Gestión de Recursos y Seguridad en Redes
Seguridad en la red con ACL, Cisco

Derman Zepeda Vega

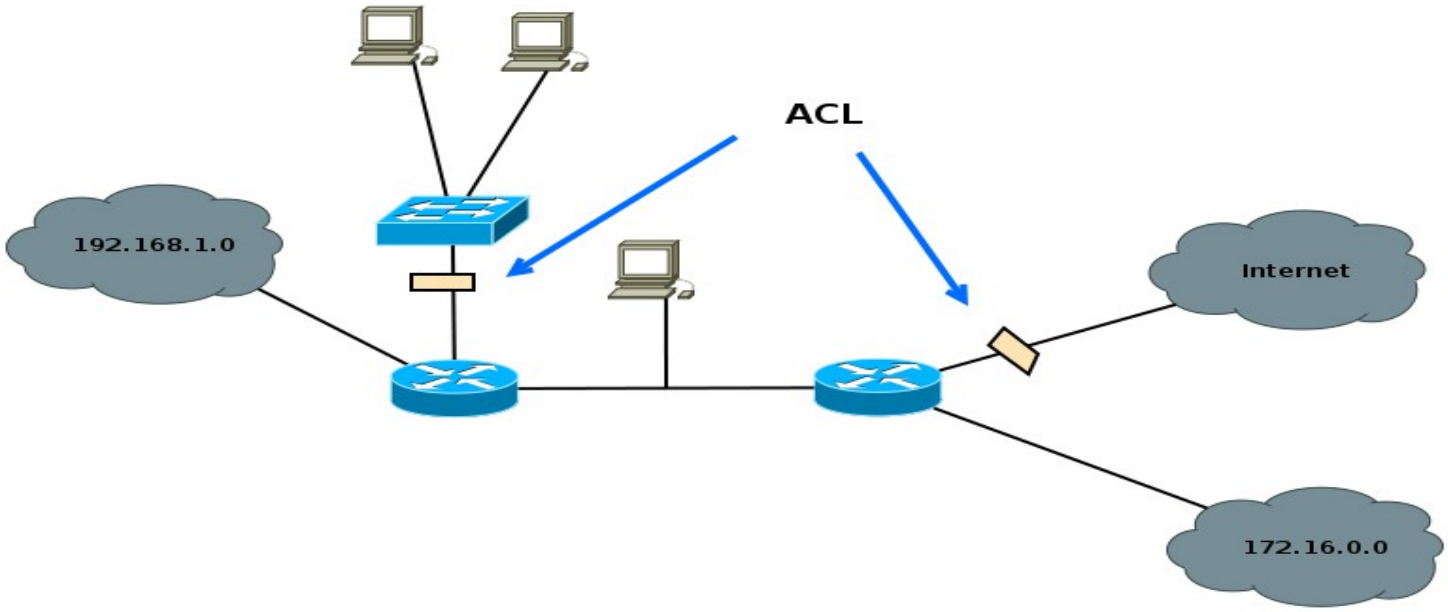
dzepeda@unan.edu.ni

Agenda

- Que es una ACL
- Como se evaluan las ACL
- Clasificacion de las ACL
- Configuracion. (Laboratorio)

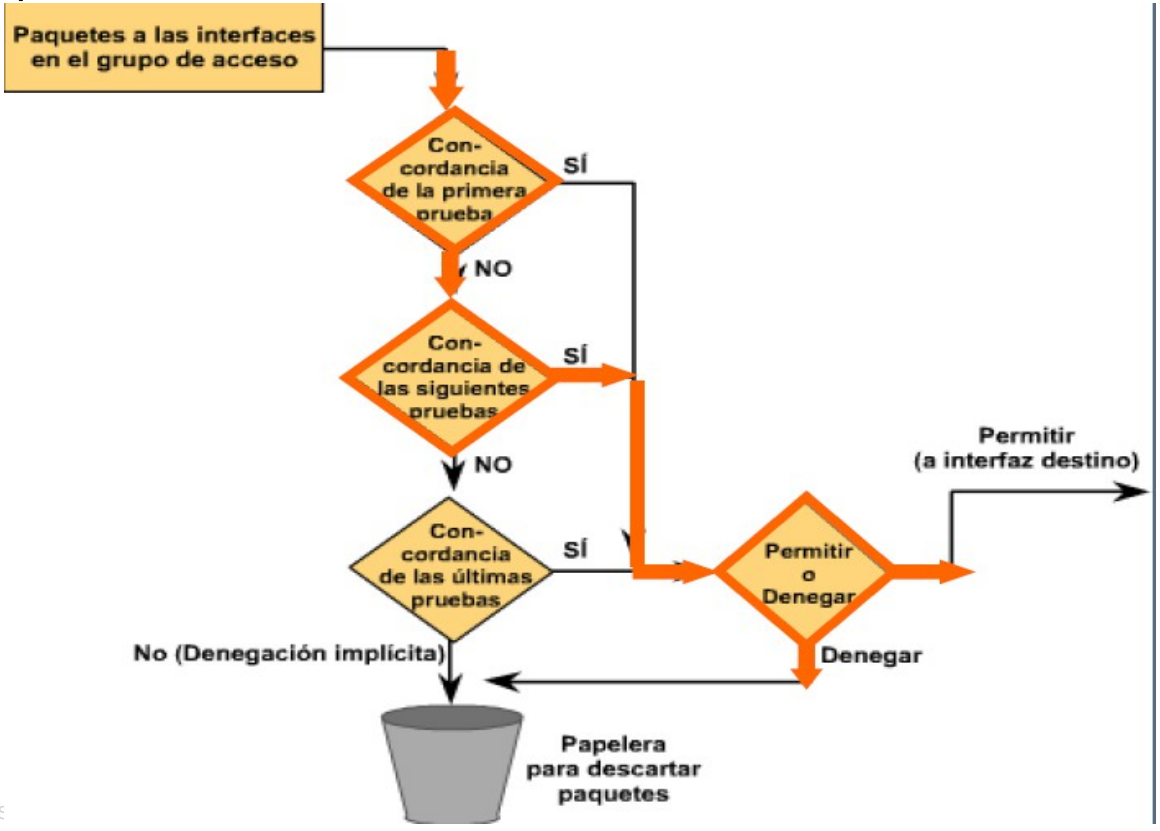
Qué son las ACLs?

