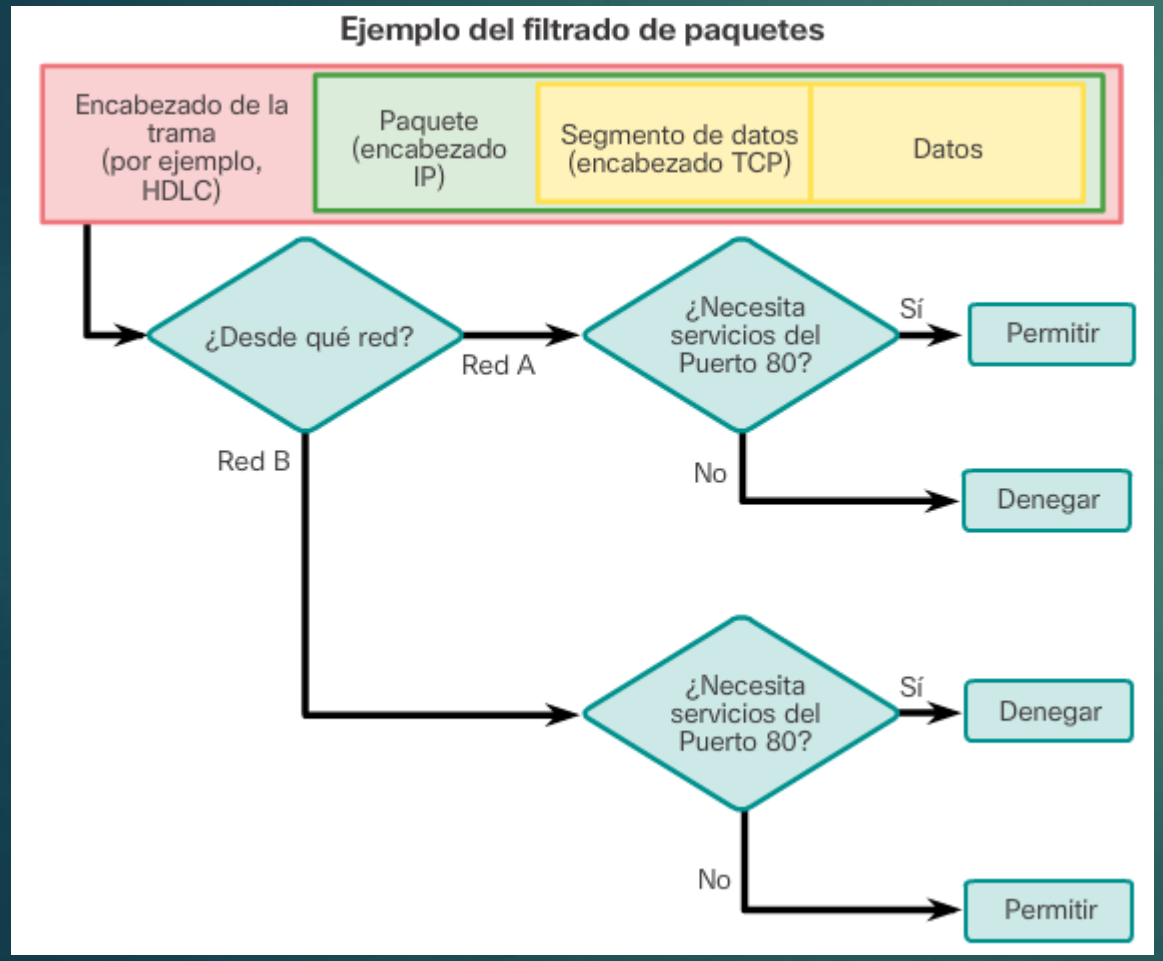
53	DNS
161	SNMP
531	AOL Instant Messenger, IRC

FILTRADO DE PAQUETES



- El filtrado de paquetes, a veces denominado “filtrado de paquetes estático”, controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según determinados criterios, como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete.
- Cuando reenvía o deniega los paquetes según las reglas de filtrado, un router funciona como filtro de paquetes.
- Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como “entradas de control de acceso” (ACE).

FILTRADO DE PAQUETES CONT.



Para esta situación, el filtro de paquetes examina cada paquete de la siguiente manera:

- Si el paquete es un SYN de TCP de la red A que utiliza el puerto 80, tiene permiso para pasar. El resto de los tipos de acceso se deniega a esos usuarios.
- Si el paquete es un SYN de TCP de la red B que utiliza el puerto 80, se bloquea. Sin embargo, se permite el resto de los tipos de acceso.

