# SEGURIDAD

ACL, FIREWALL, y DMZ

# Índice

- ACL. Listas de control de acceso.
- Firewall y DMZ

# ACL. LISTAS DE CONTROL DE ACCESO.

# ACL, ¿qué son?

- Anteriormente tratamos escuetamente el concepto de ACL.
- Una ACL es un grupo de reglas configuradas en el router, que definen cómo se procesan los paquetes que:
  - *Entran por las interfaces de entrada del router.*
  - *Se reenvían a través del router.*
  - *Salen por las interfaces de salida del router.*
- Las ACL pueden comprobar la dirección de origen o destino, el protocolo de capa superior utilizado, y el puerto.

# Aspectos a tener en cuenta con ACL

- Se configuran a nivel de interfaz.
  - *Cada interfaz del router puede tener una ACL distinta*.
- Si no hemos configurado ACL, todos los paquetes que pasen por el router tienen acceso a cualquier parte de la red.
- Una ACL no se puede modificar, hay que borrarla y volverla a crear.

# Tipos de ACL

- Existen multitud de tipos de ACL:
  - *Estándar.*
    - Solamente comprueban la dirección de origen del paquete.
    - Pueden ser numeradas o nombradas.
    - El rango válido de números en TCP/IP es 1-99 y 1300-1999.
  - *Extendidas.*
    - Comprueban dirección de origen, dirección de destino del paquete, protocolo, y puertos.
    - Pueden ser numeradas o nombradas.
    - El rango válido de números es 100-199 y 2000-2699.
  - *Dinámicas.*
    - Sirven para exigir la autenticación del usuario en el router vía Telnet.
  - *Reflexivas.*
    - Se utilizan para permitir el tráfico saliente y para limitar el tráfico de regreso de respuesta.
  - *Basadas en tiempo.*
    - Permiten definir un intervalo de tiempo real, válido para el tráfico de paquetes a través del router.
- En esta unidad trataremos las dos primeras, ACL estándar y extendidas, que son las más utilizadas.

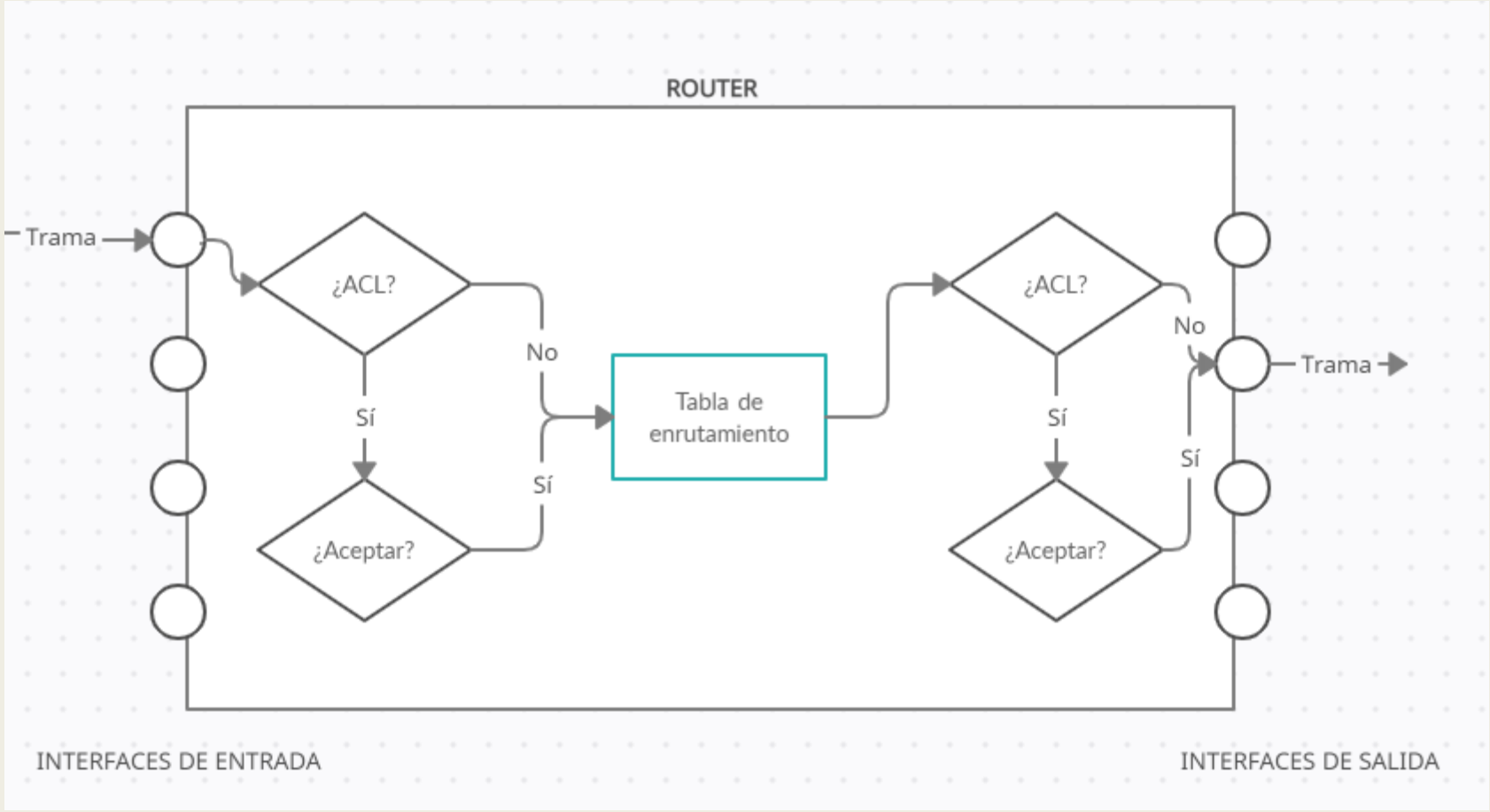
# Funcionamiento general de las ACL 1/2

- El orden en el que se escriben las sentencias de una ACL es fundamental.
- Cuando el router recibe un paquete, verifica si cumple o no cada sentencia en el mismo orden en que fueron creadas.
- Una vez se cumple alguna sentencia, ya no siguen verificando otras sentencias de condición.
- Por ejemplo, si una ACL permite todo el tráfico y está ubicada en la parte superior de la lista, ya no se verifica ninguna sentencia que esté por debajo.
  - `Router (config) # access-list 1 permit any`
- La última sentencia de una ACL siempre es deny any (denegar cualquiera).
  - Esta regla no aparece explícitamente, pero siempre está.
  - De modo que si no se cumple la regla anterior, descartará el paquete.

