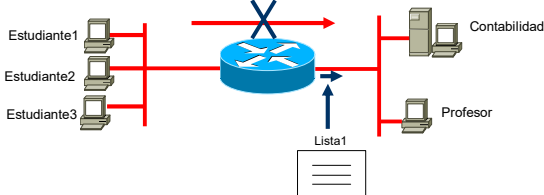


Agenda

1. ¿Por qué utilizar listas de acceso?
2. ¿Qué es una lista de acceso?
3. Tipos de listas de acceso
4. Listas de acceso Estándar
5. Ejemplos
6. Ejercicio práctico

2

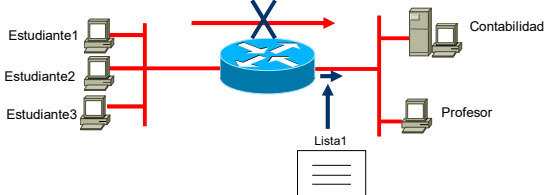


¿Por qué utilizar Listas de Acceso?

Cuando no se han configurado listas de acceso el tráfico puede pasar a través de los enrutadores sin ningún problema.

Con listas de acceso puedo **filtrar/bloquear** el tráfico que **pasa a través** de los enrutadores, y empezar a colocar restricciones de seguridad en mi red.

3



¿Qué es una lista de acceso?

- Conjunto de **instrucciones/sentencias “permit” o “deny”** que analizan el tráfico de equipos, protocolos, redes, subredes y/o aplicaciones en una red.
- Cada lista de acceso debe estar relacionada con una **interfaz física o virtual** y debe tener un **sentido de aplicación (in/out)**.

4

Aplicaciones de las listas de acceso

1. Filtrar tráfico que pasa **a través** de un enrutador

Por ejemplo: Qué solo los equipos de los estudiantes tengan acceso al correo y no puedan consultar el servidor de contabilidad.

5

Aplicaciones de las listas de acceso

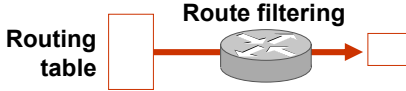
2. Definir el tráfico que se le va a dar prioridad en un esquema de encolamiento (QoS).

Priority and custom queuing

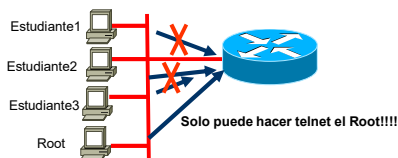
6

Aplicaciones de las listas de acceso

3. Filtrar la información de enrutamiento que propague un enrutador.



4. Limitar el acceso vía **telnet** a mis dispositivos de interconectividad (switches y enrutadores).

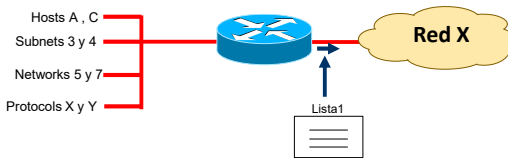


7

Secuencialidad en una lista de acceso

•Existe una red con los siguientes elementos:

Hosts A, C	Subnets: 3 y 4
Networks 5 y 7	Protocolos X y Y

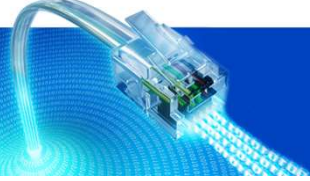


Se crea una lista de acceso:

Lista 1:
 Deny Host A
 Permit subnet 3
 Permit network 5
 Deny protocol X

- ¿ Qué pasa con el tráfico que generan host C,subnet 4 network 7 y protocol Y ?
- ¿Dicho tráfico pasará por el enrutador?
- ¿Será esto seguro?

8



Deny implícito

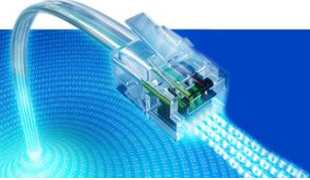
- Ante el inconveniente de “seguridad” del slide anterior, Cisco optó por colocar al final de cada lista de acceso un **deny all**.

```

Lista 1
Deny Hosts A
Permit subnet 3
Permit network 5
Deny protocol X
Deny all
  
```

El **deny all** siempre esta de manera tácita al final de cada lista de acceso.