- Una ACL, o Lista de control de acceso es una colección secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior



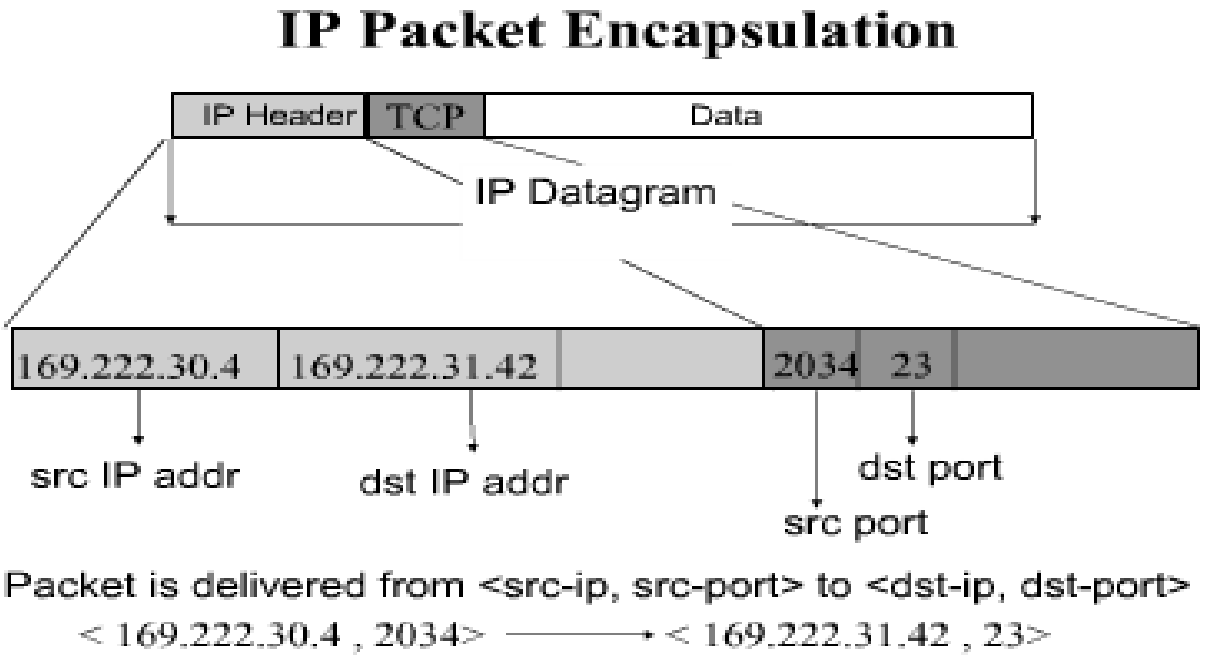
Qué son las ACLs?

- Las listas de control de acceso se evalúan en el orden en el que están escritas. Si se cumple una regla, las demás no se evalúan.



Esquema típico de un firewall

- Las ACLs, pueden contener información de:
  - –Dirección de origen (red o host)
  - –Dirección de destino (red o host)
  - –Protocolo de capa superior (ej.IP, IPX, TCP, IGRP)
  - –Puerto de capa superior (23, 80 ...)



¿Cuántos tipos de ACLs existen?

- **ACLs Estándar**

  Las listas de acceso estándar trabajan únicamente en la capa de red, y por dirección origen

- **ACLs Extendidas**

  Las listas de acceso extendidas trabajan además en la capa de transporte y capas superiores.

¿Cuántos tipos de ACLs existen?