Este es solo un ejemplo sencillo. Se pueden configurar varias reglas para permitir o denegar otros servicios a usuarios específicos.

FUNCIONAMIENTO DE ACL

La última sentencia de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Debido a esta denegación implícita, una ACL que no tiene, por lo menos, una instrucción permit bloqueará todo el tráfico.

TIPOS DE ACL IPV4

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Las ACL estándar filtran paquetes IP solamente según la dirección de origen.

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Las ACL extendidas filtran paquetes IP según varios atributos, incluidos los siguientes:

- Las direcciones IP de origen y destino
- Los puertos TCP y UDP de origen y destino
- El tipo y número de protocolo (por ejemplo: IP, ICMP, UDP, TCP, etc.)

ASIGNACION DE NUMEROS Y NOMBRES DE ACL

ACL numerada:

Asignar un número según el protocolo que se debe filtrar.

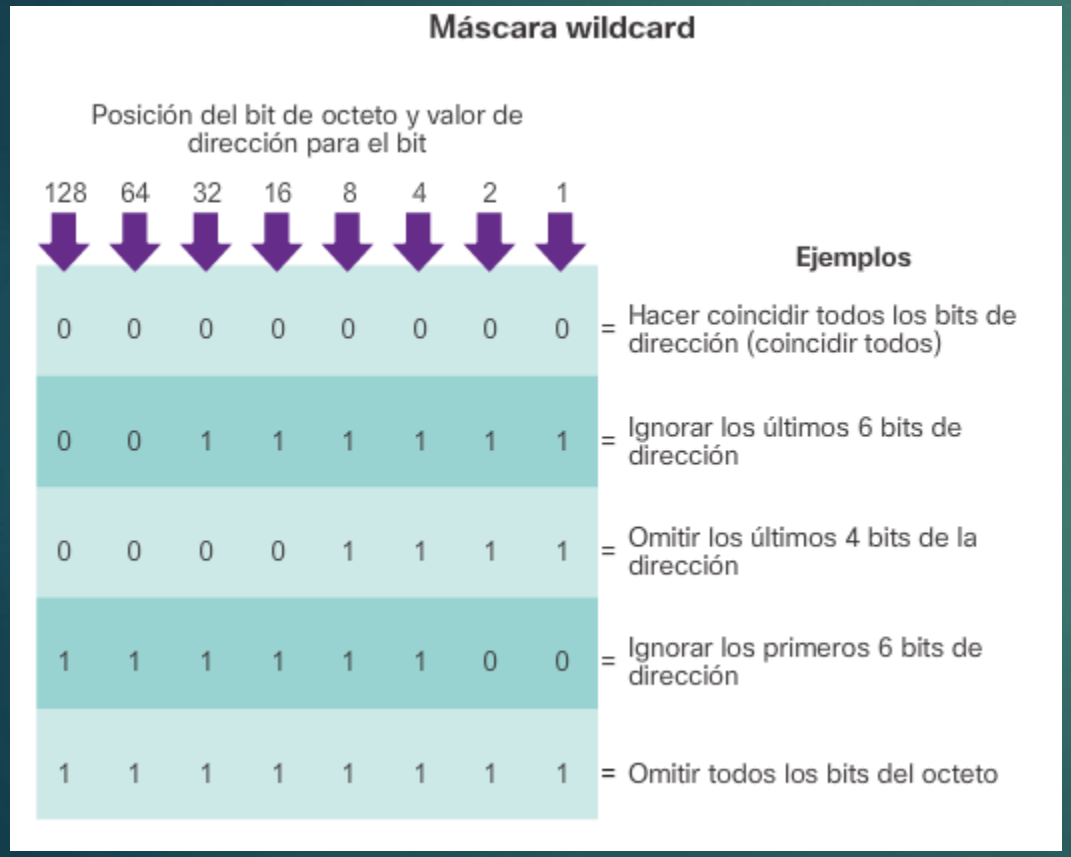
- (1 a 99) y (1300 y 1999): ACL de IP estándar
- (100 a 199) y (2000 a 2699): ACL de IP extendida

ACL con nombre:

Asignar un nombre para identificar la ACL.

- Los nombres pueden contener caracteres alfanuméricos.
- Se sugiere escribir el nombre en MAYÚSCULAS.
- Los nombres no pueden contener espacios ni signos de puntuación.
- Se pueden agregar o eliminar entradas dentro de la ACL.

MÁSCARAS WILDCARD EN ACL



Las máscaras wildcard y las máscaras de subred se diferencian en la forma en que establecen la coincidencia entre los unos y ceros binarios. Las máscaras wildcard utilizan las siguientes reglas para establecer la coincidencia entre los unos y ceros binarios:

- Bit 0 de máscara wildcard: se establece la coincidencia con el valor del bit correspondiente en la dirección.
- Bit 1 de máscara wildcard: se omite el valor del bit correspondiente en la dirección.