# Funcionamiento general de las ACL 2/2

- Por cada trama recibida, se realiza un procesamiento similar a lo siguiente:
  1. Si la trama es aceptada, se desencapsula y se comprueba si hay una ACL asociada a la interfaz de entrada.
  2. Si existe la ACL y el paquete es denegado (no cumple condiciones), se descarta.
  3. Si no existe la ACL o el paquete es aceptado, se busca la interfaz de salida en la tabla de enrutamiento.
  4. Se comprueba si la interfaz de salida tiene ACL asociada.
  5. Si existe la ACL y el paquete es denegado, se descarta.
  6. Si no existe la ACL o el paquete es aceptado, se envía por la interfaz de salida.

# Esquema de funcionamiento ACL



# Breve inciso: Máscara Wildcard

- La mencionamos brevemente en la unidad de protocolos de enrutamiento.
- Se trata de una máscara opuesta a la máscara tradicional.
  - *Porque intercambia los unos por los ceros y viceversa.*
- Ejemplo:
  - *192.168.1.1 con máscara normal de 255.255.255.0, su máscara wildcard sería 0.0.0.255*
- Los 0 indican el bit que se compara. Los 1 el bit que se ignora.
- Más ejemplos:
  - *Si queremos especificar la red 192.168.1.0/24, su dirección de red es 192.168.1.0 y su máscara 0.0.0.255.*
  - *Si queremos especificar solamente la dirección 192.168.1.1 se haría mediante la dirección 192.168.1.1 y la máscara 0.0.0.0 (equivalente al /32 o 255.255.255.255, también equivalente a any)*

# ACL Estándar

- Las ACL utilizan un número único no repetido para identificarse.
- En el caso de las estándar:
  - *Se numeran del 1 al 99 y del 1300 al 1999.*

- A continuación vamos a tratar cómo:
  - *Crear una ACL estándar.*
  - *Asignar una ACL a una interfaz.*

# ACL estándar. Creación.

- En el modo configuración global:

```
Router (config) #
access-list <num_ACL>
{permit | deny}
<dirección_origen>
```

- Este comando crea (si no existe) una ACL estándar, que define la regla de permiso/bloqueo de tráfico.
- De momento la ACL NO ESTÁ ASIGNADA a ninguna interfaz.
- Hay 3 formatos posibles para indicar la dirección_origen a la que aplicar la regla:
  - *host <dir_IP>: representa un único host*
  - *<dir_red> <máscara_wildcard>: estos dos valores representan una dirección de red y la máscara en formato wildcard (opuesta).*
  - *any: representa cualquier equipo.*

# Ejemplo de creación ACL estándar

- Ejemplo: Creación de una ACL estándar en el Router, que deniegue el tráfico procedente del host 192.168.1.4 y permita el resto del tráfico:

```
Router (config) # access-list 1 deny host 192.168.1.4
Router (config) # access-list 1 deny 192.168.1.4 0.0.0.0
```

(ambas instrucciones introducidas son equivalentes)

```
Router (config) # access-list 1 permit any
```

# ACL estándar. Asignación a una interfaz.

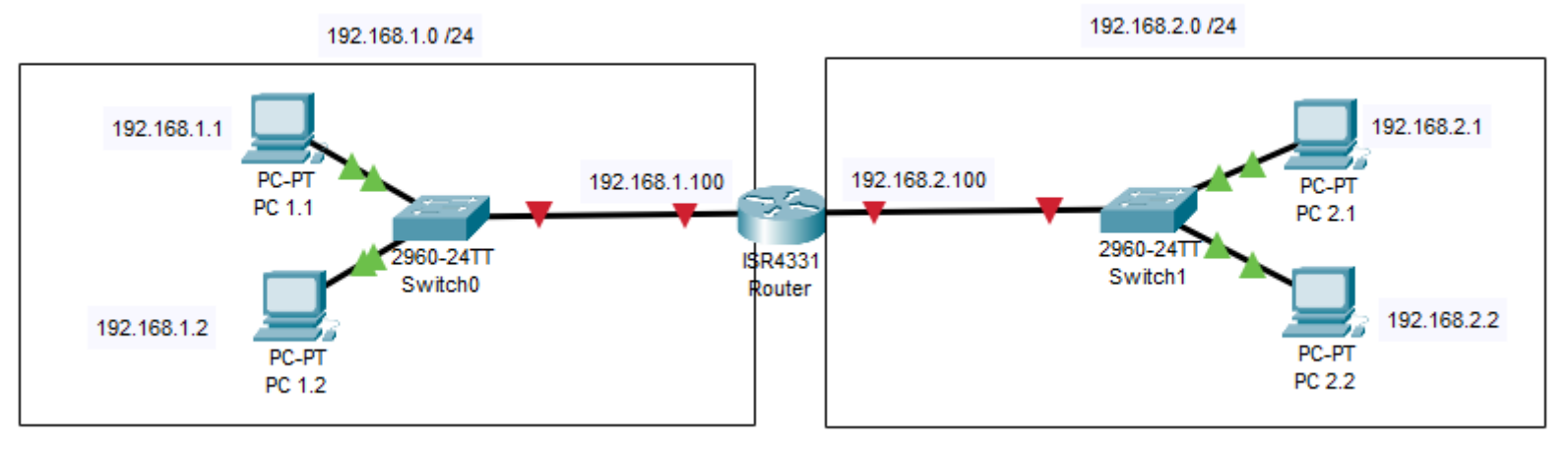
- Una vez creada la ACL se debe asignar a una interfaz.
  - *De lo contrario, la ACL no tendría efecto.*
- Para asignarla, debemos primero acceder a la interfaz que la aplicará, y a continuación, asociarle la ACL:

```
Router (config) # interface <interfaz>
Router (config-if) # ip access-group <número_ACL> {in | out}
```

- El último parámetro indica el tráfico al que se aplica:
  - *in = tráfico a filtrar que entra por la interfaz seleccionada.*
  - *out = tráfico a filtrar que sale por la interfaz seleccionada.*
- Dado que las ACL estándar solo tienen en cuenta la dirección origen del tráfico, se recomienda que se establezcan lo más cerca posible del destino.

