# Tema 4

## LISTAS DE ACCESO

# ACL: Access Control List

- Listas de control de acceso o filtro a los paquetes en los routers de Cisco, para actuar como cortafuegos
- Pueden actuar a nivel de direcciones, protocolos y puertos: capas 3 y 4
- Se puede definir diferentes ACLs y luego instalarlas sobre los interfaces del router según convenga al administrador de la red

# Listas de control de acceso

- Cada ACL es un conjunto de sentencias que filtran a cada paquete en la interfaz instalada
- Cada ACLs sobre cada interfaz, actúa en un sentido , distinguiendo tanto sentido de entrada como de salida

# Definición de ACLs

- Las listas son secuencias de sentencias de permiso (permit) o denegación (deny) y que se aplican a los paquetes que atraviesan dicha interfaz, en el sentido indicado (in/out), con riguroso orden según hayan sido declaradas .
- Cualquier tráfico que pasa por la interfaz debe cumplir ciertas condiciones que forman parte de la ACL.

# Función: Filtrar el tráfico

- Las ACL filtran el tráfico de red controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete para determinar si se debe enviar o descartar, según las condiciones especificadas en la ACL. Entre las condiciones de las ACL se pueden incluir la dirección origen o destino del tráfico, el protocolo de capa superior, u otra información.

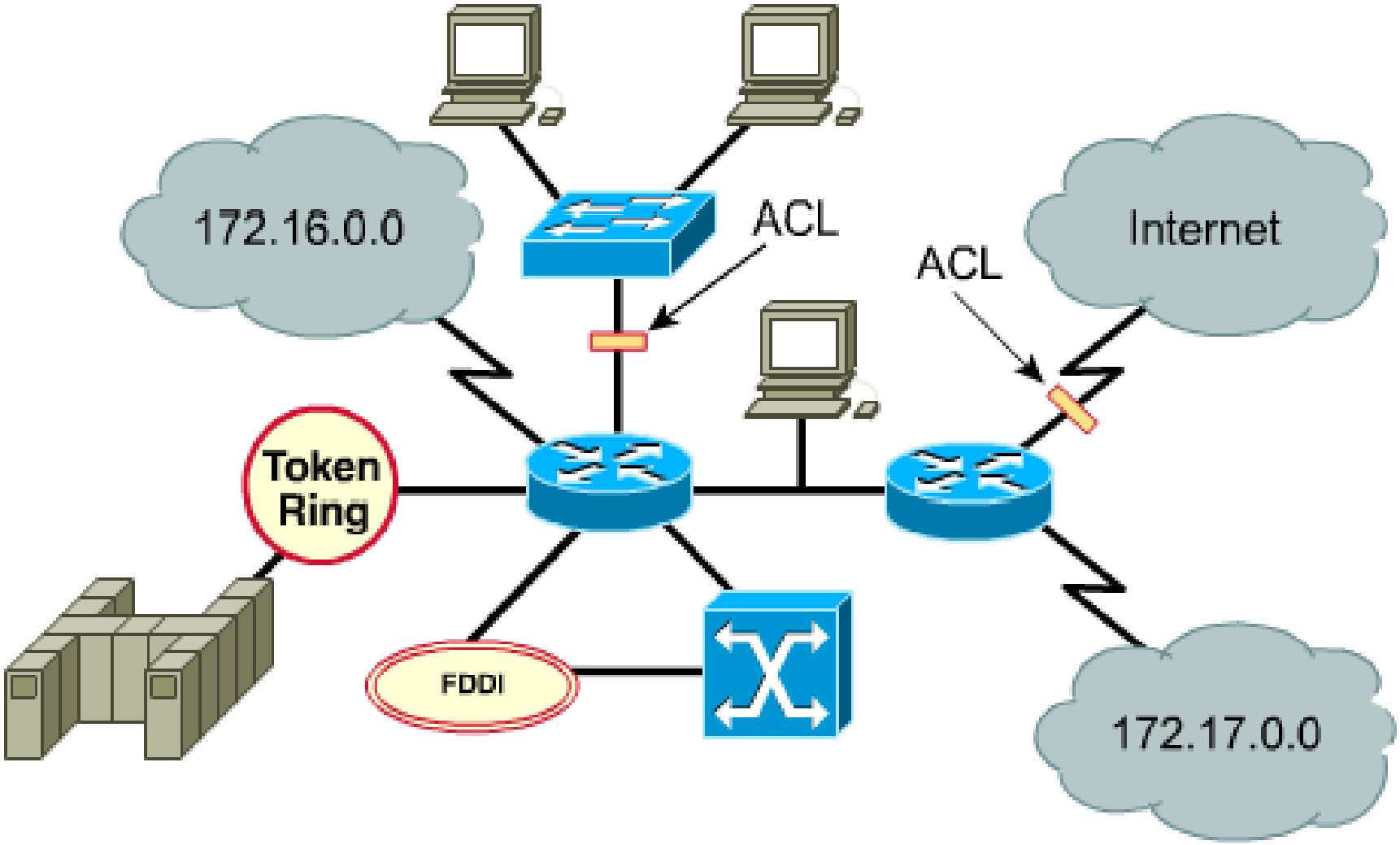
# Diferentes protocolos

- Las ACL se deben definir por protocolo. En otras palabras, es necesario definir una ACL para cada protocolo habilitado en una interfaz si desea controlar el flujo de tráfico para esa interfaz. Por ejemplo, si la interfaz de router estuviera configurada para IP, AppleTalk e IPX, sería necesario definir por lo menos tres ACL.

