# Access Control Lists (ACLs)

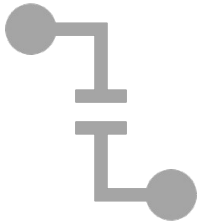
Redes II

# ¿Qué es una ACL?

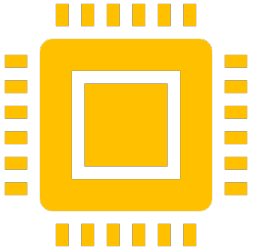
- ACLs son un conjunto de reglas utilizadas comúnmente para filtrar el tráfico de red.
- Son usadas en dispositivos de red con capacidad de “filtrado de paquetes” como los Routers y Firewalls.
- ACLs se aplican en una interfaz sobre los paquetes que salen o entran de la misma.

# Listas de control de acceso

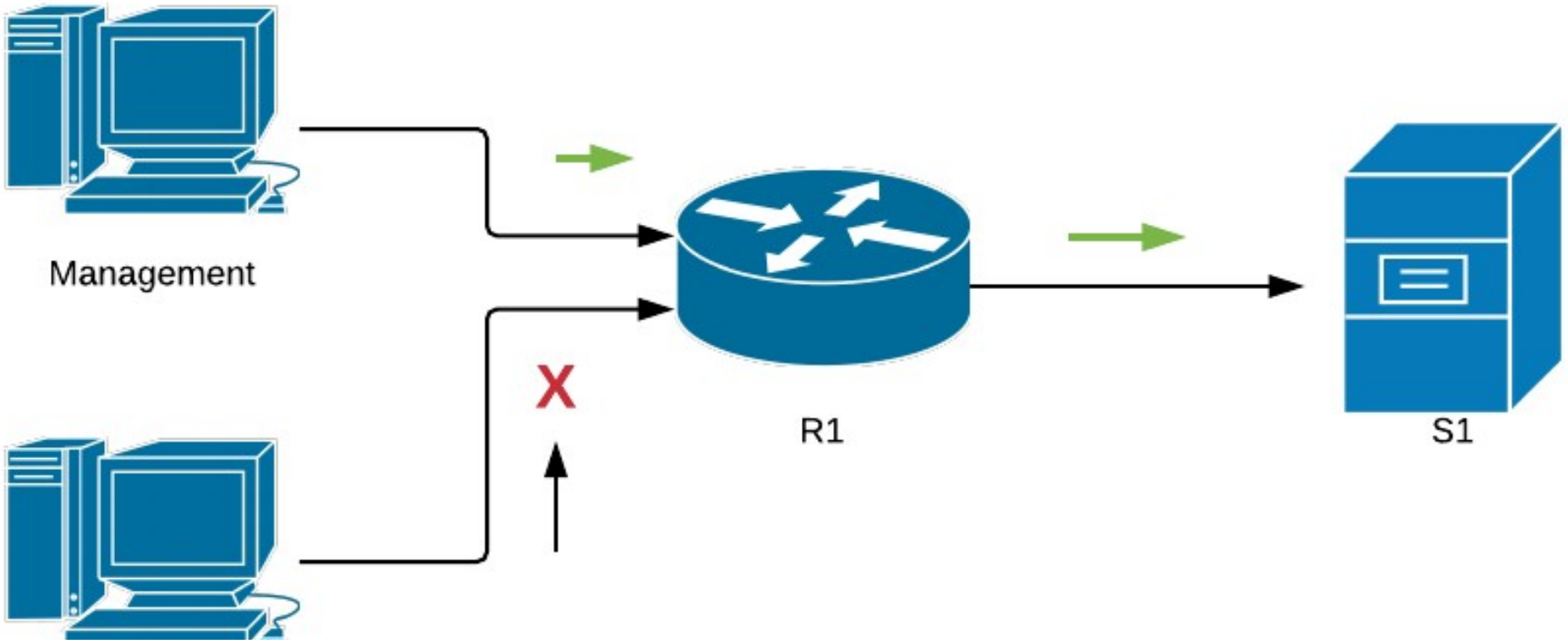
Las ACL proporcionan seguridad a una red.



Son utilizadas por los firewall para filtrar los paquetes no autorizados o potencialmente peligrosos e impiden que ingresen a la red.



En un router Cisco se puede configurar un firewall simple que proporcione capacidades básicas de filtrado mediante ACL.