# Ejemplo: Creación + Asignación

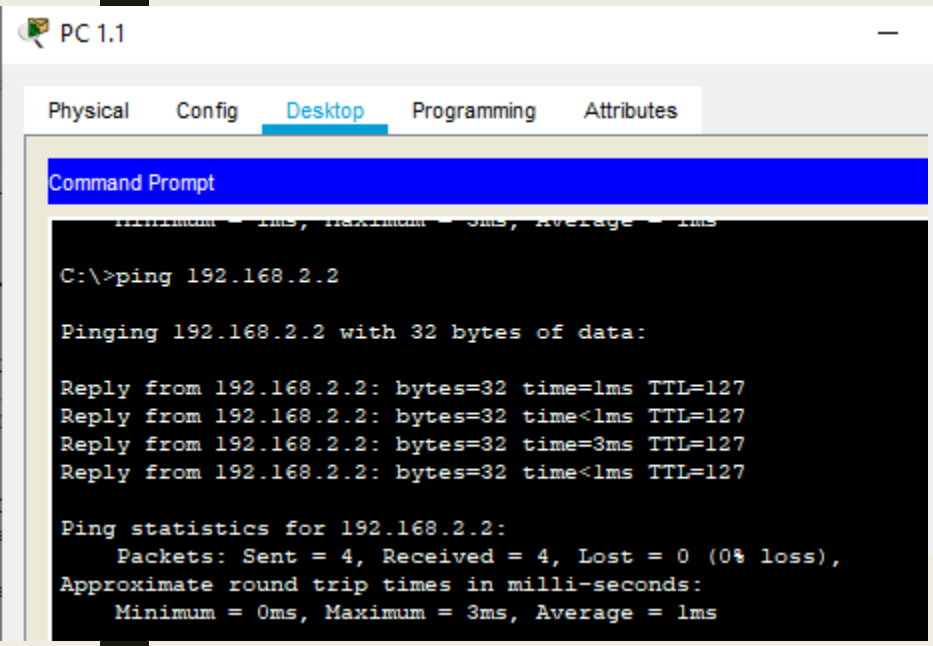
- Dada la siguiente red, se quiere definir una ACL estándar que impida el tráfico procedente del equipo PC 1.2 y permita el resto de tráfico de salida desde la red 192.168.1.0 /24.

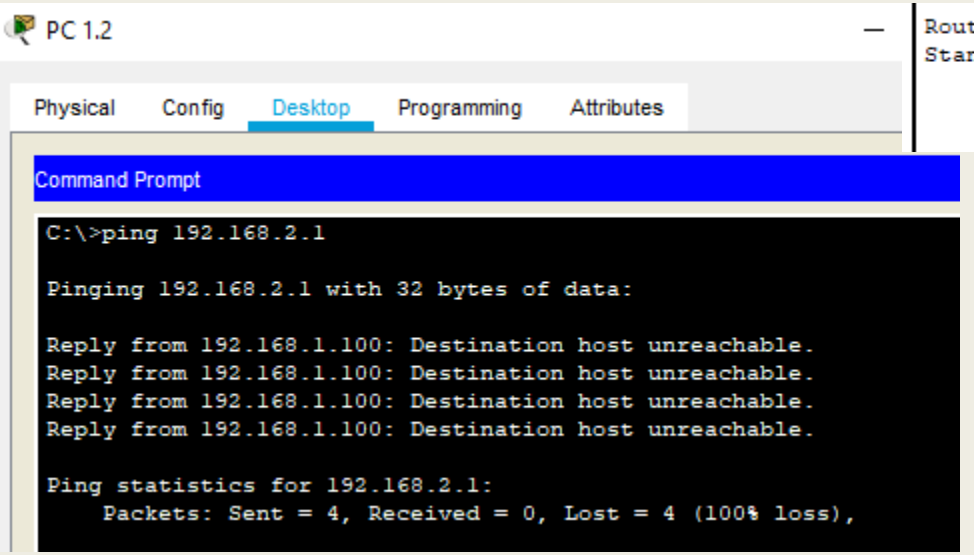


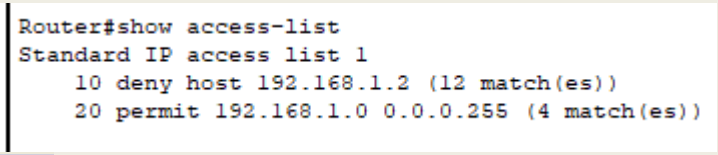

```
Router (config) # access-list 1 deny 192.168.1.2 0.0.0.0
Router (config) # access-list 1 permit 192.168.1.0 0.0.0.255
Router (config) # interface Gig0/1
Router (config-if) # ip access-group 1 in
```

# Comprobar que el ejemplo funciona

- Si hacemos un ping desde el PC 1.1 tenemos tráfico.
- Si hacemos un ping desde el PC 1.2 no puede alcanzar el destino.
- Con el comando show access-list podemos ver paquetes aceptados y rechazados.