A las máscaras wildcard a menudo se las denomina “máscaras inversas”. La razón es que, a diferencia de una máscara de subred en la que el 1 binario equivale a una coincidencia y el 0 binario no es una coincidencia, en las máscaras wildcard es al revés.

CALCULO DE LA MASCARA WILDCARD

Ejemplo 1

	255.255.255.255
–	255.255.255.000
	000.000.000.255

Ejemplo 2

	255.255.255.255
–	255.255.255.240
	000.000.000.015

Ejemplo 3

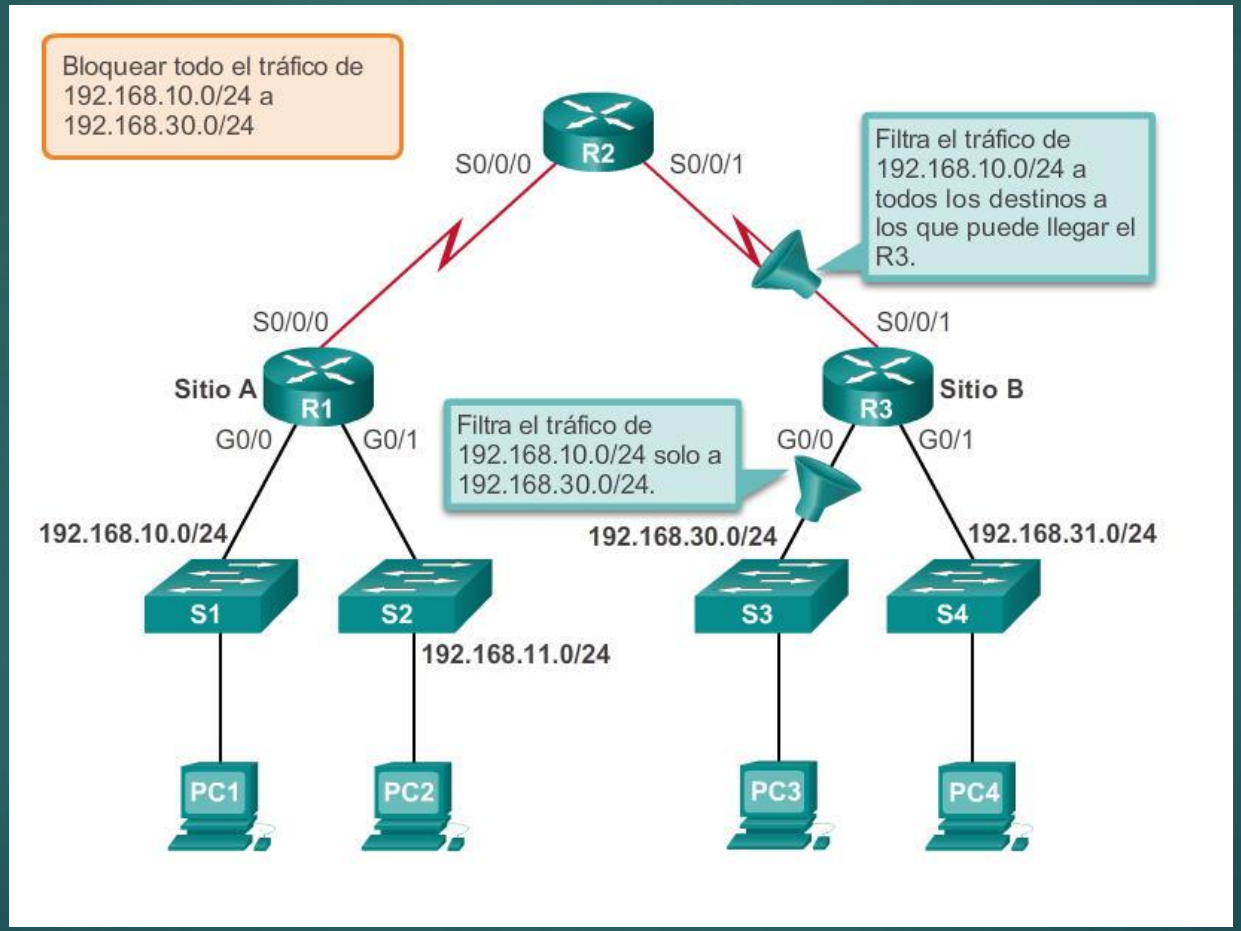
	255.255.255.255
–	255.255.254.000
	000.000.001.255

El cálculo de máscaras wildcard puede ser difícil. Un método abreviado es restar la máscara de subred a 255.255.255.255.