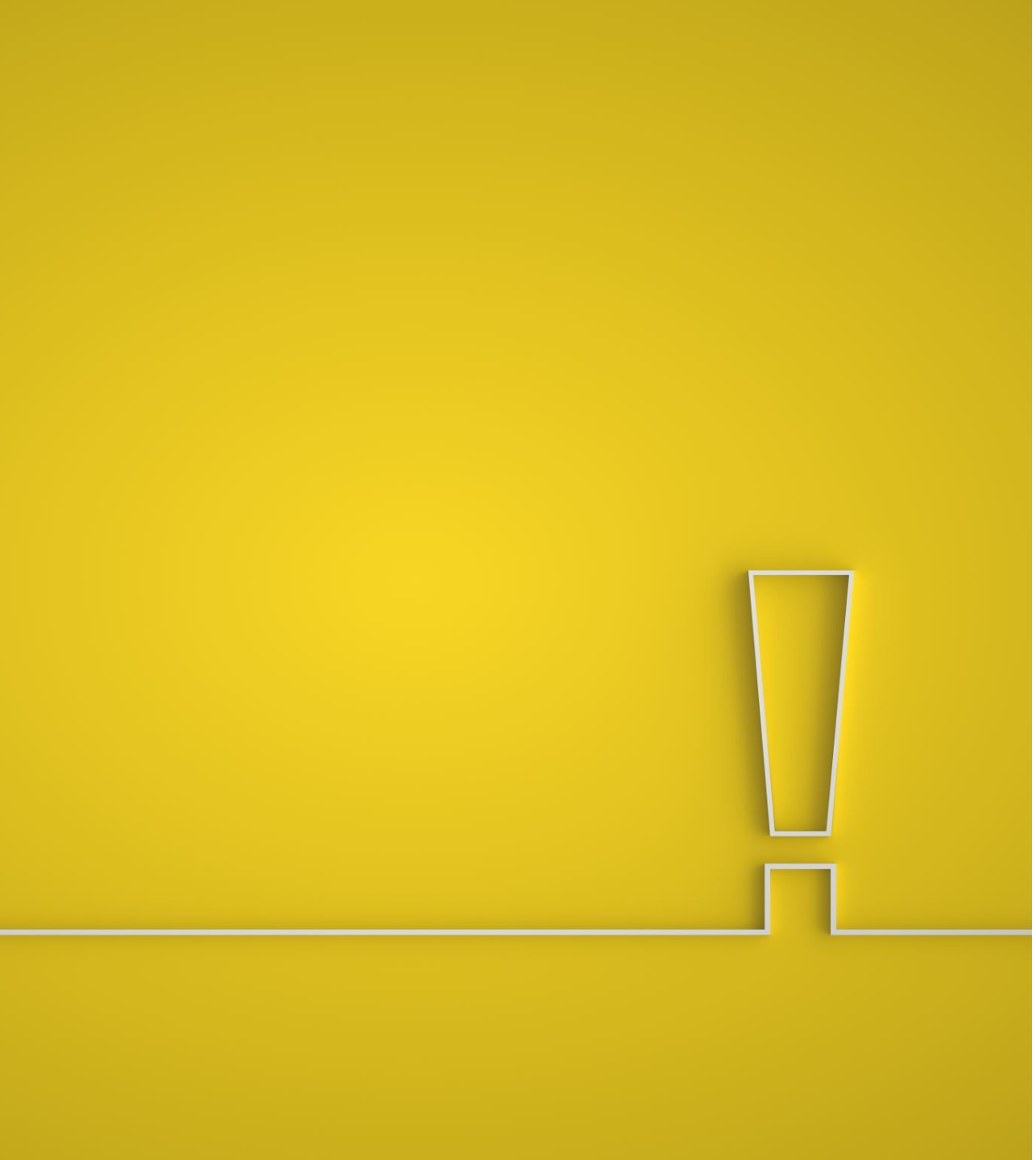



- Por ejemplo, el servidor S1 contiene algunos documentos importantes que deben estar disponibles únicamente para el personal administrativo. Podemos configurar un ACL en R1 para permitir el acceso a S1 únicamente a usuarios desde la red administrativa. Todo otro tráfico que vaya a S1 será bloqueado.

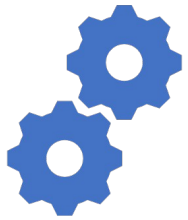
# Access Lists

Cada ACL tiene un “deny” implícito al final.

La ACL busca una coincidencia comenzando con la primera línea (top line), y cuando se encuentra la coincidencia, finaliza la búsqueda (se realiza una búsqueda secuencial). Las líneas restantes ya no son examinadas.



- Cuando un paquete ingresa y existe una interfaz que tiene aplicada una ACL, por lo menos un valor del paquete es comparado línea por línea contra la ACL. Generalmente será la IP de origen y/o la IP de destino.