# Eliminar una ACL y liberar una interfaz de una ACL

- Para eliminar una ACL que hayamos creado, podemos utilizar el siguiente comando:
  - **`Router0 (config) # no access-list <1-99>`**

- Si no queremos eliminar la ACL, y solo queremos liberar una interfaz de esa ACL, usaremos el siguiente comando:
  - **`Router (config) # interface <interfaz>`**
  - **`Router (config-if) # no ip access-group <número_ACL> {in | out}`**

# ACL extendida

- Las ACL utilizan un número único no repetido para identificarse.
- En el caso de las estándar:
  - *Se numeran del 100 al 199 y del 2000 al 2699.*
- Solo se puede especificar una ACL por protocolo y por interfaz.
- Nada más crear la ACL no está asignada a ninguna interfaz.

- A continuación vamos a tratar cómo:
  - *Crear una ACL extendida.*
  - *Ejemplo*

# ACL extendida. Creación.

- Este comando crea (si no existe) una ACL extendida:

```
Router (config)# access-list <num_ACL>
[dynamic <nombre>]
{permit | deny}
<protocolo>
<dirección_origen> [<operador> <puerto>]
<dirección_destino> [<operador> <puerto>]
[tipo_icmp]
[established]
[precedence <p>]
[tos <t>]
[time-range <tiempo>]
[remark <comentario>]
```

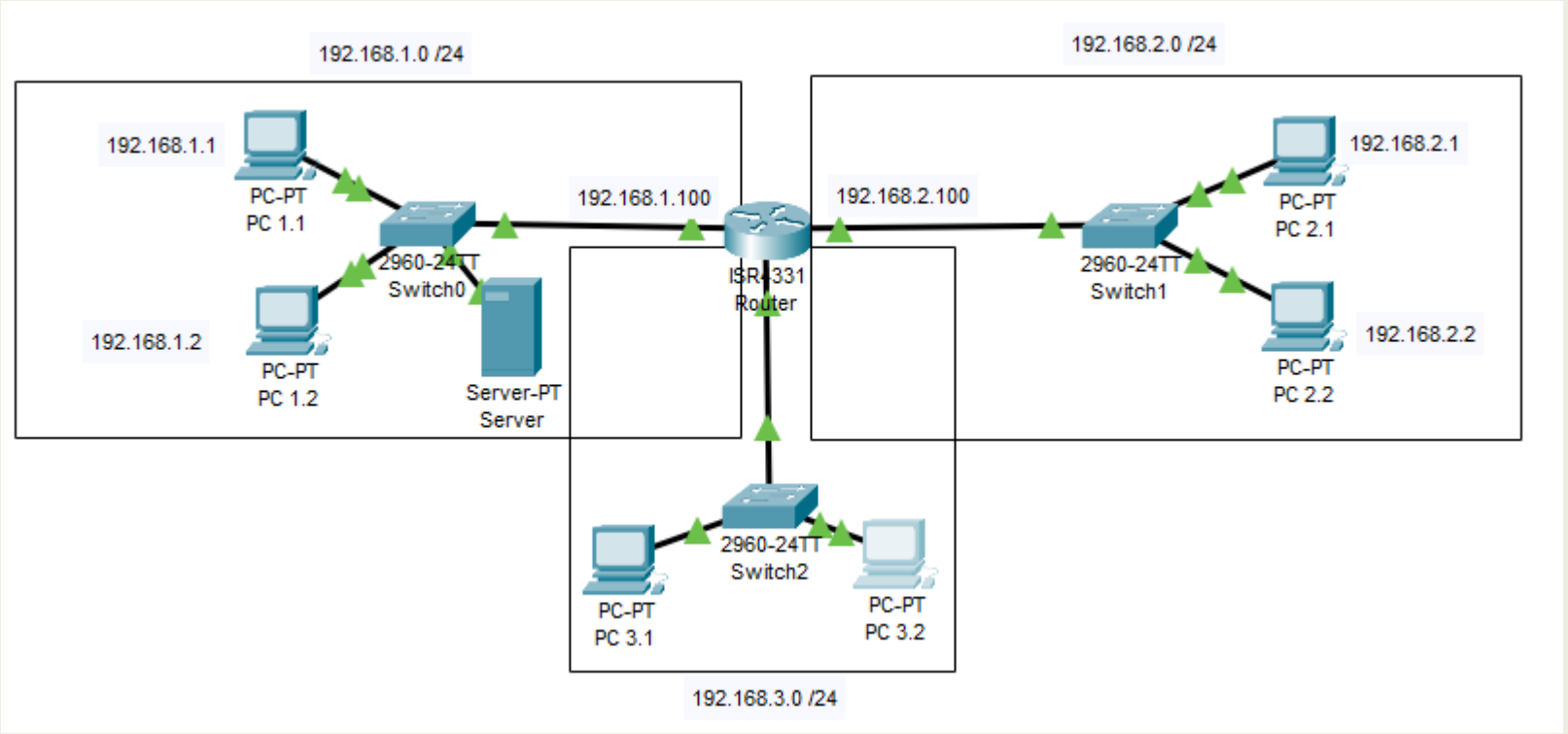
| Valores para Operador puerto | Se aplica a paquetes… |
|---|---|
| eq <puerto> | con número de puerto igual que indicado |
| gt <puerto> | con número de puerto mayor que indicado |
| lt <puerto> | con número de puerto menor que indicado |
| neq <puerto> | con número de puerto distinto que indicado |
| range <puerto1> <puerto2> | con rango de puertos indicado |

- num_ACL: número de ACL en su rango
- dynamic: permite asignar nombre a la ACL
- protocolos: eigrp, gre, icmp, ip, ospf, tcp, udp
- dirección_origen y destino: igual que ACL estándar
- operador puerto: solo con tcp y udp
- tipo_icmp: Si icmp- echo, reply, host-unreachable…
- established: permite tráfico TCP en conexiones establecidas
- precedence: filtrar tráfico por nivel de precedencia
- tos: filtrar tráfico en función del tipo de servicio
- time_range: establecer intervalo de tiempo que está activa la ACL
- remark: sirve para añadir comentarios a la ACL

# Ejemplo 1: Creación + Asignación

- Dada la siguiente red, se quiere definir una ACL extendida que impida el tráfico HTTP desde la red 192.168.2.0 /24 a la red 192.168.1.0 y permita el resto del tráfico.