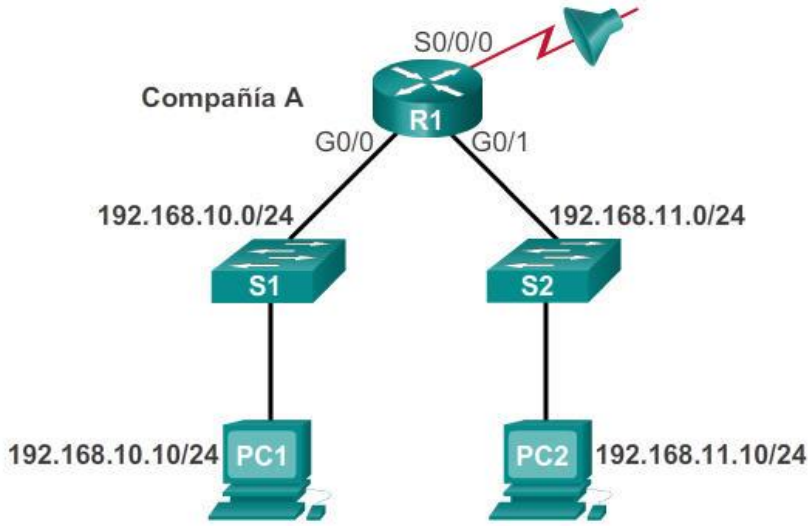
PAUTAS PARA LA GENERACION DE ACL

- Utilice las ACL en los routers de firewall ubicados entre su red interna y una red externa, como Internet.
- Utilice las ACL en un router ubicado entre dos partes de la red para controlar el tráfico que entra a una parte específica de su red interna o que sale de esta.
- Configure las ACL en los routers de frontera, es decir, los routers ubicados en los límites de las redes.
- Configure las ACL para cada protocolo de red configurado en las interfaces del router de frontera.

COLOCACION DE LAS ACL



CONFIGURACION DE ACL ESTANDAR



ACL 1

```
R1(config)#access-list 1 permit ip 192.168.10.0 0.0.0.255
```

ACL 2

```
R1(config)#access-list 2 permit ip 192.168.10.0 0.0.0.255
R1(config)#access-list 2 deny any
```

Ejemplo de ACL

- `access-list 2 deny host 192.168.10.10`
- `access-list 2 permit 192.168.10.0 0.0.0.255`
- `access-list 2 deny 192.168.0.0 0.0.255.255`
- `access-list 2 permit 192.0.0.0 0.255.255.255`

CONFIGURACION DE ACL ESTANDAR CONT.

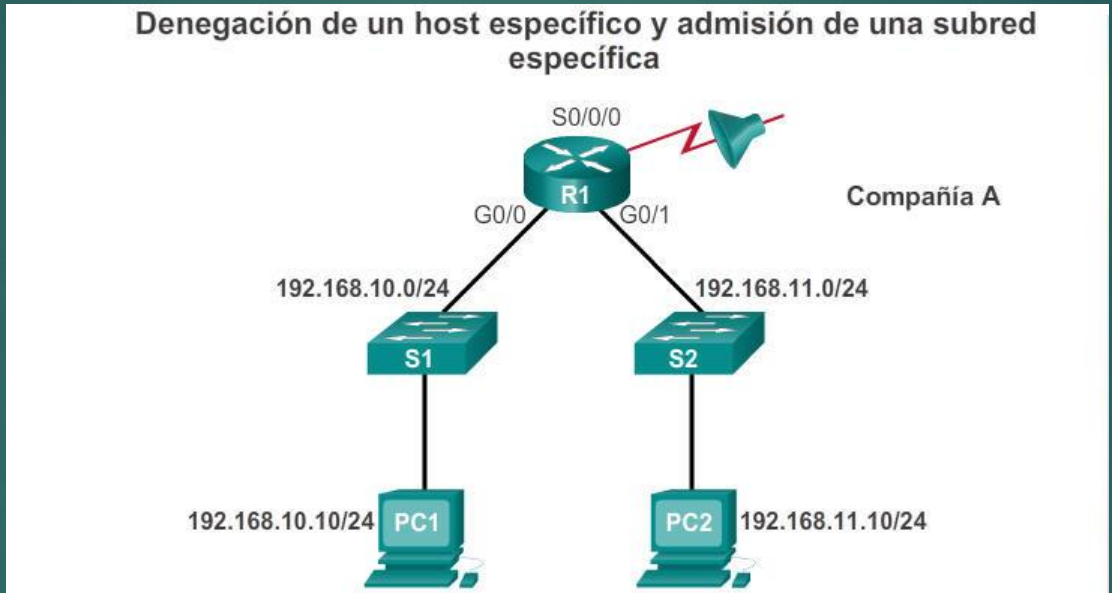
La sintaxis completa del comando de ACL estándar es la siguiente:

```
Router(config)# access-list número-lista-acceso
deny permit remark origen [ wildcard-origen ] [
log ]
```

Para eliminar la ACL, se utiliza el comando de configuración global **`no access-list`**.