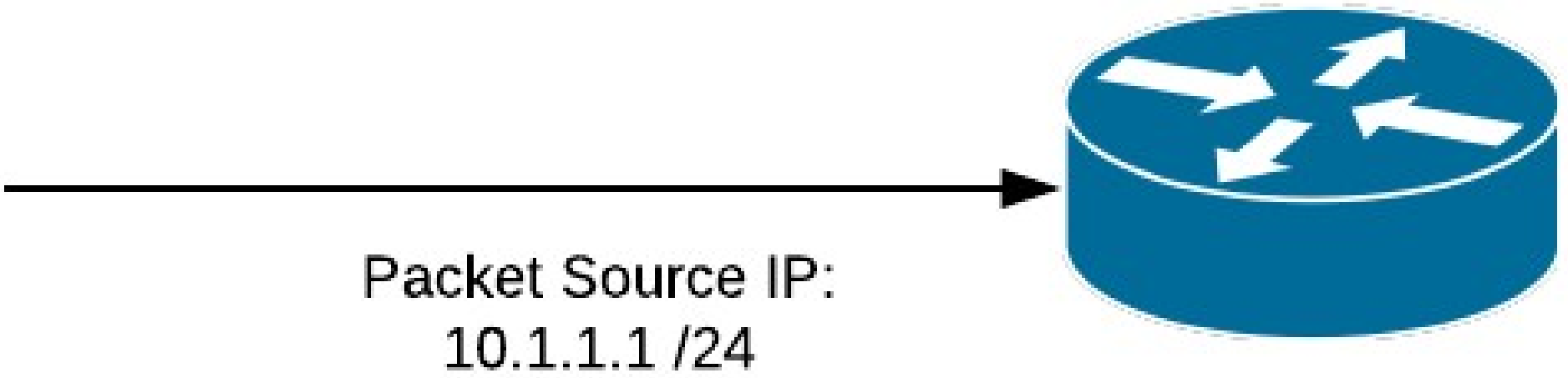
# Standard Access List

R1(config)#access-list 1 permit 10.1.1.1 0.0.0.0

R1(config)#access-list 1 permit 10.2.1.1 0.0.0.0

R1(config)#access-list 1 permit 10.3.1.1 0.0.0.0

R1(config)#access-list 1 permit 10.4.1.1 0.0.0.0




- ACLs estándar solo validan la dirección IP de origen de un paquete!