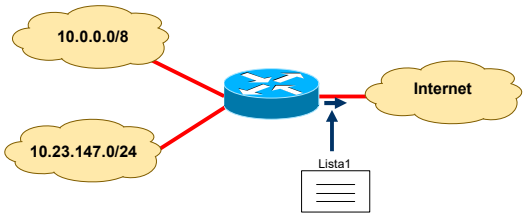
9



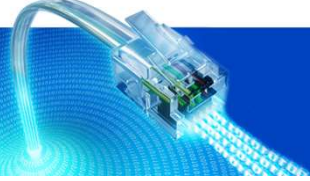
Secuencialidad en una lista de acceso

Las listas de acceso siempre se ejecutan de manera secuencial, desde la primera sentencia hasta la última. (top – down).

Ejemplo: Se desea crear una lista de acceso que no permita el tráfico de la subred 10.23.147.0/24 a Internet, pero que a su vez si permita el tráfico de la red 10.0.0./8 a Internet.



10



Secuencialidad

Ejemplo: Se desea crear una lista de acceso que no permita el tráfico de la subred **10.23.147.0/24** a Internet, pero que a su vez si permita el tráfico de la red **10.0.0.0/8** a Internet.

Caso A
Lista1

```

permit network 10.0.0.0/8
deny subnet 10.23.147.0/24
deny all!!

```

Caso B
Lista1

```

deny subnet 10.23.147.0/24
deny all!!

```

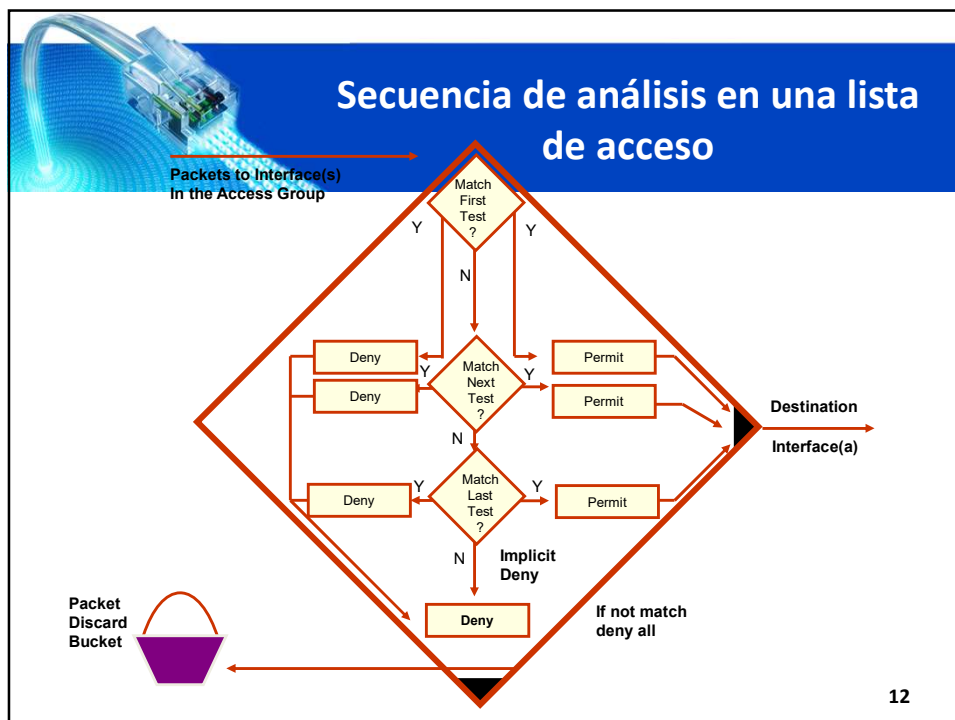
Caso C
Lista1

```

deny subnet 10.23.147.0/24
permit network 10.0.0.0/8
deny all!!