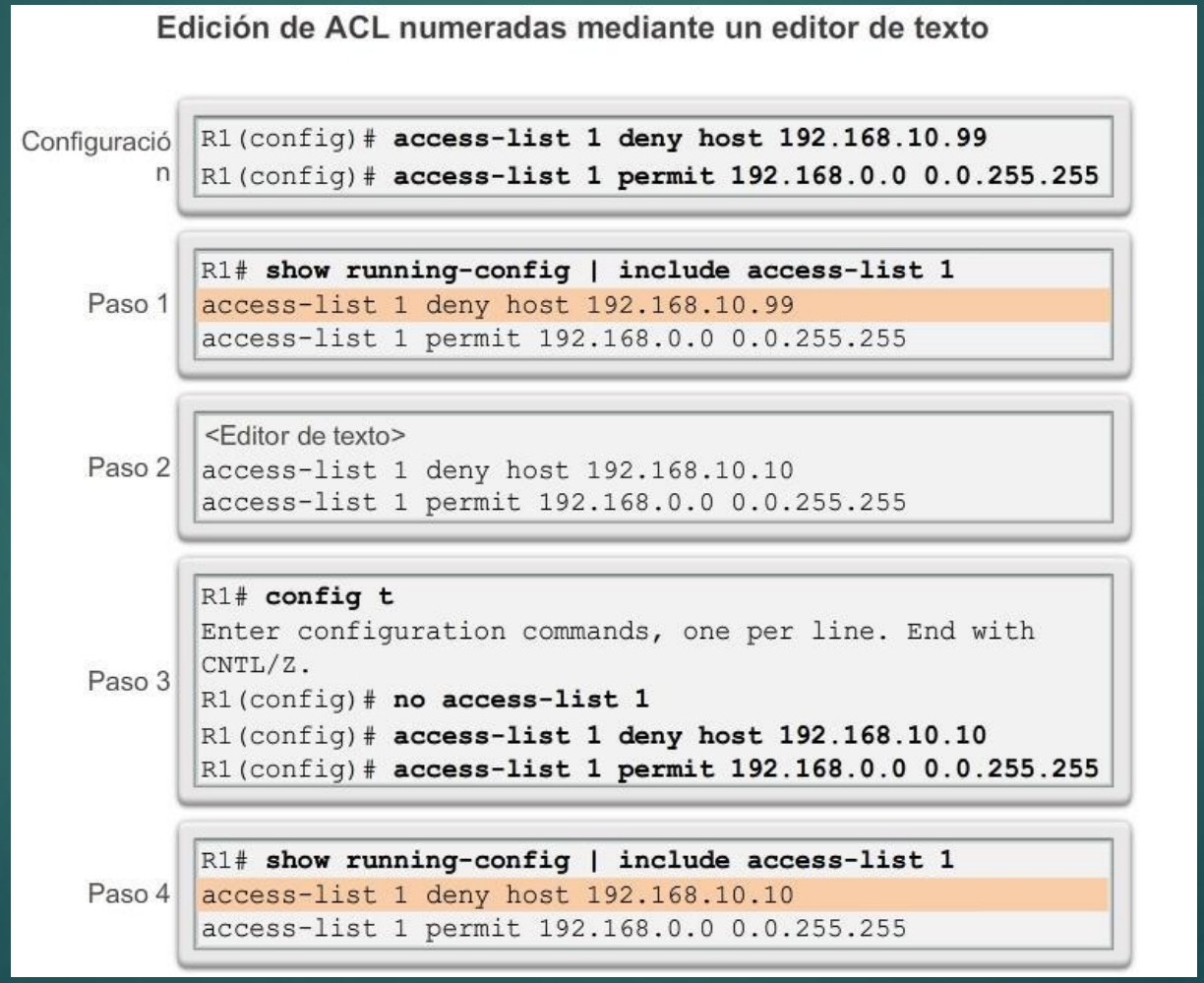
La palabra clave **`remark`** se utiliza en los documentos y hace que sea mucho más fácil comprender las listas de acceso.