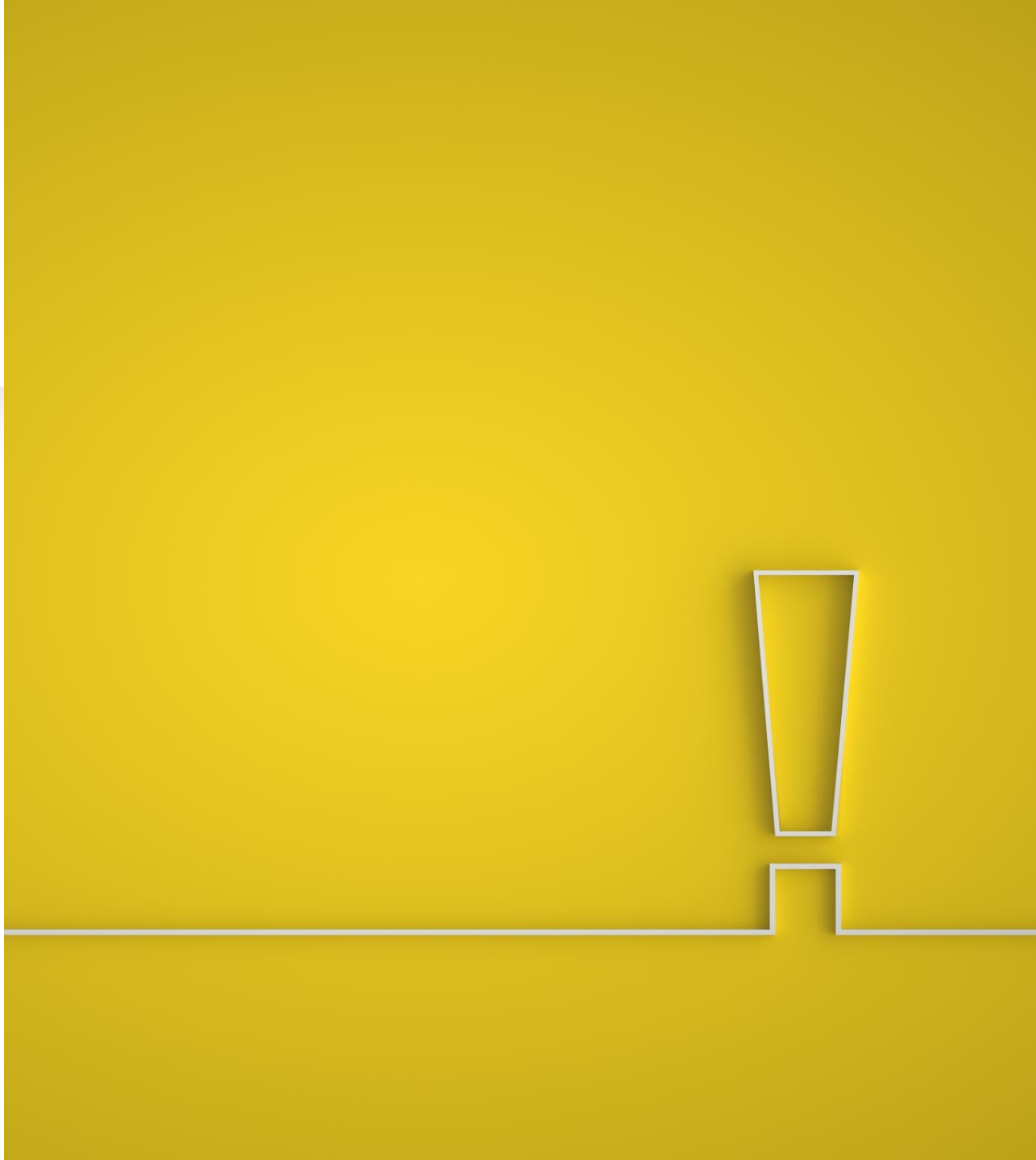
Cuando un paquete llega a una interfaz con la ACL 1 aplicada, la IP origen es comparada contra la ACL línea por línea. Si la IP origen coincide con la primer línea de la ACL, la acción apropiada de “permit” o “deny” es realizada, y finaliza el proceso completo. Si no existe coincidencia con la primer línea, el valor del paquete es comparado contra la segunda línea de la ACL, y así sucesivamente hasta que la coincidencia es encontrada.

Cuando ninguna coincidencia es encontrada, el “deny” implícito es aplicado al paquete. El “deny” implícito es realmente un “deny invisible” que no se encuentra escrito visiblemente. Al ser un “deny” no visible es muy fácil de olvidar que existe! especialmente si se es nuevo en el manejo de ACLs. Olvidar el “implicit deny” es la razón #1 por la que un ACL no brinde los resultados deseados.

# Wildcard Masking en ACLs

- Ceros significan bits que “Importan”, son bits que deben coincidir para que la ACL tome efecto.

- Unos son bits “No importantes”, bits que no tienen que coincidir en nada para que una línea de la ACL sea considerada una coincidencia. Son bits que no se toman en cuenta.



# Ejemplo

- Se necesita una ACL que permita paquetes del origen 196.17.100.0 /24 ingresar a la interfaz FastEthernet del Router, y paquetes de cualquier otro origen deben ser bloqueados.

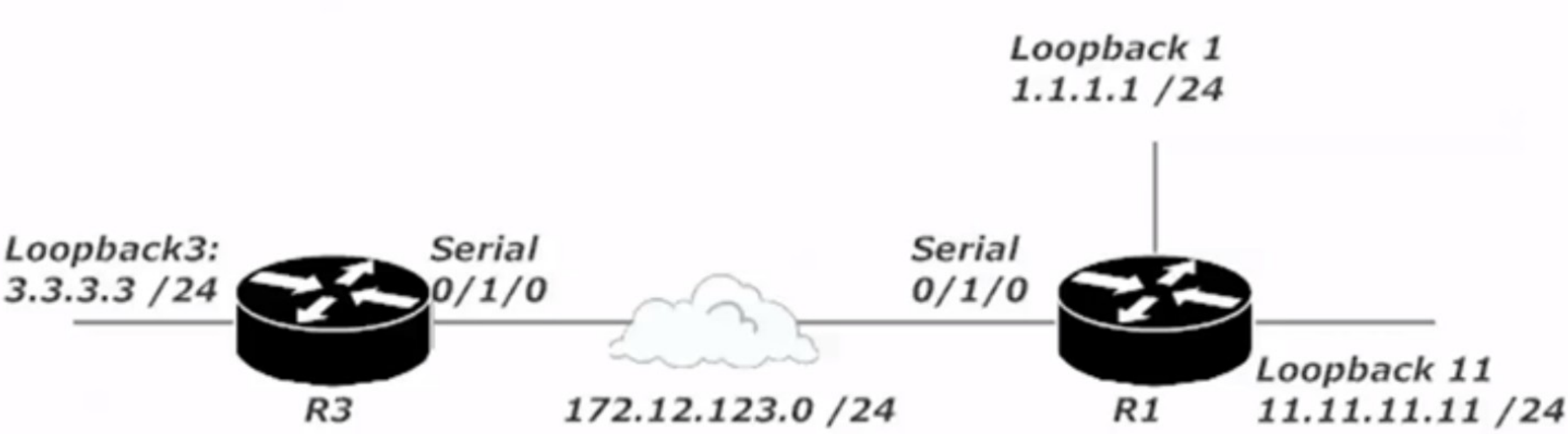
- Para lograr que lo anterior suceda, se necesita una ACL que permita pasar paquetes si la dirección IP de origen coincide con los tres primeros octetos exactamente (196.17.100).

