ACL de IPv4 extendidas

Estructura de una ACL de IPv4 extendida

Los pasos del procedimiento para configurar ACL extendidas **son los mismos que para las ACL estándar**.

Se deben poner lo más **cerca** posible **del origen**.

Hay ACLs extendidas **numeradas** (**100-199, 2000-2699**) y **nombradas**

Con una ACL extendida se puede filtrar por:

- Protocolo(ip, tcp, udp, icmp,…?
- Dirección IP de origen
- Puerto de origen(80, 22, 23, .../www, ssh, telnet…) (Normalmente se omite porque se las aplicaciones escogen un puerto de origen mas o menos aleatorio).
- Dirección IP de de destino
- Puerto de destino (80, 22, 23, .../http, ssh, telnet…)
- **established**(permite que entre tráfico de respuesta a una petición previa)

Antes de los puertos lleva un operador: **eq**(Igual que), **neq**(Distinto), **gt**(Mayor que), **lt**(Menor que)

access-list *numero-acl* {**deny** | **permit** | **remark**} protocolo *IP-fuente* [wilcard] [operador] [número-de-puerto o nombre] *IP-destino* [wilcard] [operador] [número-de-puerto o nombre] [**established**]

Pueden estar presentes las palabras **any** y **host** igual que en las ACLs estándar

Ejemplos:

- access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
- access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
- access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established

Sin el parámetro **established** en esta última instrucción de ACL, los clientes pueden enviar tráfico a un servidor web, pero no recibir el tráfico que vuelve de dicho servidor.

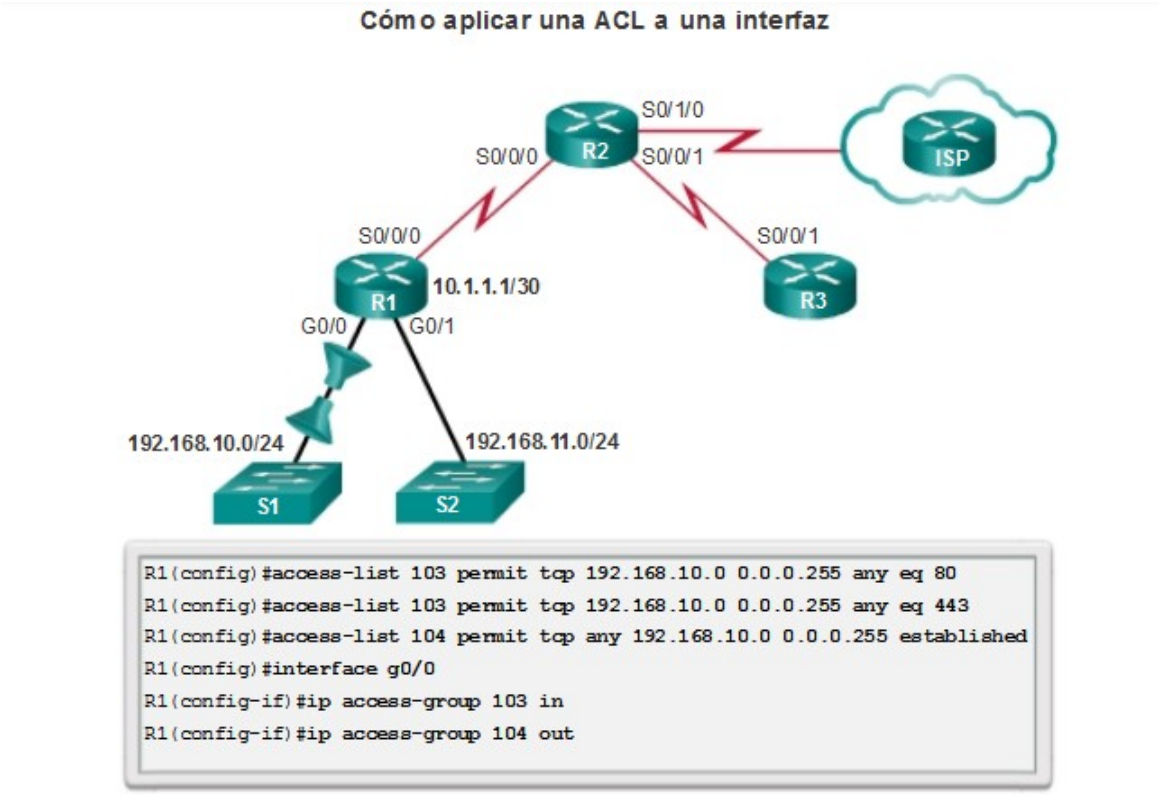
El parámetro **established** permite que solo las respuestas al tráfico procedente de la red 192.168.10.0/24 vuelvan a esa red. Si el segmento TCP que regresa tiene los bits ACK o de restablecimiento (RST) establecidos, que indican que el paquete pertenece a una conexión existente, se produce una coincidencia.