```

11





Tipos de Listas de Acceso

Existen principalmente dos tipos de listas de acceso:

Listas de Acceso Estándar

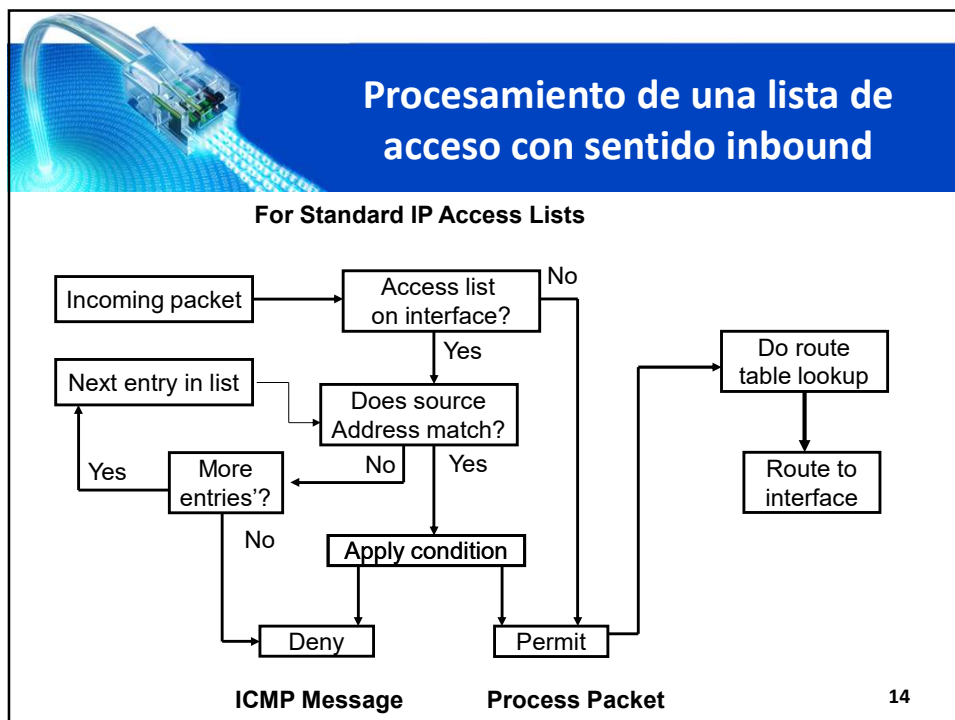
- Analizan la **dirección IP fuente únicamente**.
- Generalmente permiten o filtran **todo** un protocolo.

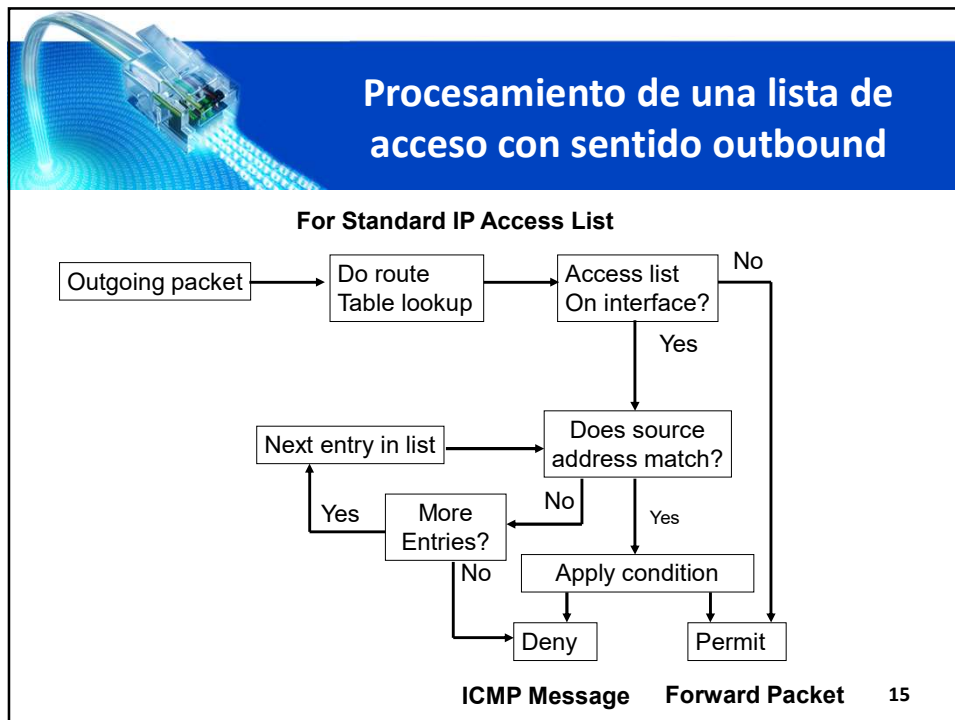
Listas de Acceso Extendidas

- Analizan **dirección IP fuente y destino**.
- Permiten o filtran protocolos y aplicaciones (puertos).