- Por regla general, colocar la ACL extendida lo más cerca posible del origen del tráfico denegado.
  - *En este caso es de nuevo la interfaz Gig0/1*

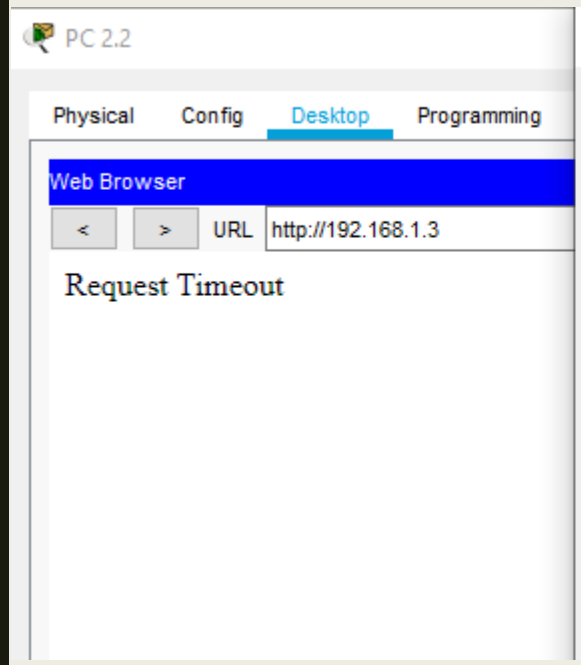


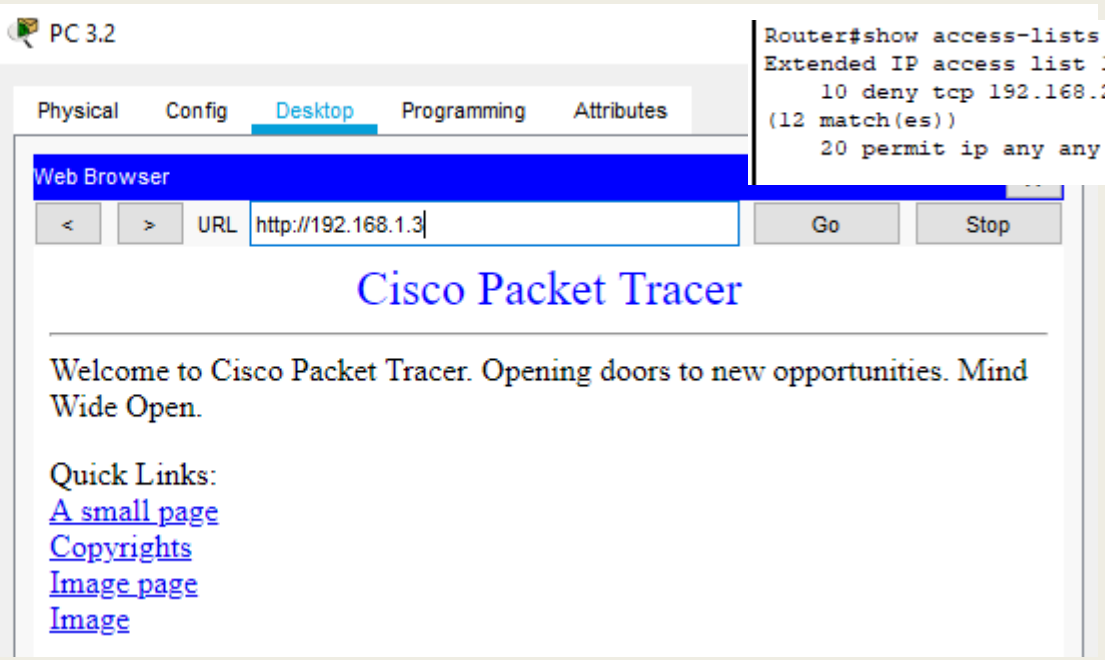
# Parámetros de red

```
Router (config) # access-list 101 deny tcp 192.168.2.0
0.0.0.255 192.168.1.0 0.0.0.255 eq 80

Router (config) # access-list 101 permit ip any any

Router (config) # interface Gig0/1

Router (config-if) # ip access-group 101 in
```

# Comprobar que el ejemplo funciona

- Si abrimos la web en 192.168.1.3 desde el PC 2.2 no tenemos tráfico.
- Si abrimos la web en 192.168.1.3 desde el PC 3.2 tenemos tráfico.
- Con el comando show access-list podemos ver paquetes aceptados y rechazados.