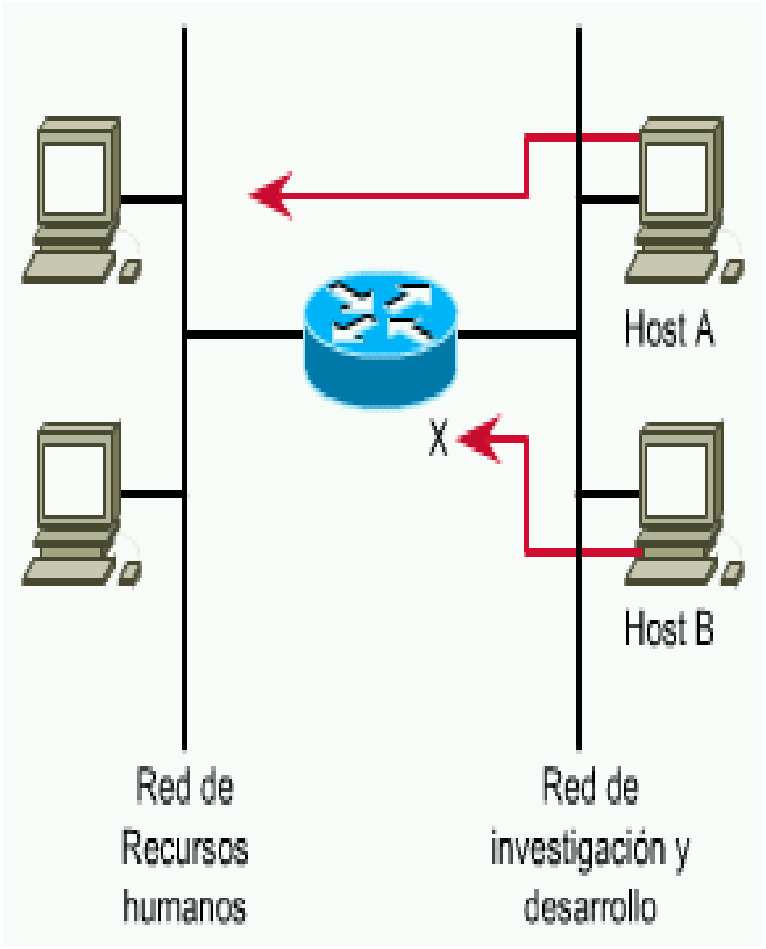
# Justificación de ACLs

Pueden ser utilizadas para priorizar tráfico, para mejorar el rendimiento de una red, restringir acceso de tráfico no deseado, aumentar la seguridad, introducir control administrativo o de protocolos como e-mails, ...

OTRAS...