APLICACIÓN DE ACL ESTANDAR

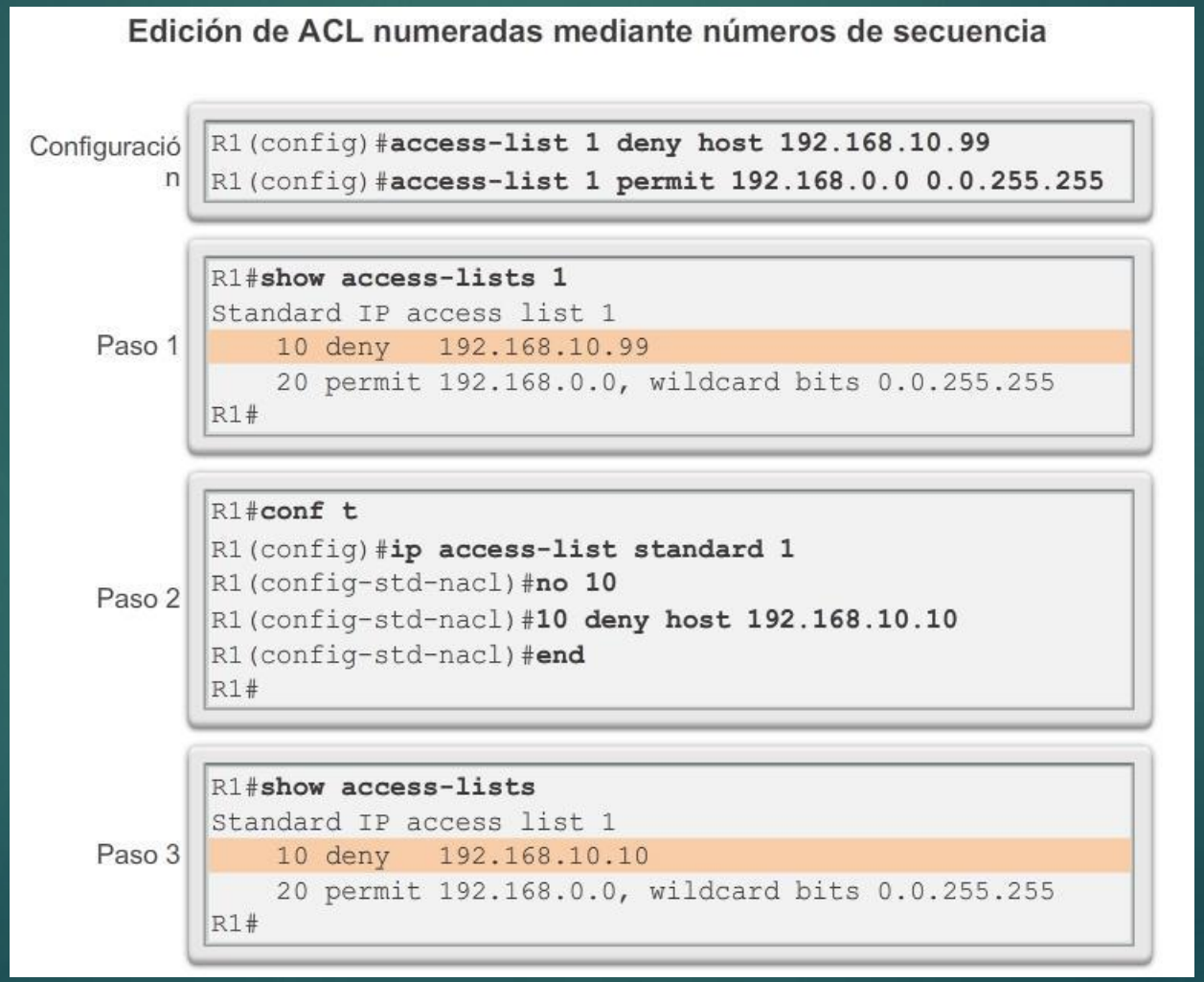



```
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 1 out
```

EDICION DE ACL



EDICION DE ACL ESTANDAR NUMERADAS



VERIFIACION DE ACL

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
  Inbound  access list is not set
<output omitted>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
  Inbound  access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