| | 1st Octet | 2nd Octet | 3rd Octet | 4th Octet |
|---|---|---|---|---|
| All bits must match | 00000000 | | | |
| All bits must match | | 00000000 | | |
| All bits must match | | | 00000000 | |
| We don’t care! | | | | 11111111 |

- Solo se validarán los primeros tres octetos de la dirección de origen, ya que la wildcard tiene en 0 dichos octetos.

# Standard ACLs

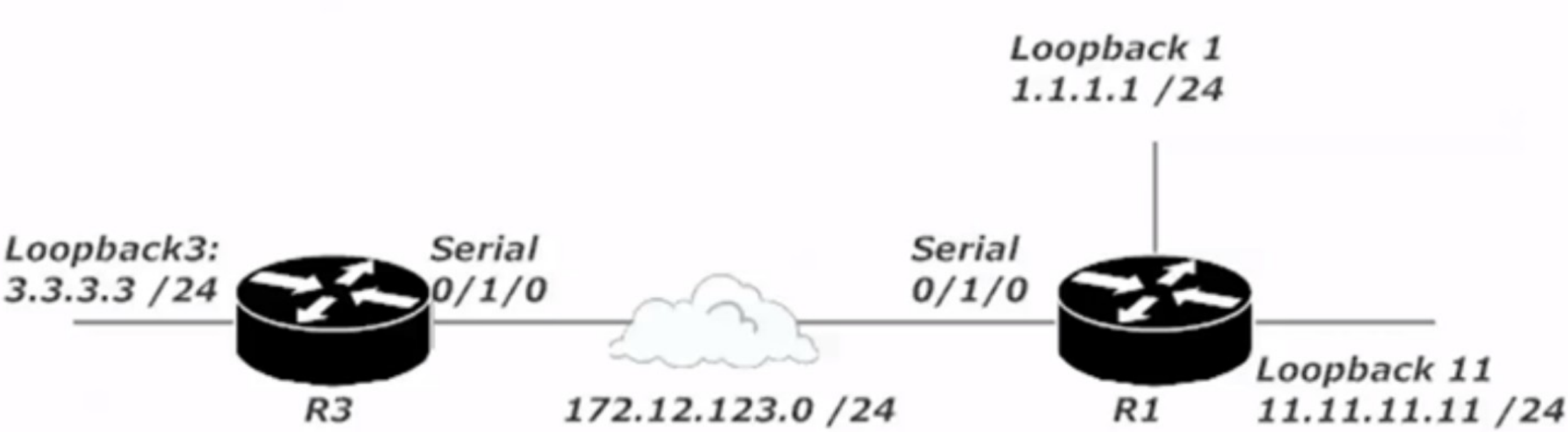
- Una ACL estándar está relacionada únicamente con la IP de origen del paquete.
- 1-99
- 1300-1999 (expanded range)
- Debido a que se limitan únicamente a las IP origen, estás ACLs son complicadas de utilizar en algunas situaciones, como la siguiente:




# Ejemplo práctico

Requerimientos:

- Bloquear el tráfico originado desde la subred 3.3.3.0 /24 si lleva como destino la subred 11.11.11.0 /24
- R1 debe aceptar paquetes desde la 3.3.3.0 /24 si se dirige a cualquier otra subred, incluyendo cualquier otra subred agregada en el futuro.
- La ACL debe ser aplicada en la interfaz serial de R1.