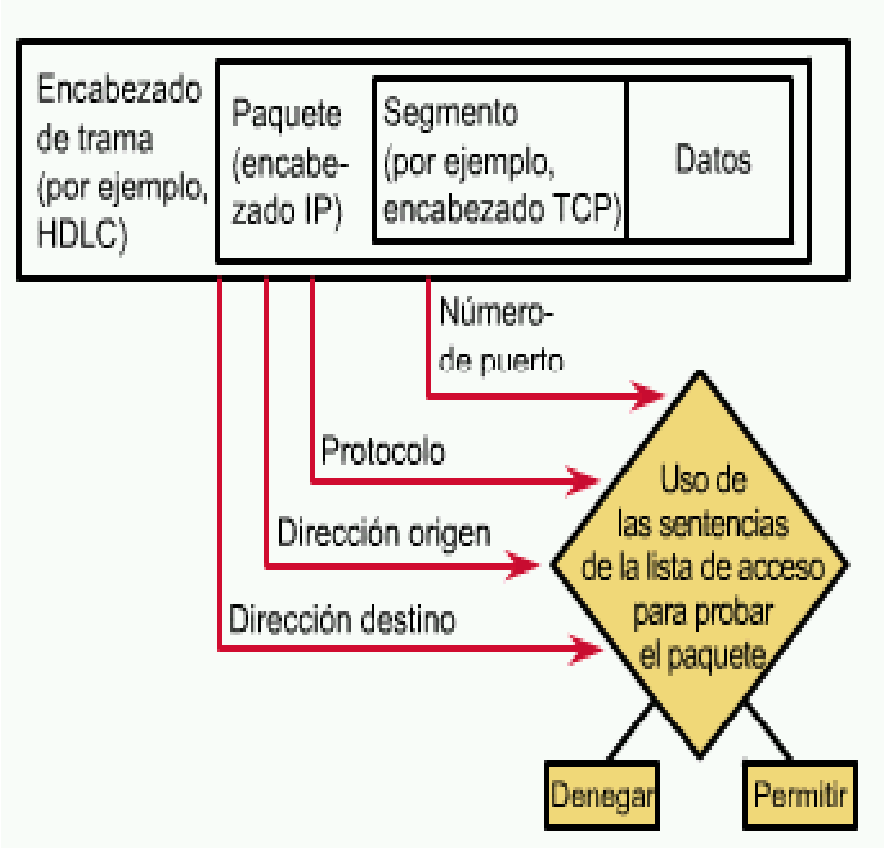

172.16.0.0
ACL
ACL
Internet
Token
Ring
FDDI
172.17.0.0

# Posibles usos de ACL’s



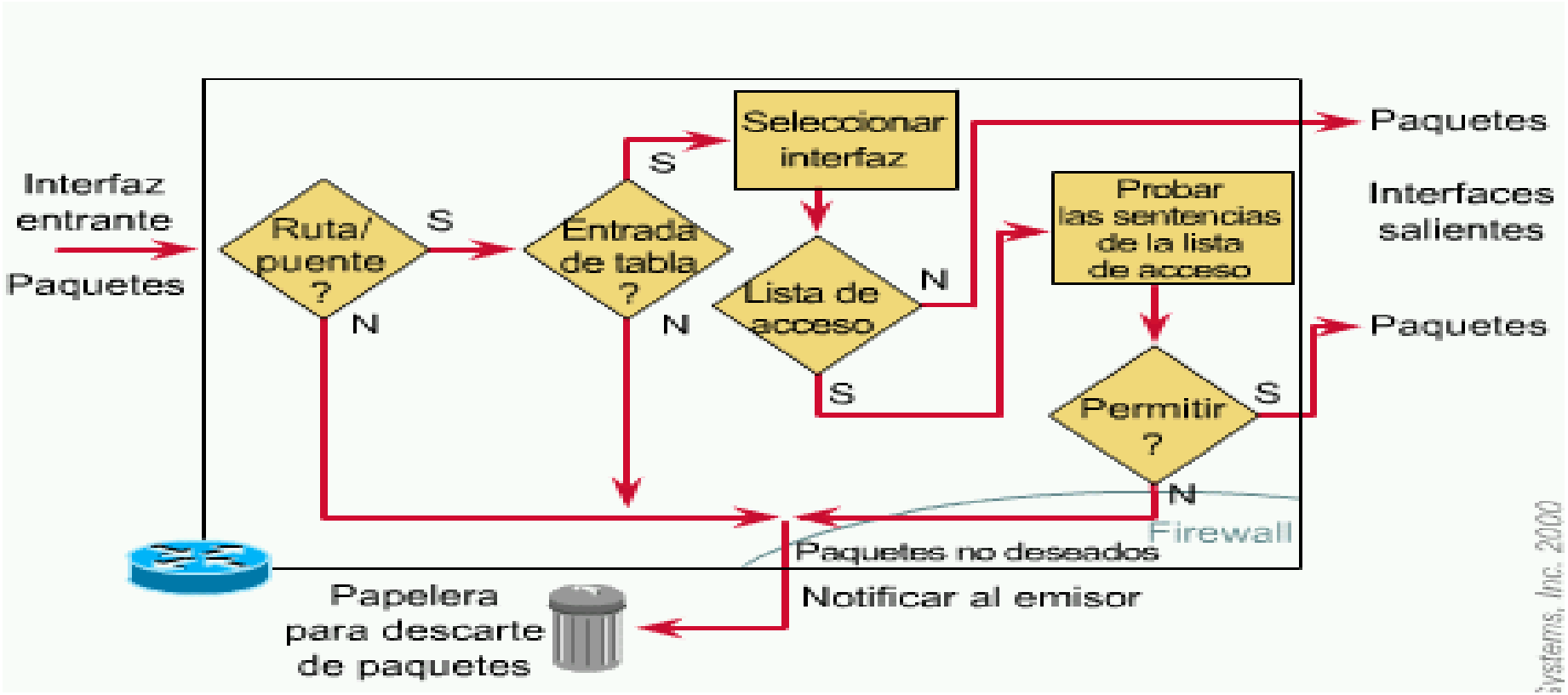

- **Limitar el tráfico de red y mejorar el rendimiento de la red.** Por ejemplo, las ACL pueden designar ciertos paquetes para que un router los procese antes de procesar otro tipo de tráfico, según el protocolo.
- **Brindar control de flujo de tráfico.** Por ejemplo, las ACL pueden restringir o reducir el contenido de las actualizaciones de enrutamiento.
- **Proporcionar un nivel básico de seguridad para el acceso a la red.** Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área.
- **Se debe decidir qué tipos de tráfico se envían o bloquean en las interfaces del router.** Por ejemplo, se puede permitir que se enrute el tráfico de correo electrónico, pero bloquear al mismo tiempo todo el tráfico de telnet**.**

# Verificación de encabezados de paquete y de capa superior




- Después de que una sentencia de ACL verifica un paquete para ver si existe coincidencia, al paquete se le puede denegar o permitir el uso de una interfaz en el grupo de acceso. Las ACL de Cisco IOS verifican los encabezados de paquete y de capa superior.