Adicionalmente las listas de acceso se deben aplicar sobre una interfaz física en **un sentido**, ya sea **Inbound (entrada)** u **Outbound (salida)**.

13

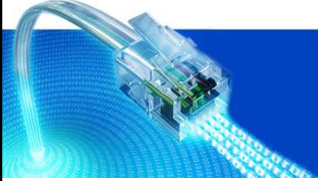




Guía de configuración

1. Mediante el número de la lista de acceso defino si es estándar o extendida.
2. Se debe configurar una lista por interfaz, protocolo y dirección.
3. El orden de las sentencias es crucial para el análisis de lo que se desea.
4. Las sentencias más restrictivas deben ubicarse al inicio de la lista.
5. Siempre al final de cada lista hay un “deny all” implícito, por lo tanto debe configurarse un “permit” de tal manera que no se filtre todo el tráfico.
6. Cree las listas de acceso antes de aplicarlas a las interfaces.
7. Las listas de acceso filtran **el tráfico que pasa a través** del enrutador, y no se aplican al tráfico originado desde el enrutador (caso especial).

16



Comandos de Configuración

1. Crear la lista de acceso según los requerimientos en modo de configuración global.
Router(config)#
access-list *access-list-number* { **permit** / **deny** } { **test conditions** }
2. Aplicar la lista de acceso a la interfaz requerida, teniendo en cuenta la dirección del tráfico a analizar.
Router(config-if)#
{ **protocol** } **access-group** *access-list-number* { **in** / **out** }

17

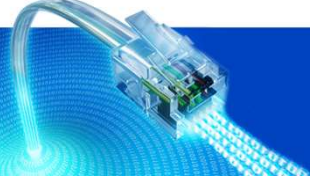


Como identificar el tipo de lista de acceso

Listas de acceso estándar rango:
1-99 , 1300-1999

Listas de acceso extendidas rango:
100-199, 2000-2699

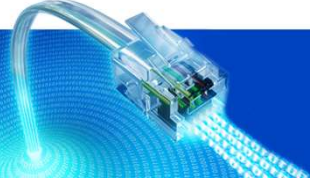
18



Componentes de una Lista de Acceso

- **Fuente:** La dirección IP del origen del tráfico.
- **Destino:** La dirección IP del destino del tráfico.
- **Protocolo:** El tipo de protocolo (TCP, UDP, ICMP, etc.).
- **Puerto:** El puerto o rango de puertos involucrados (solo para TCP/UDP).
- **Acción:** La acción a tomar (permitir o denegar).
- **Sentido:** inbound or outbound

19



Máscara invertida en las listas de acceso

Para analizar la **dirección IP de un host** la máscara invertida debe chequear todos los bits, así:

Dir_IP: 192.168.10.10

Wildcard mask: 0 . 0 . 0 . 0
(Analiza todos los bits)

Por lo tanto : 192 . 168 . 10 . 10 0 . 0 . 0 . 0 analiza toda la dirección.

Para abreviar la configuración se puede utilizar la palabra **host** antes de la dirección IP así:

host 192.168.10.10

20



Máscara invertida en las listas de acceso

Cuando se desea permitir o denegar a **cualquier host** se debe colocar una máscara invertida que ignore todos los bits:

Cualquier Dir_IP:	0 . 0 . 0 . 0
Wildcard mask:	255.255.255.255 (Ignora todos los bits)

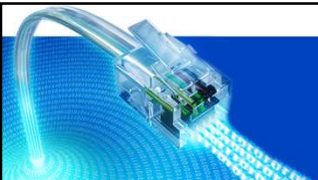
Por lo tanto para analizar cualquier dirección se debe colocar lo siguiente : 0 . 0 . 0 . 0 255 . 255 . 255 . 255

Para abreviar se utiliza la palabra **any**.