**Crear ACL:**

R1#conf t

R1(config)#access-list 5 deny 3.3.3.0 0.0.0.255

R1(config)#access-list 5 permit any

**Asociar ACL con interfaz:**

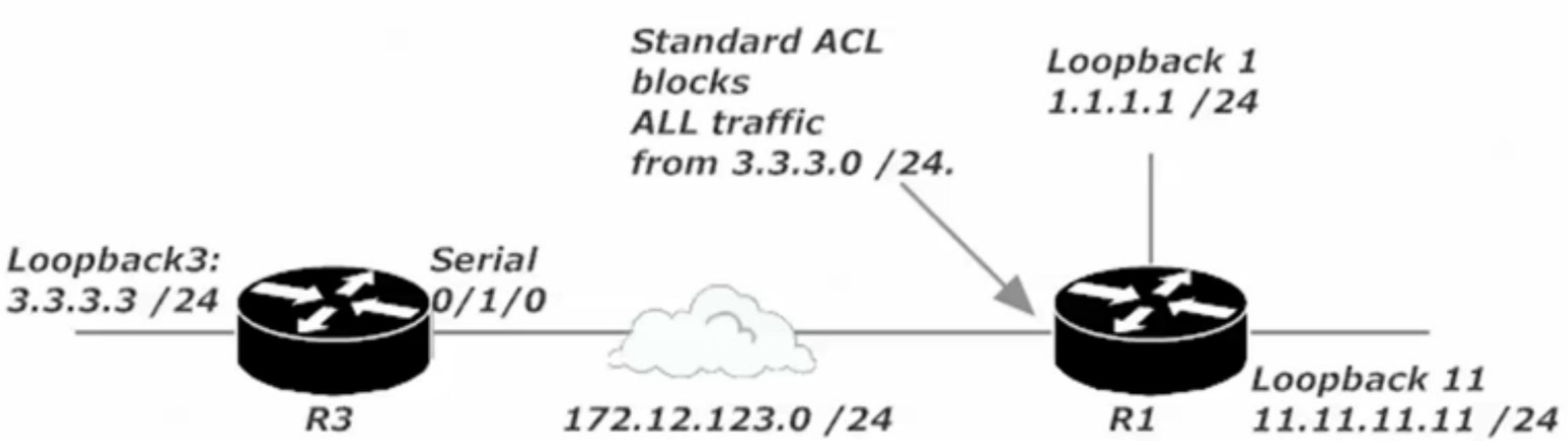
R1#conf t

R1(config)#interface serial 0/1/0

R1(config-if)#ip access-group 5 in

**Para mostrar ACLs creadas:**

R1#show ip access-list

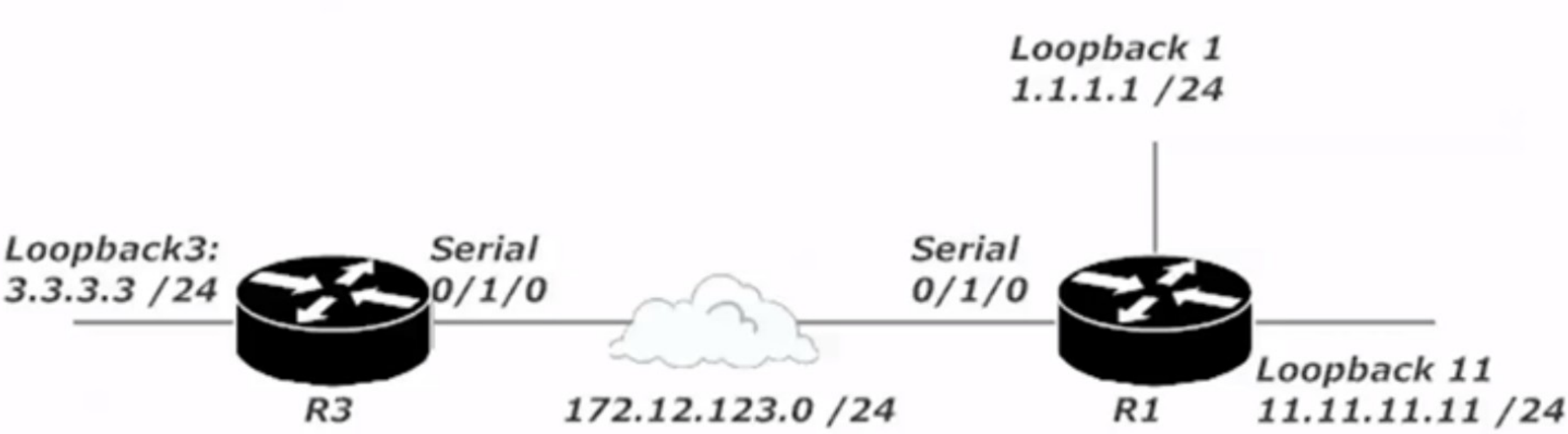



# Problema de ACLs estándar

# Extended ACLs

100 – 199

Source and destination address, protocols and port numbers.