# ¿Cómo funcionan?

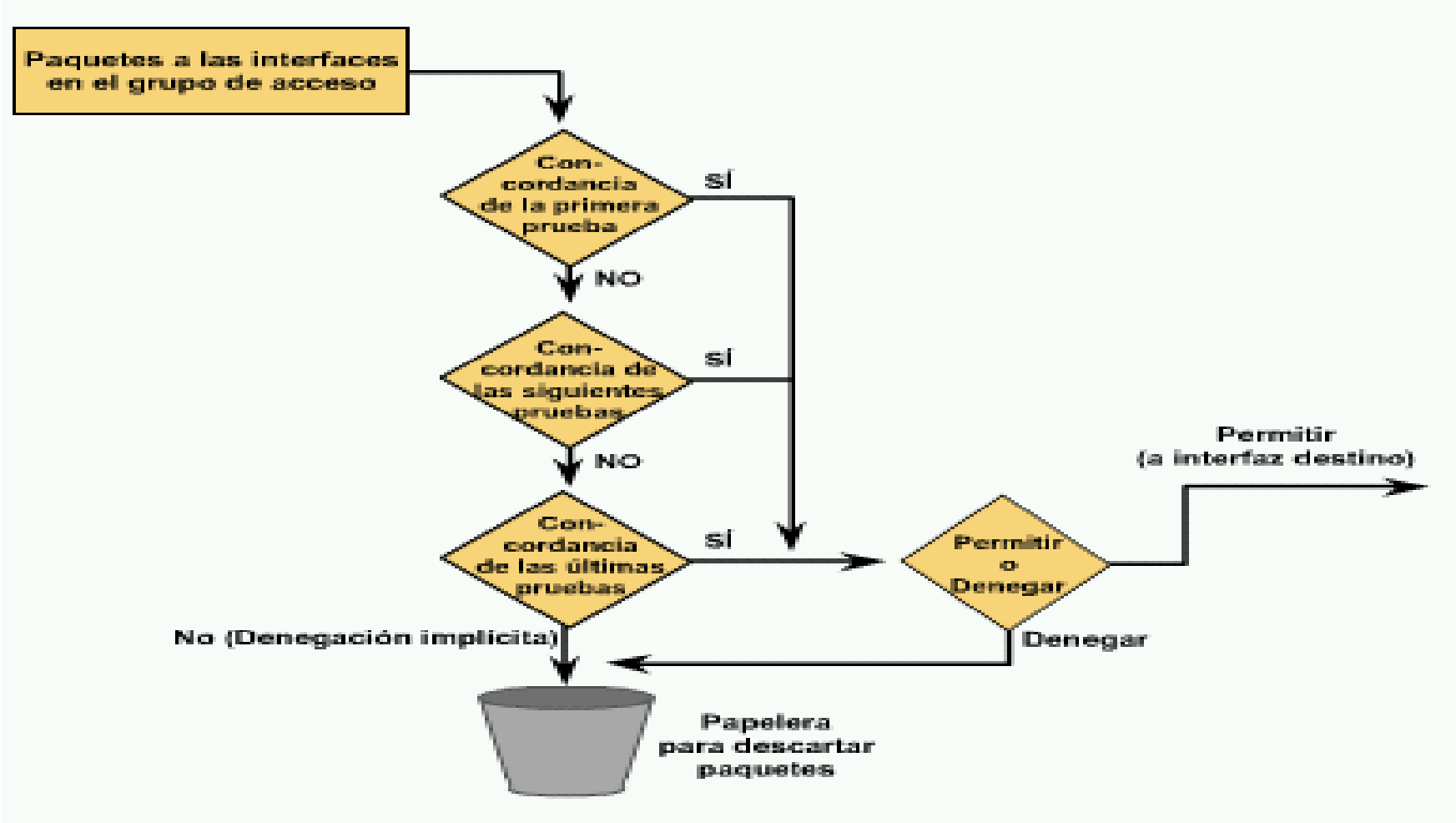



Cuando un paquete accede a una interfaz, el router comprueba si es enrutable o puenteable. Comprueba si la interfaz de entrada tiene ACL y si la hay se comprueban las condiciones. Si se permite el paquete, se coteja con las entradas de la tabla ...

# Declaración de ACLs

- Al conjunto de sentencias que forman la ACL se le llama grupo
- Los **pasos a seguir** para crear una ACL son:
  - definimos la lista que formará un grupo
    - access-list ***número*** .....sentencia..
    - access-list ***número*** .....sentencia..
    - **La última sentencia implícitamente es negar ( deny any)**
  - luego aplicamos dicha ACL sobre los interfaces en el sentido deseado con
    - ip access-group ***número (in/out)***

# Flujo en la comparación de ACL's




**Se manda paquete ICMP**
**Destino inalcanzable**

# Tareas clave para la creación de ACL

- Las ACL se crean utilizando el modo de configuración global.
- Al especificar un número de ACL del 1 al 99 se instruye al router que debe aceptar las sentencias de las ACL estándar. Al especificar un número de ACL del 100 al 199 se instruye al router para aceptar las sentencias de las ACL extendidas.
- Se deben seleccionar y ordenar lógicamente las ACL de forma muy cuidadosa. Los protocolos IP permitidos se deben especificar; todos los demás protocolos se deben denegar.
- Se deben seleccionar los protocolos IP que se deben verificar; todos los demás protocolos no se verifican. Más adelante en el procedimiento, también se puede especificar un puerto destino opcional para mayor precisión.

# Consideraciones sobre ACL´s

- ***Agrupación de ACL en interfaces***
- El primer paso es crear una definición de ACL, y el segundo es aplicar la ACL a una interfaz.
- Las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente, según la configuración. **Las ACL salientes son generalmente más eficientes que las entrantes**, y por lo tanto siempre se prefieren. Un router con una ACL entrante debe verificar cada paquete para ver si cumple con la condición de la ACL antes de conmutar el paquete a una interfaz saliente.
- ***Asignación de un número único a cada ACL***
- Al configurar las ACL en un router, **se debe identificar cada ACL de forma exclusiva**, asignando un número a la ACL del protocolo. Cuando se usa un número para identificar una ACL, **el número debe estar dentro del intervalo específico de números que es válido para el protocolo.**
- Se pueden especificar ACL por números para los protocolos enumerados para la tabla. La tabla también incluye el intervalo de números de ACL que es válido para cada protocolo.
- Después de crear una ACL numerada, debe asignarla a una interfaz para poderla usar. **Si desea alterar una ACL que contiene sentencias de ACL numeradas, necesita eliminar todas las sentencias en la ACL numerada mediante el comando** `no access-list` list-number.

# Pasos en la definición (1/2)

**Paso 1**

Definir la ACL utilizando el siguiente comando:

```
Router(config)# access-list access-list-number
   {permit | deny} {test-conditions}
```

Una sentencia global identifica la ACL. Específicamente, el intervalo 1-99 se reserva para IP estándar. Este número se refiere al tipo de ACL. En la versión 11.2 o posterior de Cisco IOS, las ACL también pueden usar un nombre de ACL, como educación_grupo, en lugar de un número

El término permitir o denegar de la sentencia ACL global indica cuántos paquetes que cumplen con las condiciones de prueba son manejados por el software Cisco IOS. Permitir generalmente significa que el paquete puede usar una o más interfaces que se especificaran posteriormente. El (Los) último(s) término(s) especifican las condiciones de prueba que utiliza la sentencia ACL.

# Pasos en la definición (2/2)

| | |
|---|---|
| **Paso 2** | A continuación, debe aplicar las ACL en una interfaz utilizando el comando access-group, como se muestra en el ejemplo.<br><br>`Router(config-if)# (protocol) access-group access-list-number`<br><br>Todas las sentencias ACL identificadas con access-list-number están relacionadas con una o más interfaces. Cualquier paquete que pase las condiciones de prueba de la ACL está habilitado para usar cualquier interfaz en el grupo de acceso de las interfaces. |

# Tipos de ACLs

Las ACLs se clasifican según el número utilizado en access-list ***número*** .....y que están definidos

1. Estandar IP 1-99
2. Extended IP 100-199
3. AppleTalk 600-699
4. IPX 800-899
5. Extended IPX 900-999
6. IPX Service Advertising Protocol 1000-1099

# ACLs: IP estándar y extended

## Se definen en modo global de configuración

Router(config)#

- Las ACLs estándar su formato es

**access-list** acl-number {**deny** | **permit**} source [source-wildcard ] [**log**]

- Las ACLs extended su formato es

**access-list** acl_number {**deny** | **permit**} proto **source** [source- wildcard] [operand port] **destination** [destination-wildcard] [operand port] [established] [**log**]