ACL EXTENDIDAS

Uso de números de puerto

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Uso de palabras clave

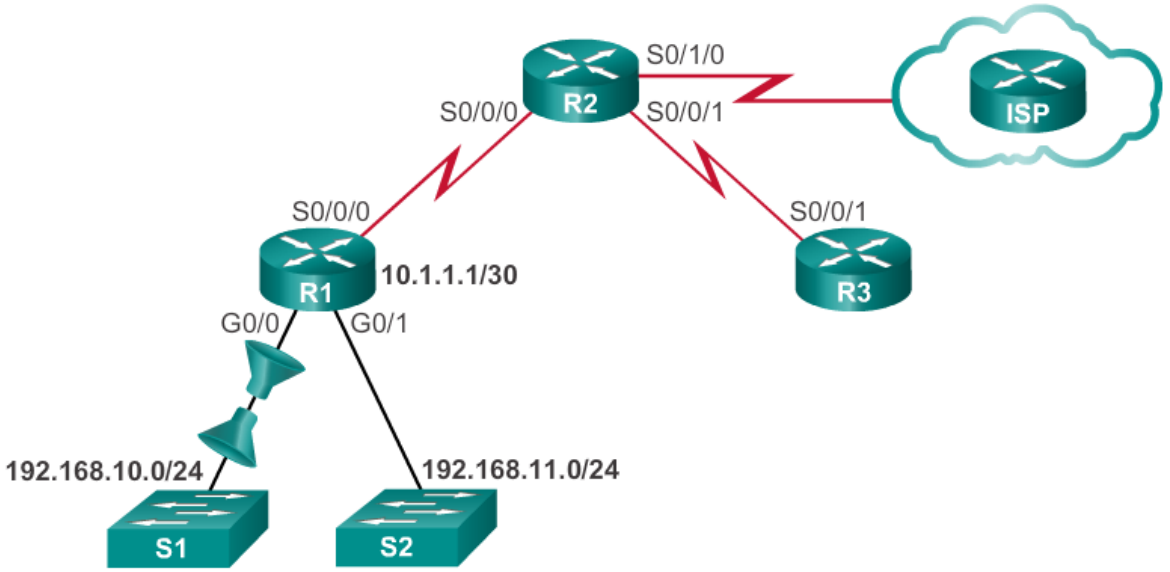
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

CONFIGURACION DE ACL EXTENDIDAS

Los pasos del procedimiento para configurar ACL extendidas son los mismos que para las ACL estándar. Primero se configura la ACL extendida y, a continuación, se activa en una interfaz. Sin embargo, la sintaxis de los comandos y los parámetros son más complejos, a fin de admitir las funciones adicionales proporcionadas por las ACL extendidas.

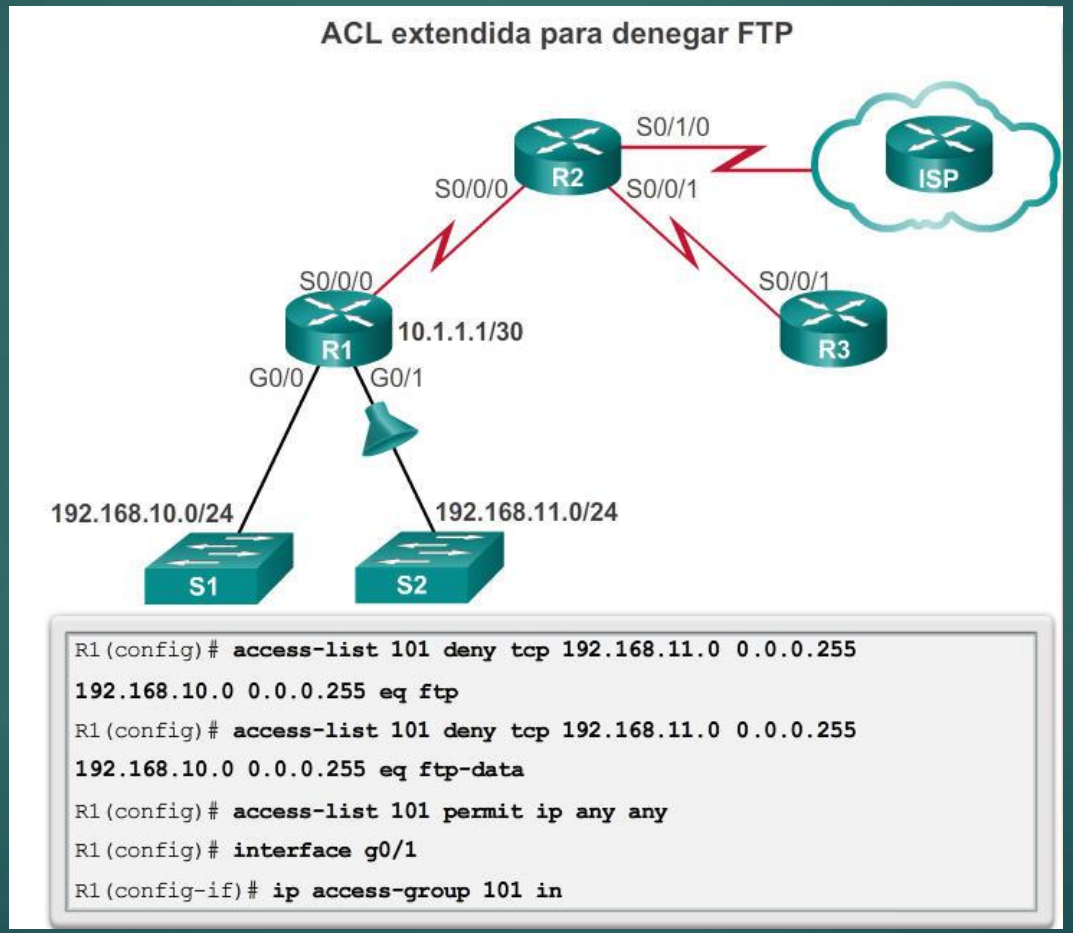
```
access-list access-list-number {deny | permit | remark}
protocol source [source-wildcard] [operator operand]
[port port-number or name] destination [destination-wildcard]
[operator operand] [port port-number or name][established]
```