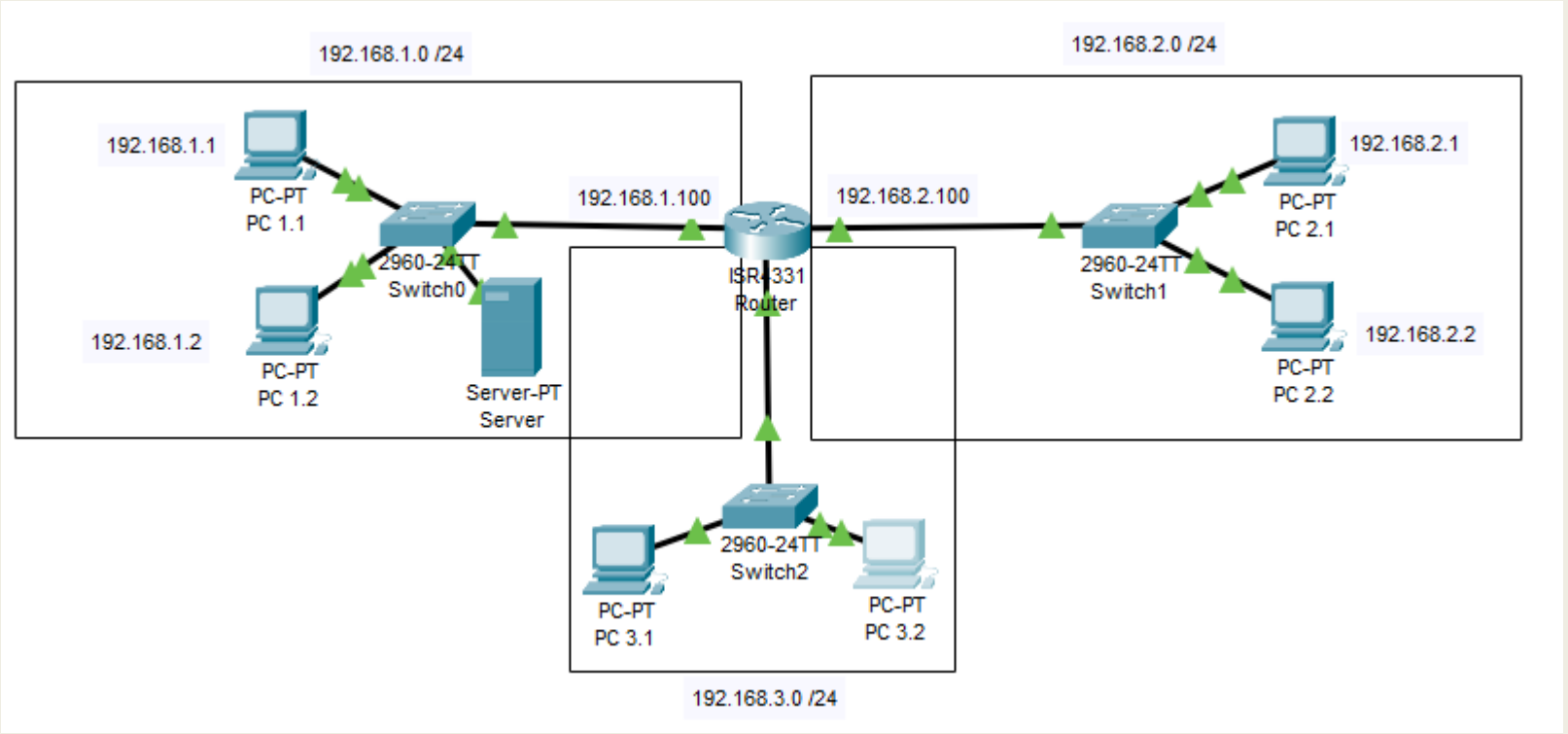

```
Router#show access-lists
Extended IP access list 101
    10 deny tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 eq www
(12 match(es))
    20 permit ip any any (4 match(es))
```

# Ejemplo 2: Creación + Asignación

- Partiendo de la red del ejemplo 1. Crear una ACL que impida el tráfico de ping hacia la red 192.168.1.0 (hay que impedir el tráfico ICMP desde las redes 192.168.2.0 y 192.168.3.0 hacia la red 192.168.1.0).

Tenemos dos opciones:

- Crear una ACL extendida de entrada y asignarla a las interfaces Gig0/1 y Gig0/2 (menos procesamiento).
- Crear una ACL extendida de salida y asignarla a la interfaz Gig0/0 (más procesamiento porque se consulta la tabla de rutas)



# Parámetros de red

- Solución 1:

```
Router (config) # access-list 102 deny any icmp 192.168.1.0 0.0.0.255
Router (config) # access-list 102 permit ip any any
Router (config) # interface Gig0/1
Router (config-if) # ip access-group 102 in
Router (config-if) # exit
Router (config) # interface Gig0/1
Router (config-if) # ip access-group 102 in
```

- Solución 2:

```
Router (config) # access-list 102 deny icmp any 192.168.1.0 0.0.0.255
Router (config) # access-list 102 permit ip any any
Router (config) # interface Gig0/0
Router (config-if) # ip access-group 102 out
```

# Comprobar que el ejemplo funciona

- Si hacemos un ping desde el PC 2.2 a PC 1.1 no tenemos tráfico.
- Si hacemos un ping desde el PC 2.2 a PC 3.1 sí tenemos tráfico.
- Con el comando show access-list podemos ver paquetes aceptados y rechazados.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.2.100: Destination host unreachable.
Reply from 192.168.2.100: Destination host unreachable.
Reply from 192.168.2.100: Destination host unreachable.
Reply from 192.168.2.100: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.1: bytes=32 time=1ms TTL=127
Reply from 192.168.3.1: bytes=32 time<1ms TTL=127
Reply from 192.168.3.1: bytes=32 time<1ms TTL=127
```