Ejemplo:

```
access-list 1 permit 0.0.0.0 255.255.255.255 por
access-list 1 permit any
```

21



Configuración de listas de acceso estándar

1. Crear la lista de acceso:

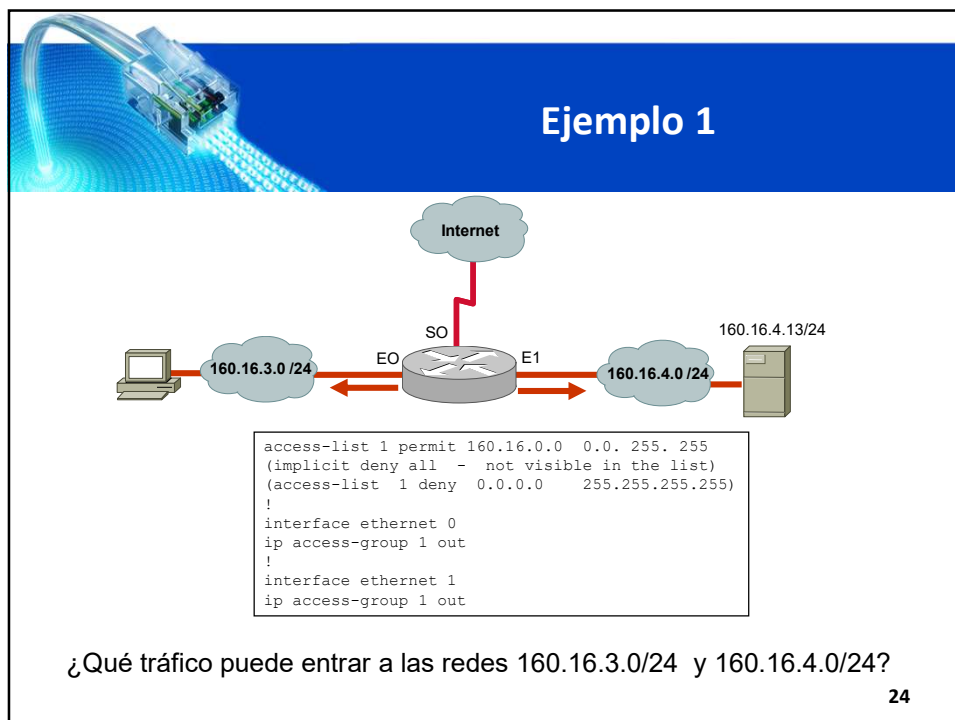
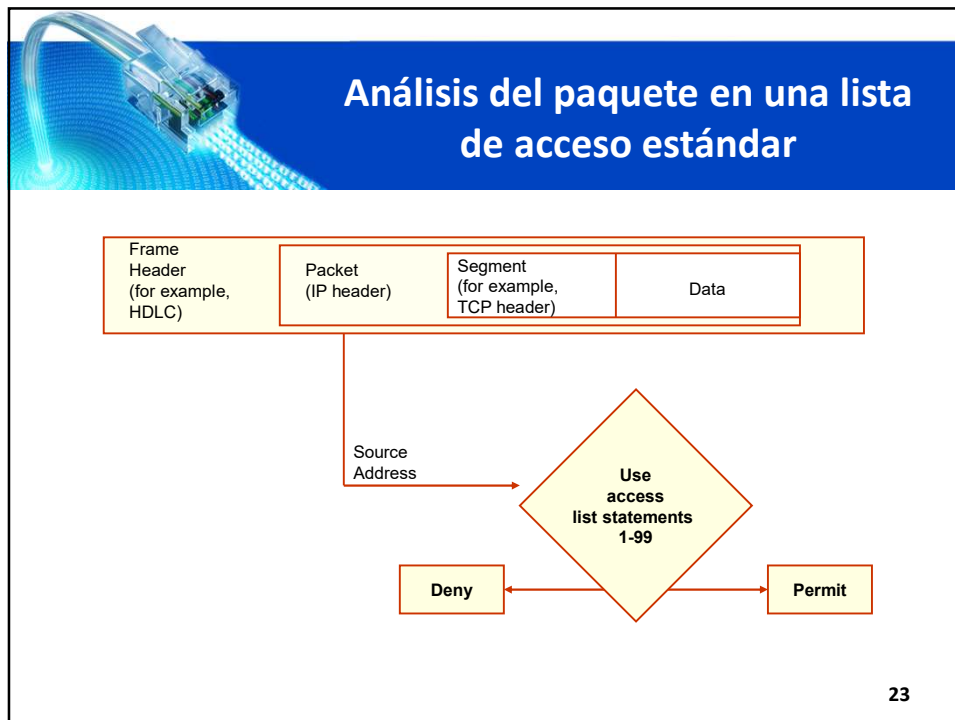

```
Router(config)#
access-list access-list-number { permit /deny } dir_ip_source wildcard_mask
```