APLICACIÓN DE ACL EXTENDIDA



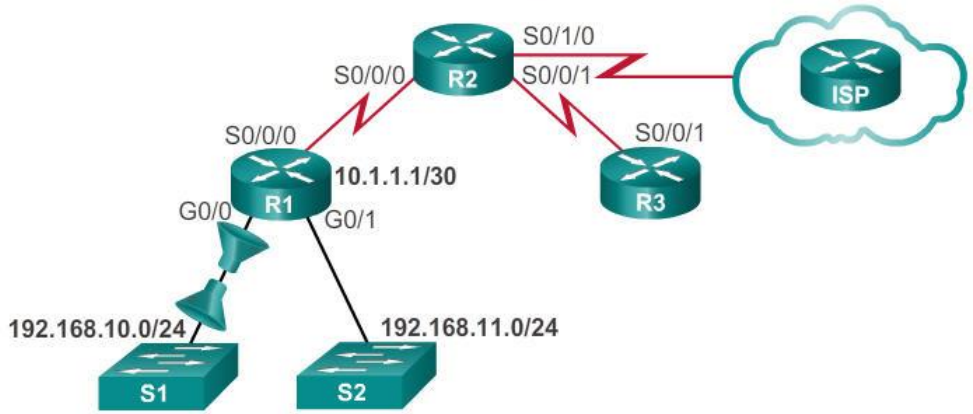

```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

FILTRADO DE TRAFICO



CREACION DE ACL EXTENDIDAS

Creación de ACL extendidas con nombre




```
R1(config)#ip access-list extended SURFING
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended BROWSING
R1(config-ext-nacl)#permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)#exit
R1(config)#interface g0/0
R1(config-if)#ip access-group SURFING in
R1(config-if)#ip access-group BROWSING out
```

VERIFICACION DE ACL EXTENDIDAS

```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted for brevity>
  Outgoing access list is BROWSING
  Inbound  access list is SURFING
<output omitted for brevity>
```

LOGICA DE ACL DE ENTRADA

- Los paquetes se prueban en relación con una ACL de entrada, si existiera una, antes de enrutarlos.
- Si un paquete entrante coincide con una instrucción de ACL con un permiso, se envía para enrutarlo.
- Si un paquete entrante coincide con una instrucción de ACL con una denegación, se descarta y no se enruta.
- Si un paquete entrante no coincide con ninguna instrucción de ACL, se “deniega implícitamente” y se descarta sin enrutarlo.

LOGICA DE ACL DE SALIDA

- Antes de enviar los paquetes a una interfaz de salida, se comprueba que tengan una ruta. Si no hay ruta, los paquetes se descartan.
- Si una interfaz de salida no tiene ninguna ACL, los paquetes se envían directamente a esa interfaz.
- Si hay una ACL en la interfaz de salida, se la verifica antes de que los paquetes se envíen a esa interfaz.
- Si un paquete saliente coincide con una instrucción de ACL con un permiso, se lo envía a la interfaz.

CREACION DE ACL CON NOMBRE

```
Router(config)# ip access-list [standard | extended] name
```

La cadena de nombres alfanuméricos debe ser única y no puede comenzar con un número.

```
Router(config-std-nacl)# [permit | deny | remark] {source
[source-wildcard]} [log]
```

```
Router(config-if)# ip access-group name [in | out]
```

Activa la ACL de IP con nombre en una interfaz.