```
Router#show access-lists
Extended IP access list 101
    10 deny tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 eq www
(12 match(es))
    20 permit ip any any (4 match(es))
Extended IP access list 102
    10 deny icmp any 192.168.1.0 0.0.0.255 (4 match(es))
    20 permit ip any any (7 match(es))
```

# FIREWALL Y DMZ

# ¿Qué es un firewall?

- Un firewall o cortafuegos es un componente de red, hardware o software, cuya finalidad es filtrar tráfico por diferentes aspectos:
  - *direcciones de origen y/o destino*
  - *puertos de origen y/o destino*
  - *protocolos de origen y/o destino*
- En general, el firewall se define como un mecanismo de seguridad tanto para accesos como para envíos.
- Está basado en el filtrado de paquetes.

# Dispositivos cortafuegos

- Existen dispositivos físicos dedicados y programas informáticos que realizan una función de cortafuegos.
- Algunos routers, mediante las ACL, también realizan la misma función.
- Hay cortafuegos que operan en diferentes niveles del modelo OSI.
  - *Los cortafuegos que operan en niveles bajos:*
    - Fácilmente configurables.
    - Pero poco flexibles.
  - *Los cortafuegos que operan en niveles superiores pueden investigar el contenido de cada paquete:*
    - Son más lentos
    - Pero muy flexibles.

# Capacidades de los cortafuegos actuales

- **Traducción de direcciones (NAT).**
  - *Consiste en que las direcciones IP utilizadas por los equipos solo tienen validez dentro de la propia LAN.*
  - *El cortafuegos puede sustituir la dirección IP de la Intranet por otras direcciones IP virtuales, protegiendo de este modo contra accesos indeseados.*
- **Protección frente a virus.**
  - *Al analizar los paquetes, pueden detectar anomalías en datos y programas.*
- **Auditoría.**
  - *Puede auditar recursos concretos de la Intranet y avisar a través de un sistema de mensajría electrónica del intento de violación de algún recurso o acceso indebido.*
- **Gestión de actividad.**
  - *A través de agentes SNMP, propios de la gestión de red, se puede monitorizar el cortafuegos con el fin de realizar informes sobre la actividad de la red.*

# Firewalls comunes de tipo software

Entre los firewalls de tipo software, podemos encontrar dos tipos principales:

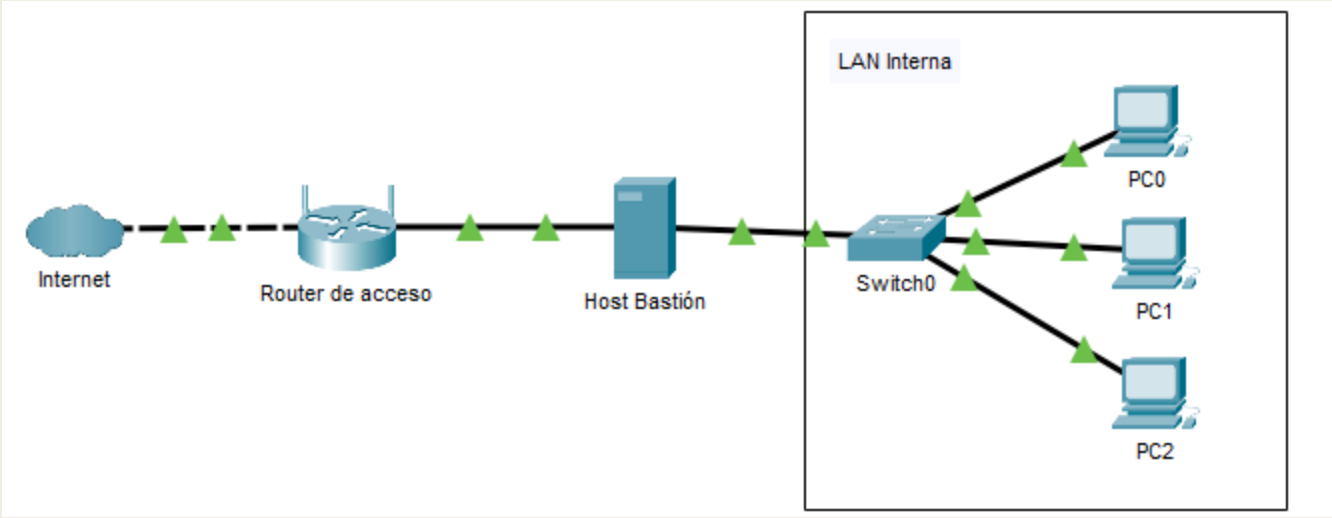
- **Firewall personal**
  - *Para uso doméstico.*
  - *Se instala en cada equipo.*
  - *Ejemplo: Zone Alarm.*
- **Firewall específico**
  - *Para uso en empresa.*
  - *Se instala en los equipos que realizarán el filtrado para ofrecer seguridad a la red.*
  - *Ejemplo: iptables, wipfw*

# Arquitectura de firewalls

- Existen diversas arquitecturas de firewalls.
- Vamos a tratar dos de las principales:
  - *Host Dual-Homed*
  - *Arquitectura Screened Host*
  - *Arquitectura Screened Subnet*

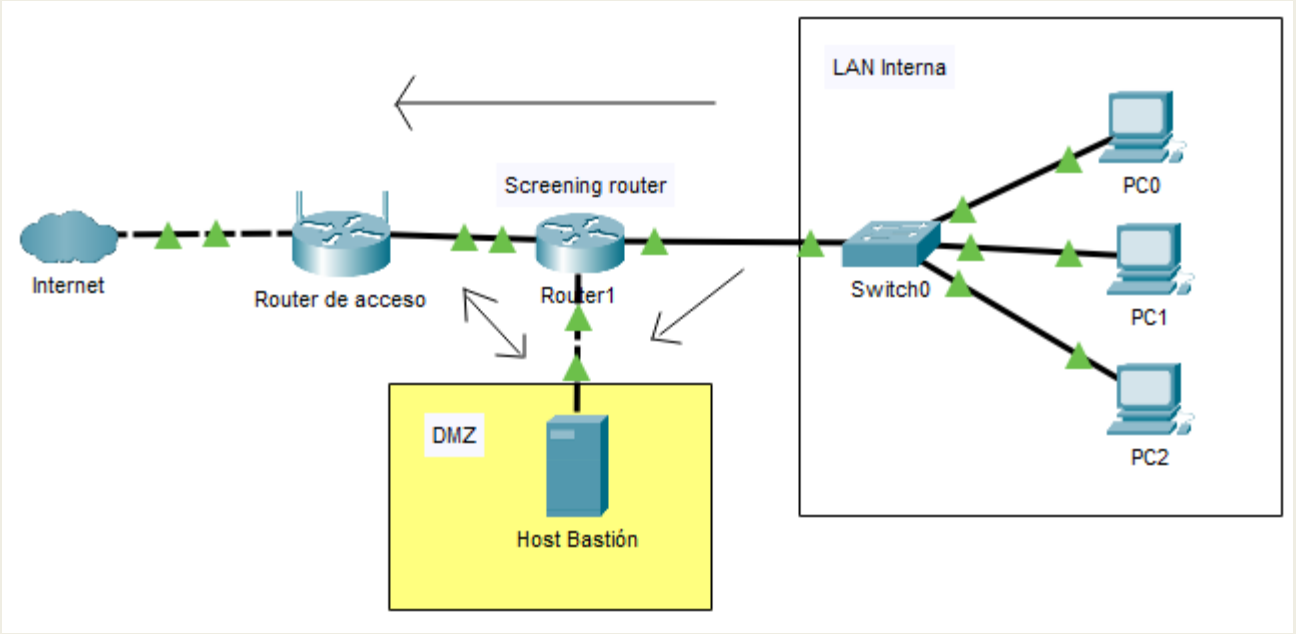
# Host Dual-Homed

- Está construida con un equipo con dos interfaces de red y software específico de filtrado.
- Este equipo suele denominarse Bastión, y actúa como router entre las dos redes que conoce.