## A nivel de interfaz:

```
Router(config-if)#ip access-group access-list-number {in | out}
```

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

**proto**: ip, tcp, udp, icmp, gre, igrp

**operation operand**: lt(less than), gt(greater than), eq (equal), neq (non equal) y un número de puerto

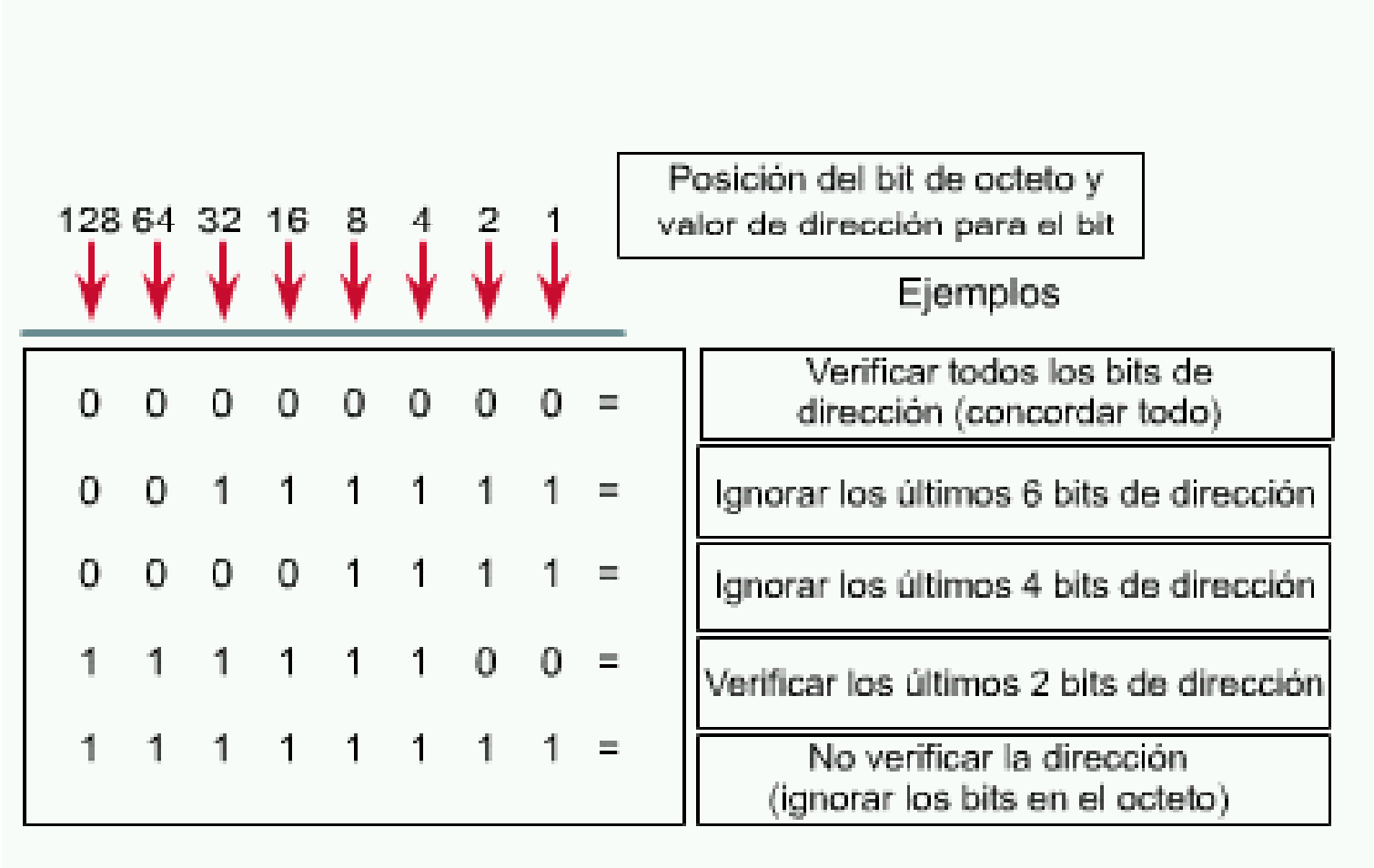
**established**: si la conexión TCP está establecida con acks

# Máscara (wildcard) 1/2

- En las direcciones IP especificadas, para cada bit de la dirección se especifica con una máscara si se comprueba o no dicho bit:
  - 0 indica bit a chequear
  - 1 indica bit a ignorar

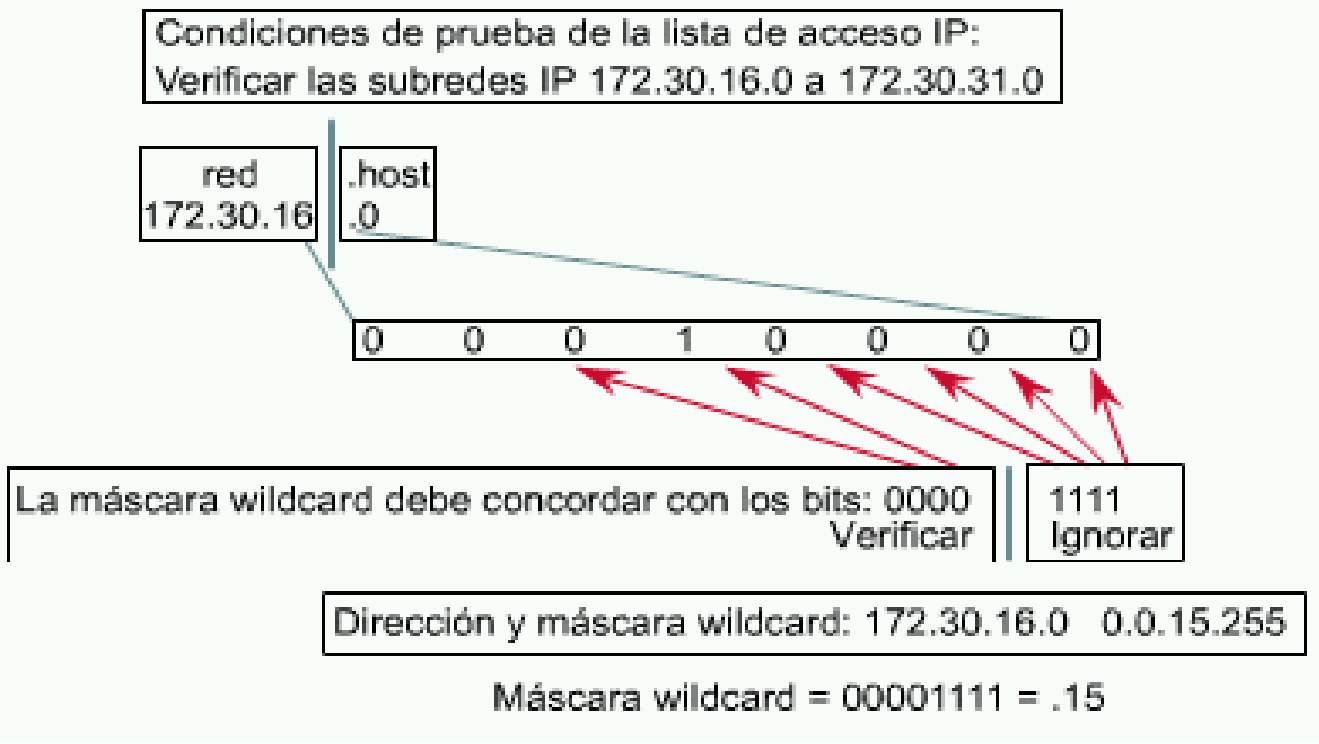
  Su significado es justo la inversa de los bits en las máscaras de las subredes.