 - Las listas de acceso estándar usan como access-list-number el rango 1 a 99.
 - La wildcard mask por defecto es : 0.0.0.0
 - El comando `no access-list access-list-number` borra toda la lista de acceso.
2. Aplicar la lista de acceso a la interfaz requerida, teniendo en cuenta la dirección del tráfico a analizar:

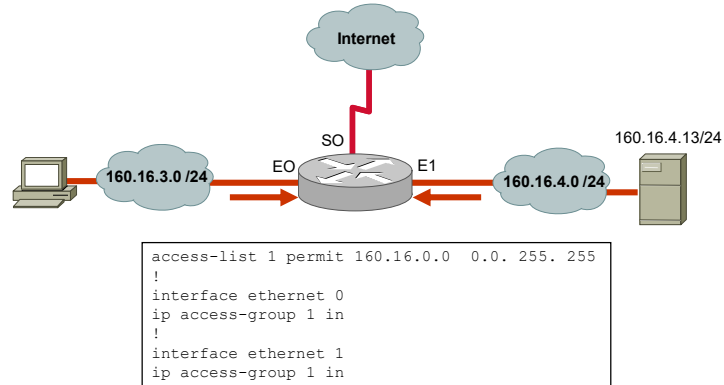

```
Router(config-if)#
ip access-group access-list-number { in / out }
```

 - Este comando activa la lista de acceso en la interfaz.
 - La dirección por defecto es: outbound (out).
 - El comando `no ip access-group access-list-number` remueve la lista de acceso de la interfaz.

22



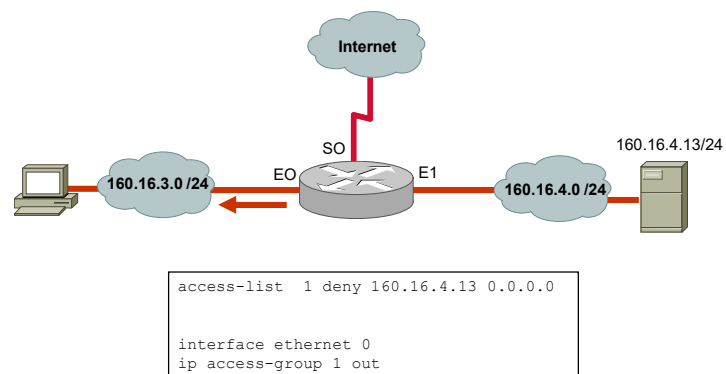
Ejemplo 2



¿Qué pasa la cambiar el sentido de la lista de acceso a "in en ambas interfaces?

25

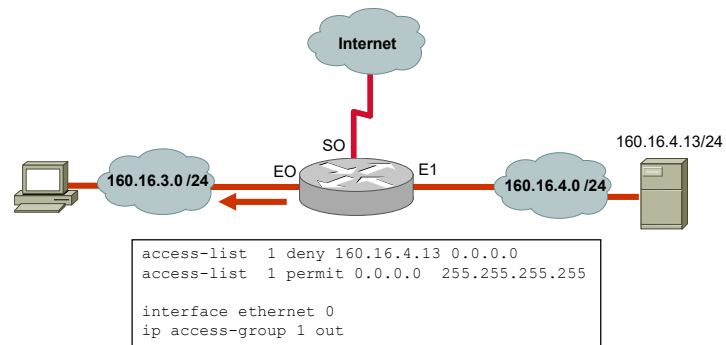
Ejemplo 3



¿Qué tráfico esta permitido en esta configuración?

26

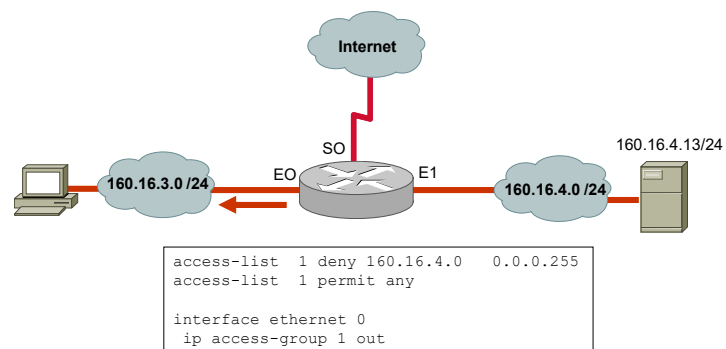
Ejemplo 4



¿Que tráfico esta permitido en esta configuración ahora que se agregó otra sentencia a la lista de acceso?