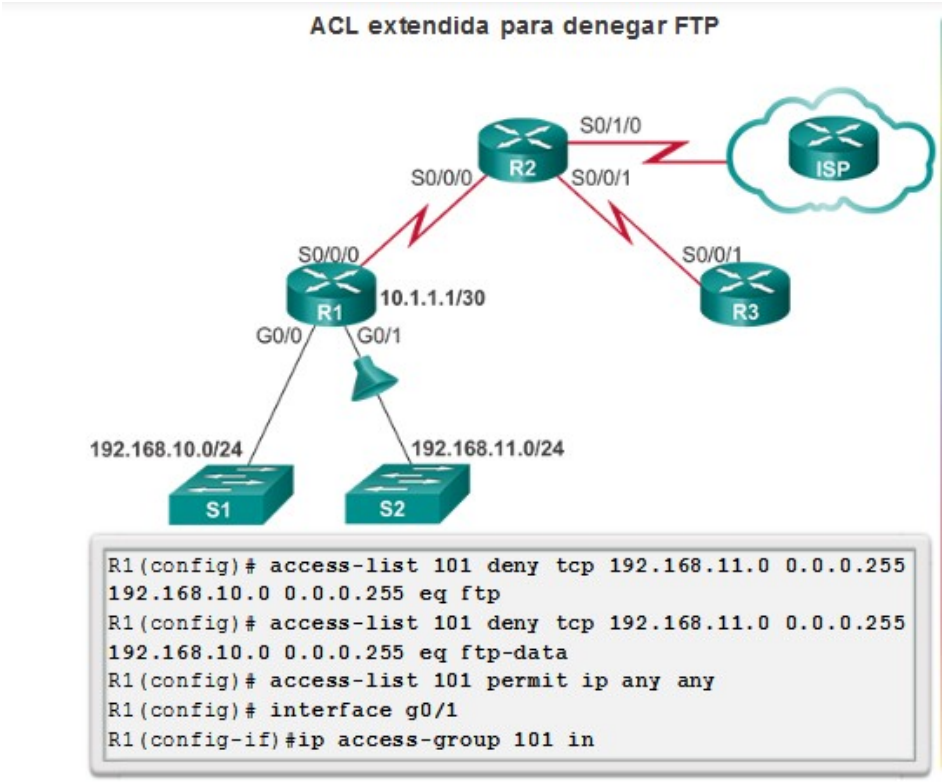
established solo se utiliza para el protocolo **TCP** e indica una conexión establecida.

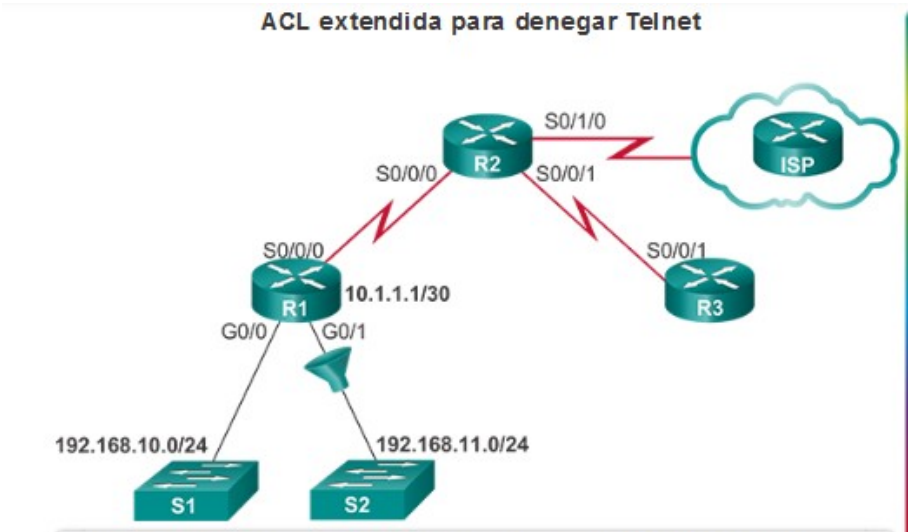
Es decir, solo respuestas a una petición desde dentro de la red.

Nota: la lógica interna aplicada al ordenamiento de las instrucciones de las ACL estándar no se aplica a las ACL extendidas. **El orden en que se introducen las instrucciones durante la configuración es el orden en que se muestran y se procesan**.

Aplicación de ACL extendidas a las interfaces

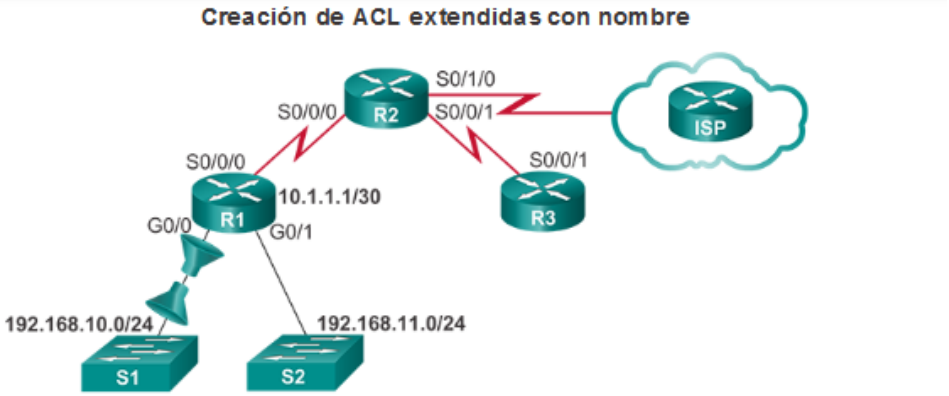







```
R1(config)# access-list 102 deny tcp any 192.168.11.0
0.0.0.255 eq 23
R1(config)# access-list 102 permit ip any any
R1(config)# interface g0/1
R1(config-if)# ip access-group 102 out
```

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
```

Verificación de ACL extendidas

show access-lists

show ip interface g0/0