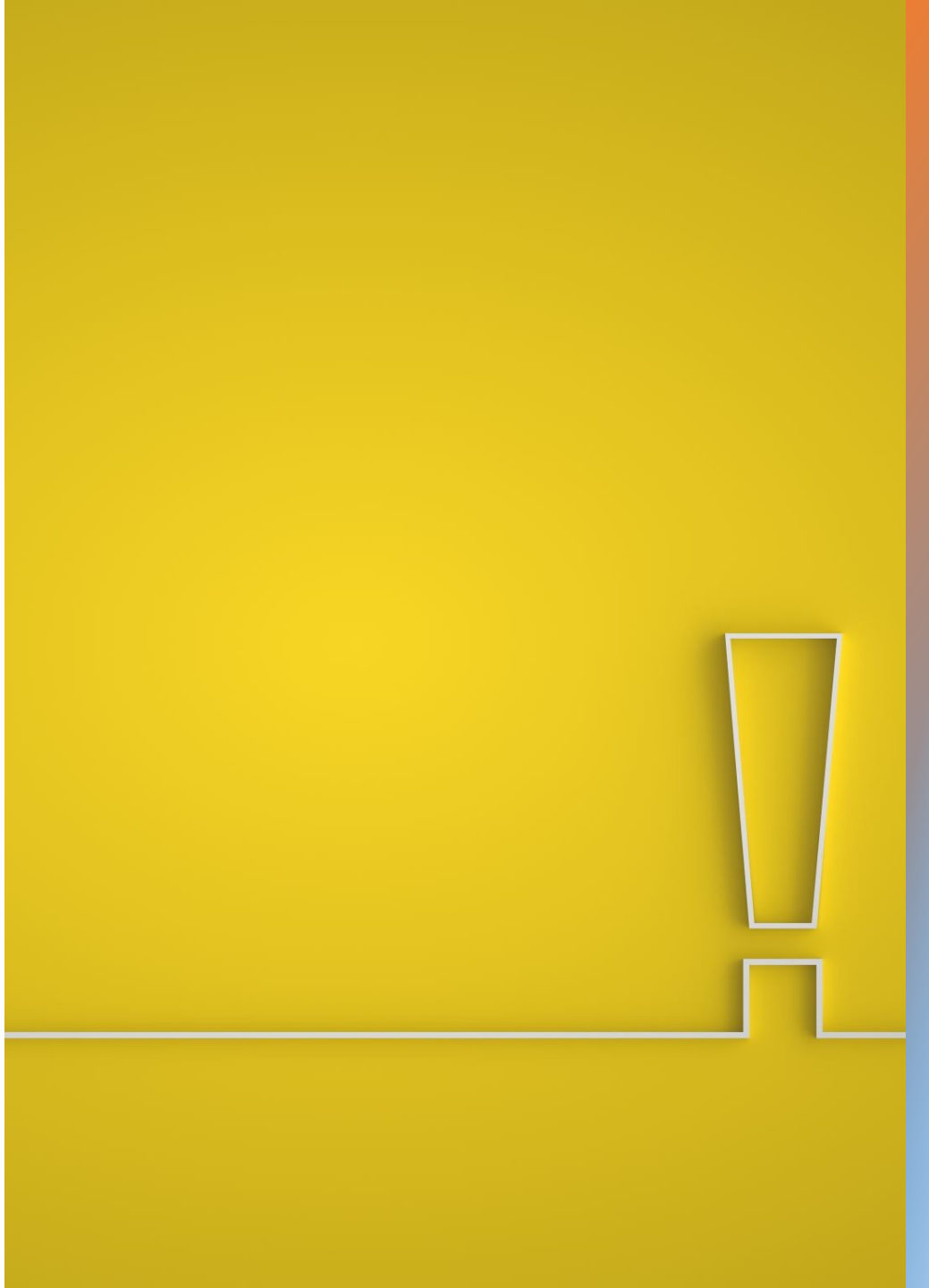



# Aplicación de extended ACLs

- R1(config)#access-list 100 deny ip 3.3.3.0 0.0.0.255 11.11.11.0 0.0.0.255
- R1(config)#access-list 100 permit ip any any

# Reglas para las ACL

- Un ACL por protocolo, por interfaz, por dirección
- Un deny implícito existe al final de cada ACL
- ACLs se leen de arriba hacia abajo línea por línea