# Máscara (wildcard) 2/2



# Ejemplo de máscara

La dirección IP 172.30.16.0 con máscara 0.0.15.255 evalua las subredes 172.30.16.0 hasta 172.30.31.0.



# Términos Any y host

- Si especificamos que cualquiera cumple la sentencia pondríamos como dirección IP 0.0.0.0 y de máscara todo 1’s para que se ignore (255.255.255.255), por tanto la palabra **any** sustituye a 0.0.0.0 255.255.255.255
- Si especificamos una dirección IP determinada, daremos la dirección y luego la máscara de todo 0’s, que se simplifica con la palabra **host**

# Ejemplos any y host

## ANY

**access-list 1 permit 0.0.0.0 255.255.255.255**

Se puede poner como

**access-list 1 permit any**

## HOST

**access-list** 1 permit 172.30.16.29 0.0.0.0

Se puede poner como

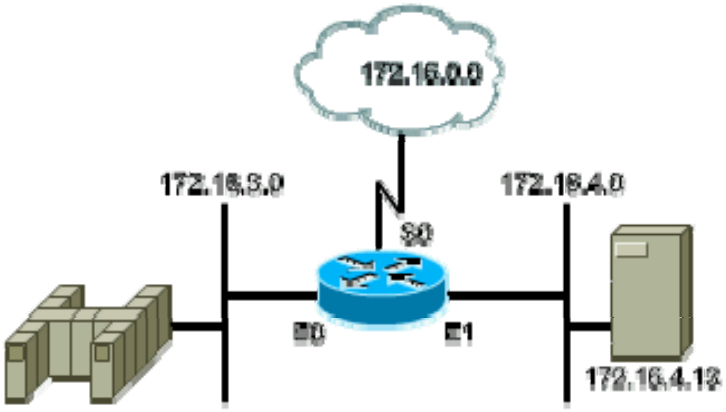
**access-list** 1 permit host 172.30.16.29

# ACL’s estándar


Estándar
- Especificaciones de dirección más simples
- Por lo general permite o deniega un conjunto de protocolo completo

Extendido
- Especificaciones de dirección más complejas
- Por lo general permite o deniega protocolos específicos

# Ejemplo1: ACL estándar




Resultado del comando

```
access-list 1 permit 172.16.0.0  0.0.255.255
(implícitamente "denegar cualquiera"
- no visible en la lista)
(access-list 1 deny 0.0.0.0  255.255.255.255)
interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```

- En este ejemplo, la ACL sólo permite que se envíe el tráfico desde la red origen 172.16.0.0. El tráfico que no es de 172.16.0.0 se bloquea. El ejemplo muestra cómo la ACL sólo permite que se envíe el tráfico desde la red origen 172.16.0.0 y que se bloquee el que no es de 172.16.0.0.

# Ejemplo2: Denegar un host específico

**Resultado del comando**

```
access-list 1 deny 172.16.4.13  0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny any)
(access-list 1 deny 0.0.0.0  255.255.255.255)

interface ethernet 0
ip access-group 1 out
```

- ACL para bloquear el tráfico proveniente de una dirección específica, 172.16.4.13, y para permitir que todo el tráfico restante sea enviado en la interfaz Ethernet 0. El primer comando **`access-list`** usa el parámetro deny para denegar el tráfico del host identificado. La máscara de dirección 0.0.0.0 en esta línea requiere que en la prueba coincidan todos los bits.
- En el segundo comando **`access-list`** la combinación de máscara wildcard / dirección IP 0.0.0.0 255.255.255.255 identifica el tráfico de cualquier origen.

# Ejemplo 3: Denegar un dirección de red

**Resultado del comando**

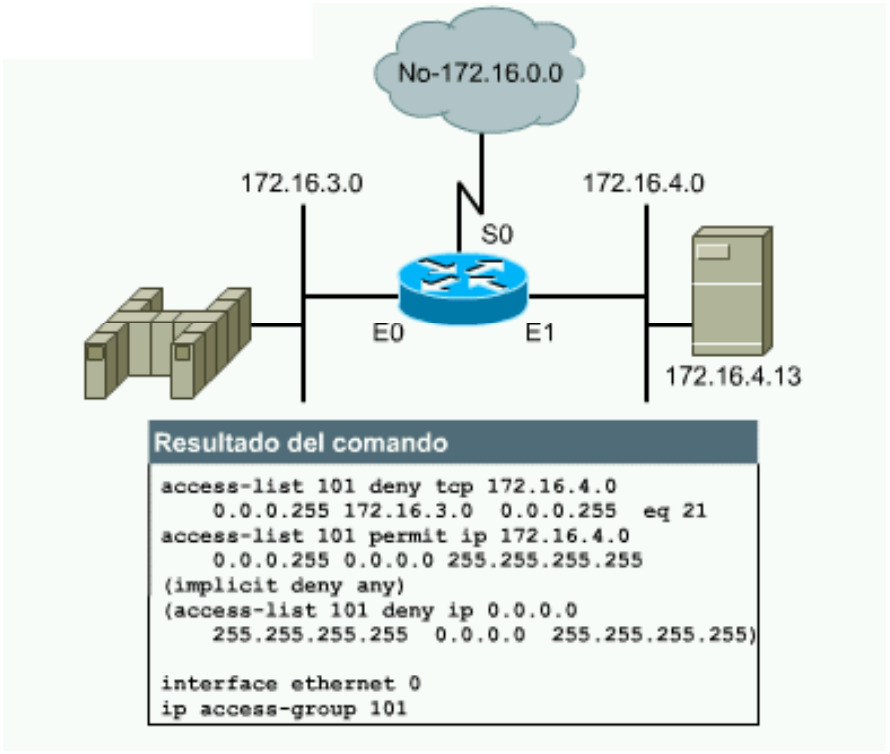
```
access-list 1 deny 172.16.4.0  0.0.0.255
access-list 1 permit any
(implicit deny any)
access-list 1 deny any