- Los paquetes IP de una red a la otra no son enrutados directamente. La red interna puede comunicarse con el dual-homed host, y la red externa también puede comunicarse con él, pero las redes no se comunican directamente.



# Arquitectura Screened Host (Firewall de 3 patas)

- Esta arquitectura combina un screening router con un host bastión.
  - *Screening router es un router configurado para permitir o denegar tráfico en base a un conjunto de reglas.*




- El principal nivel de seguridad proviene del filtrado de paquetes mediante ACL.
- Las ACL son definidas por el administrador de la red, según aquellas direcciones y servicios que van a ser analizados.
- El filtrado de paquetes del screening router está configurado de modo que el host bastión es el único sistema de la red interna accesible desde la red externa.

# DMZ (Zona Desmilitarizada)

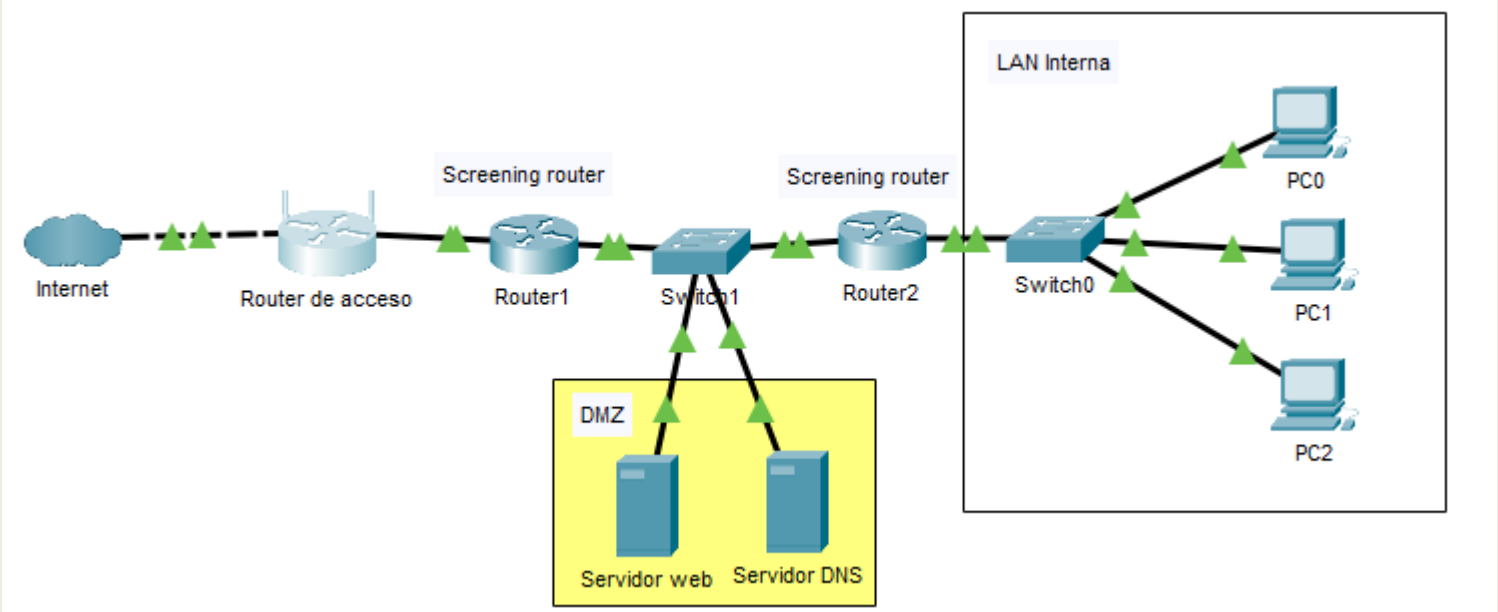
- Una zona desmilitarizada (DMZ) o red perimetral, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente internet.
- En una DMZ:
  - *Las conexiones desde la red interna a la DMZ están permitidas.*
  - *Las conexiones desde la red externa a la DMZ están permitidas.*
  - *Las conexiones desde la DMZ solo se permiten a la red externa.*
    - Los equipos en la DMZ no pueden conectar con la red interna.
- Esto permite que los equipos de la DMZ puedan dar servicios a la red externa, a la vez que protegen la red interna, en el caso de que intrusos comprometan la seguridad de los equipos de la zona desmilitarizada.

# Arquitectura Screened Subnet 1/2

- Es la arquitectura más segura.
- Aumenta un nivel más el nivel de seguridad de screened host.
- Añade un perímetro a la red que aísla fuertemente la red interna de Internet.
- Los hosts bastión son las máquinas más vulnerables en la red.
  - *Porque son visibles desde la red externa.*
- Para reducir la vulnerabilidad del host bastión:
  - *Se recurre a aislar el host bastión en un perímetro o red intermedia.*
- Esta arquitectura tiene dos “screening router” cada uno conectado al perímetro:
  - *Uno conectado al perímetro de la red interna y otro al de la red externa.*
  - *Un atacante deberá pasar por ambos para llegar a la red interna.*

# Arquitectura Screened Subnet 2/2

- Si alguien quiere atacar la red interna, debe pasar por los dos Screening Router.
- **Perímetro**. Red adicional entre la red externa y la LAN interna.
  - *Nivel adicional de protección entre la red interna y el atacante.*




- **Router exterior**. Situado entre el mundo externo y el perímetro. Filtra paquetes.
  - *Las reglas de filtrado protegen las máquinas del perímetro (bastión y router interno)*
- **Router interior.** Ubicado entre la red interna y el perímetro.
  - *No hace filtrado principal de paquetes, sino que permite seleccionar qué servicios usar en la red interna.*
  - *Los servicios que el router permite entre la DMZ y la LAN interna no son los mismos que permite al router externo.*

# ¿Preguntas?

# SEGURIDAD

ACL, FIREWALL, y DMZ