# Configuración standard ACLs

**Forma 1:**

R1(config)#access-list <ACL_Number> permit|deny <IP_source> <Wildcard_mask>

**Forma 2:**

R1(config)#access-list <ACL_Number> permit|deny host <IP_source>

# Configuración extended ACLs

R1(config)#access-list <ACL_Number> permit|deny <protocol> <IP_source> <Wildcard_mask> [protocol information] <IP_destination> <Wildcard_mask> [protocol information]

# ¡Cuidado con el orden de las líneas en las ACLs!

- Poner una línea en el lugar equivocado en una ACL puede romper todo lo que se intenta hacer.
- Por ejemplo, necesitamos denegar el tráfico de 172.18.18.0 /24 mientras se permite el tráfico de cualquier otra subnet.
- ¿Cuál de las cuatro ACLs a continuación es la correcta?

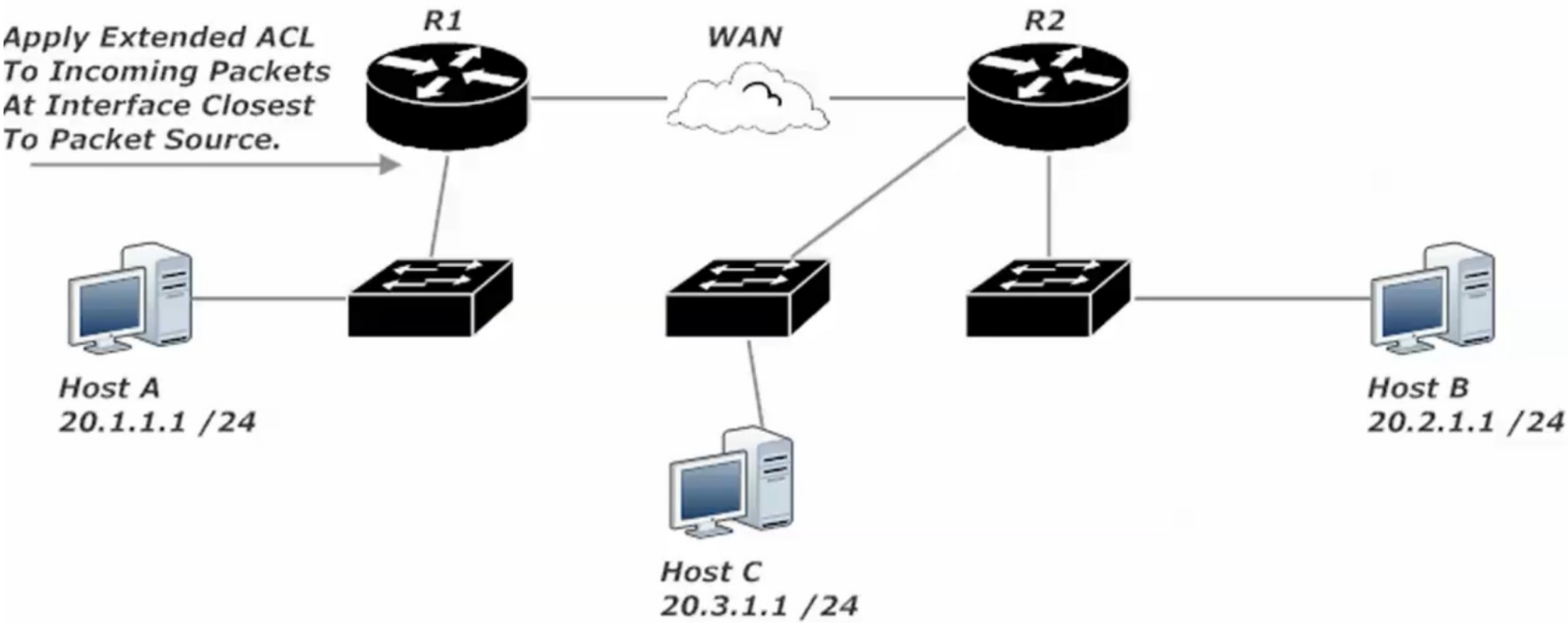
- R5(config)#access-list 17 deny 172.18.18.0 0.0.0.255
- R5(config)#access-list 17 permit any

- R5(config)#access-list 18 permit any
- R5(config)#access-list 18 deny 172.18.18.0 0.0.0.255

- R5(config)#access-list 19 deny 172.18.18.0 255.0.0.0
- R5(config)#access-list permit any

- R5(config)#access-list 20 permit any
- R5(config)#access-list 20 deny 172.18.18.0 255.0.0.0

# ¿Dónde usar cada tipo de ACL?



# ¿Dónde usar cada tipo de ACL?