interface ethernet 0
ip access-group 1 out
```

- El ejemplo muestra cómo una ACL está diseñada para bloquear el tráfico desde una subred específica, 172.16.4.0, y para permitir que el resto del tráfico sea enviado.

# Números de puerto reservados

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

# Ejemplo 4:  ACL extendida que bloquea el tráfico de FTP.




- Observe que el bloqueo del puerto 21 evita que se transmitan los comandos FTP, evitando de esta manera las transferencias de archivo FTP. El bloqueo del puerto 21 evita que el tráfico mismo se transmita, pero no bloquea los comandos FTP. Los servidores FTP se pueden configurar fácilmente para funcionar en diferentes puertos. Se debe de entender que los números de puerto conocidos son simplemente eso: conocidos. No existen garantías de que los servicios estén en esos puertos, aunque normalmente lo están.

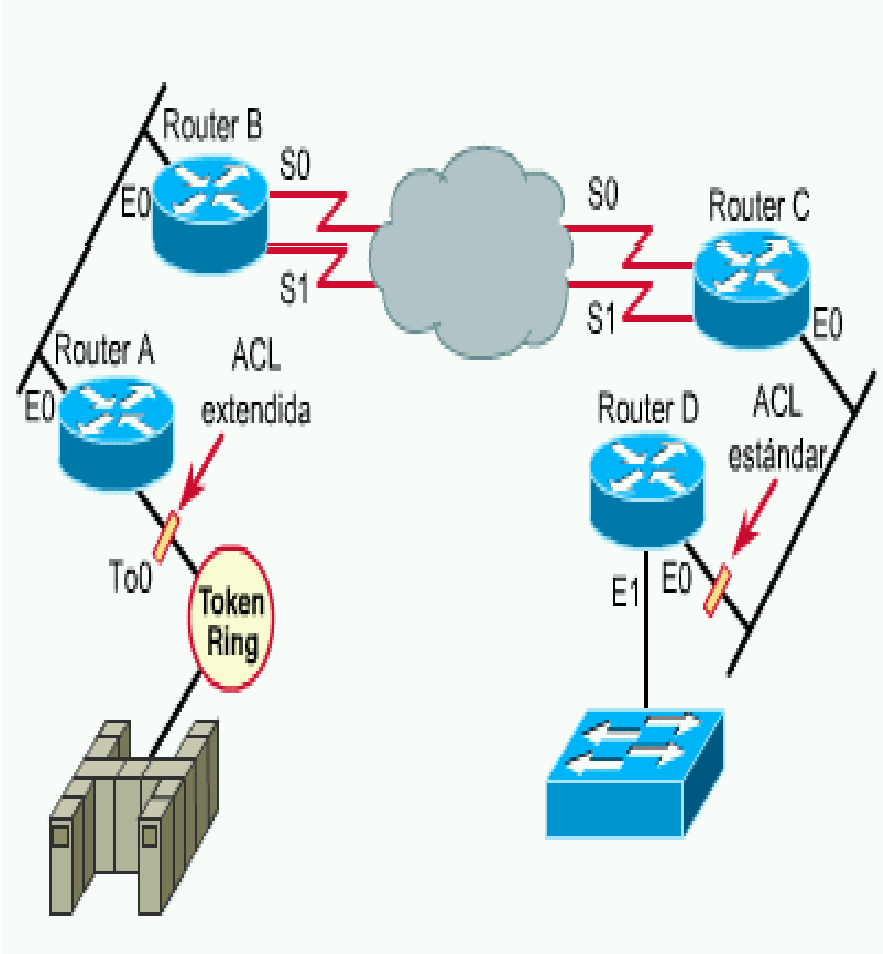
# Ejemplo 5: Denegar conexiones telnet de una subred

**Resultado del comando**

```
access-list 101 deny tcp 172.16.4.0  0.0.0.255 any eq 25
access-list 101 permit ip any any
(implicit deny any)
(access-list 101 deny ip 0.0.0.0  255.255.255.255
    0.0.0.0  255.255.255.255)

interface ethernet 0
ip access-group 101 out
```

- no permite que el tráfico de Telnet (eq 23) desde 172.16.4.0 se envíe desde la interfaz E0. Todo el tráfico desde cualquier otro origen a cualquier otro destino se permite, según lo indica la palabra clave **`any`**. La interfaz E0 está configurada con el comando **`access-group 101 out`** ; es decir, ACL 101 se encuentra enlazada a la interfaz saliente E0.

# Ubicación de las ACL´s




- La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado.
- Las ACL estándar no especifican direcciones destino, de manera que se debe colocar la ACL estándar lo más cerca posible del destino.
- Dentro de las interfaces se colocan en el sentido de salida, para no procesar tanto paquete

# ACL´s con nombre

- **Se usan cuando:**

  - Se desea identificar intuitivamente las ACL utilizando un nombre alfanumérico.

  -Existen más de 99 ACL simples y 100 extendidas que se deben configurar en un router para un protocolo determinado.

- **Hay que tener en cuenta que:**

  -Las ACL nombradas no son compatibles con las versiones Cisco IOS anteriores a la versión 11.2

  -No se puede usar el mismo nombre para múltiples ACL. Además, las ACL de diferentes tipos no pueden tener el mismo nombre. Por ejemplo, no es válido especificar una ACL estándar llamada Administración y una ACL extendida con el mismo nombre.

# Etiquetado de ACLs