27

Ejemplo 5



¿Qué tráfico esta permitido en esta configuración?

28

Ejemplo 6

```

Router (config) # access-list 2 permit 10.48.0.3
Router (config) # access-list 2 deny 10.48.0.0 0.0.255.255
Router (config) # access-list 2 permit 10.0.0.0 0.0.255.255
Router (config) # ! (Note: all other access implicitly denied)
Router (config) # interface ethernet 0
Router (config-if) # ip access-group 2 in
  
```

¿Qué equipo(s) se pueden conectar con A?

29

Ejemplo 7: Ubicación de las listas de acceso

- ¿En qué enrutador se debe configurar la lista de acceso para denegar el acceso del host Z a la red 10.20.0.0?
- ¿Qué se debe analizar para lograr la ubicación ideal de la lista de acceso?

30



Filtrando el acceso vía telnet hacia los enrutadores



console E0

↑ ↑

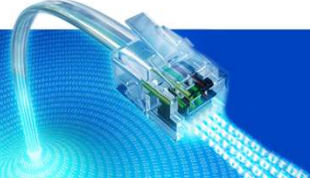
Puerto de Consola Puerto Físico

Conexión directa

Puertos Virtuales 0 a 4 (vty's)

- El enrutador soporta 5 conexiones simultáneas vía telnet (line vty 0 4).
- Se puede filtrar el número de usuarios que le pueden hacer telnet al enrutador.
- Esto es un caso especial ya que el tráfico **no esta pasando a través** del enrutador.

31



Comandos de configuración para limitar el acceso vía telnet

```
Router(config) #
```

`line vty {vty# | vty-range}`

- Entra al modo de configuración para una vty o un rango de ellas.

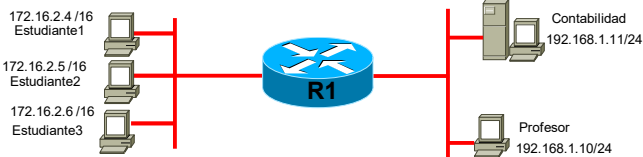
```
Router(config-line) #
```

`access-class access-list-number {in|out}`

- Restringe el tráfico de los equipos que desean hacer telnet.

32

Ejemplo 8



Configure una lista de acceso que solo permita a los equipos de la red 192.168.1.0/24 y el equipo del Estudiante1 hacer telnet al Enrutador R1.

```

R1(config)# access-list 2 permit 172.16.2.4 0.0.0.0
R1(config)# access-list 2 permit 192.168.1.0 0.0.0.255

R1(config)# line vty 0 4
R1(config-line)# access-class 2 in
  
```

33

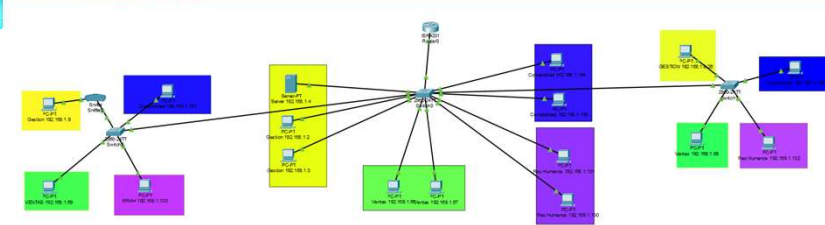
Meme

Cuando conoces una persona
 que sabe configurar:
 VLAN, Trunk ports, RIP, OSPF,
 SNMP, Access Control Lists ...
 Y tu solo sabes instalar: **Packet Tracer**



34

Ejercicio



Amarillo: Gestión
Azul: Contabilidad
Verde: Ventas
Violeta: RRHH

1. Verificar que todos los equipos pueden hacer ping entre sí y pueden acceder al TFTP y HTTP del servidor de Gestión.
2. Que solo los equipos de la VLAN de Contabilidad y Ventas puedan verse con la VLAN de Gestión.
3. Que solo un equipo de la VLAN de RRHH tenga acceso al servidor de Gestión.
4. Que solo los equipos de la VLAN de Gestión puedan hacer telnet a los switches y enrutadores.

35