```
Router(config)# ip access-list
  {standard | extended} name
ip access-list standard
  Internetfilter
  permit 128.88.0.0 0.0.255.255
  permit 36.0.0.0 0.255.255.255
  !(Note:all other access
  implicitly denied)
```

# Comandos DENY / PERMIT

- Se utiliza el comando de configuración de ACL **deny** para establecer condiciones para una ACL nombrada. La sintaxis completa del comando es: **deny** {source [source-wildcard] | **any**}
- Se usa la forma **no** de este comando para eliminar una condición de denegar, utilizando la siguiente sintaxis:
- no **deny** {*source* [source-wildcard] | **any**}

- Se utiliza el comando de configuración de lista de acceso **permit** para establecer condiciones para una ACL nombrada estándar. La sintaxis completa del comando es:
- **permit** {source [source-wildcard] | **any**} [**log**]
- Se usa la forma **no** de este comando para eliminar una condición de una ACL, utilizando la siguiente sintaxis:
- **no permit** {source [source-wildcard] | **any**}

# Ejemplo uso Deny / Permit

```
ip access-list standard Internetfilter
deny 192.5.34.0.0.0.0.255
permit 128.88.0.0.0.0.255.255
permit 36.0.0.0.0.255.255.255
! (Nota: cualquier otro acceso está denegado de forma implicita)
```

- En la figura establece una condición de denegar y permitir para una ACL estándar denominada Internetfilter

# Comandos del router

- **`show ip interface`** indicada si cualquier ACLs está establecida
- **`show access-lists`** muestra los contenidos de todas las ACLs

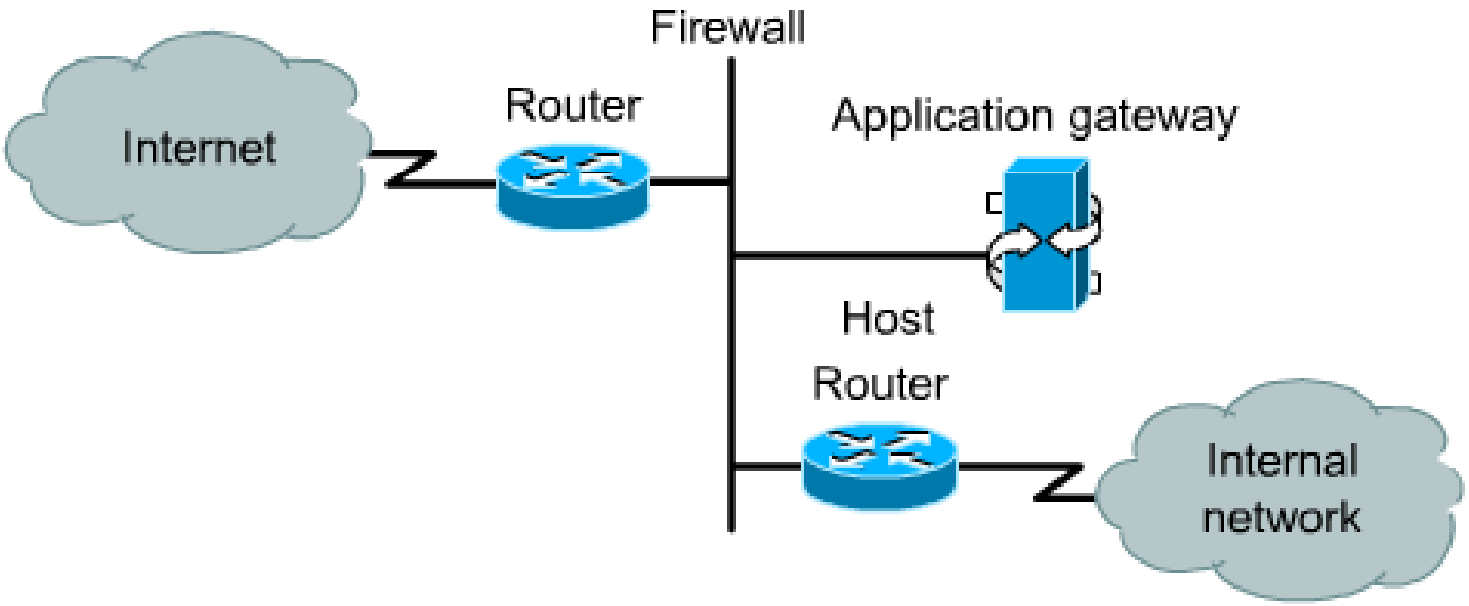
# Show ip interface. Resultado

```
Ethernet0 is up, line protocol is up
  Internet address is 192.54.22.2, subnet mask is 255.255.255.0
  Broadcast address is 255.255.255.255
  Address determined by nonvolatile memory
  MTU is 1500 bytes
  Helper address is 192.52.71.4
  Secondary address 131.192.115.2, subnet mask 255.255.255.0
  Outgoing ACL 10 is set
  Inbound ACL is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are never sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  Gateway Discovery is disabled
  IP accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
Router>
```

# ACL´S en routers fronterizos

- Para aprovechar las ventajas de seguridad de las ACL, como mínimo se deben configurar las ACL en los routers fronterizos, que son routers situados en las fronteras de la red. Esto proporciona protección básica con respecto a la red externa, u otra parte menos controlada de la red, para un área más privada de la red. En estos routers fronterizos, las ACL se pueden crear para cada protocolo de red configurado en las interfaces del router. Se pueden configurar las ACL para que el tráfico entrante, el tráfico saliente, o ambos, sean filtrados en una interfaz.

# Firewall Architecture




El router externo manda el tráfico a la pasarela.
El router interno sólo acepta tráfico de la pasarela.