- Las listas de acceso estándar, van de 1 a 99
- Las listas de acceso extendidas, van de 100 a 199.
- En IPX van de 800 a 899 y de900 a 999 respectivamente.

Protocolo	Intervalo
IP	1-99
IP extendido	100-199
AppleTalk	600-699
IPX	800-899
IPX extendido	900-999
Protocolo de publicación de servicio IPX	1000-1099

ACLs Estandares

- Sintaxis:
  - –access-list *num* permit *src-ip mask*
  - –*access-list num deny   src-ip mask*
- Ejemplo:

access-list 1 permit 192.168.3.8

access-list 1 permit 192.168.3.9

access-list 1 permit 192.168.3.10

access-list 1 permit 192.168.3.11

access-list 1 permit 192.168.3.12

access-list 1 permit 192.168.3.13

access-list 1 permit 192.168.3.14

- En su lugar se puede escribir

access-list 1 permit 192.168.3.8 0.0.0.7

ACLs Extendida

- Sintaxis:
  - –permit proto *src-ip mask op dst-ip mask op dst-port*
  - –*deny   proto src-ip mask op dst-ip mask op dst-port*
- Ejemplo:

access-list 100 permit tcp 192.168.3.9 0.0.0.255 host 192.168.3.9 eq 80

access-list 100 permit tcp host 192.168.3.9 host 192.168.3.9 eq 22

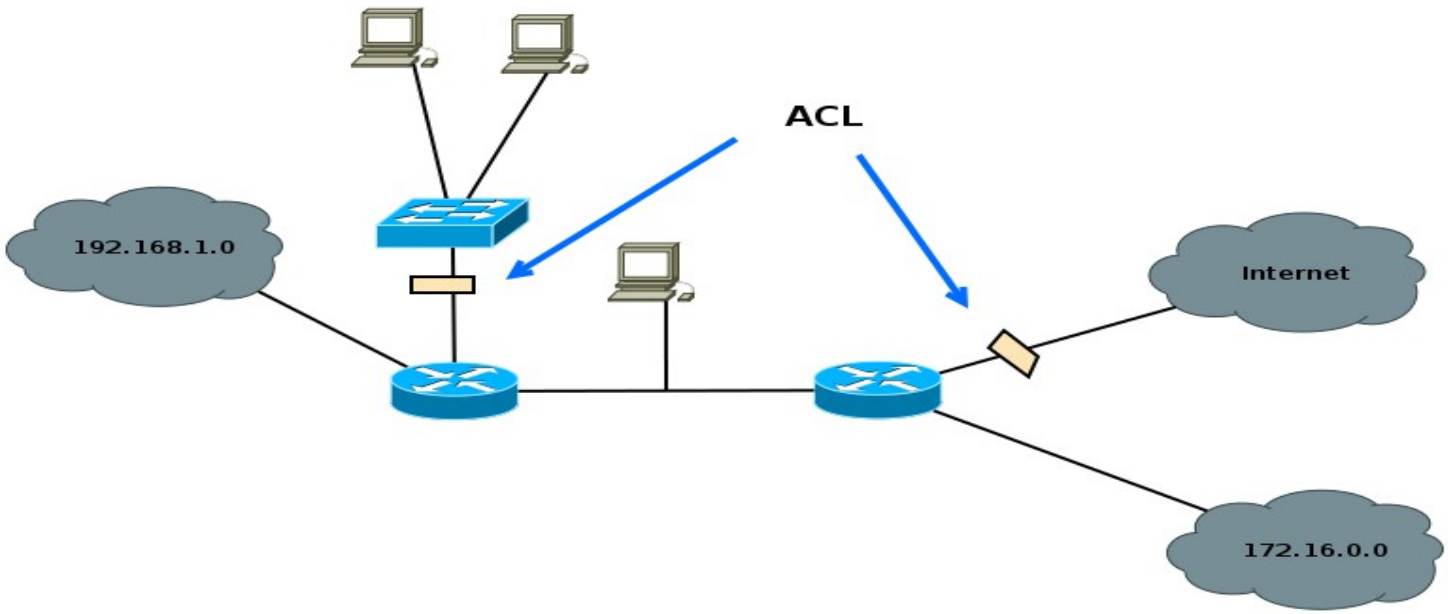
access-list 100 deny tcp host 192.168.3.9 any eq 22

access-list 100 deny tcp host 192.168.3.9 any eq 21

access-list 100 deny any any

¿Cómo se ubican las listas de acceso?

- Las reglas para ubicar las acls:
  - –Las listas estándar : cerca del destino
  - –Las listas extendidas : cerca de la fuente



¿Cómo se verifican las listas de acceso?

- Show access
- listsShow ip interface (muestra si están instaladas y en que dirección out o in)
- Con la opción “log”al crear la lista(muestra el primer paquete al cualse aplica y luego cada 5 minutos)

Resumen

- El propósitode las listas de acceso
- Como son evaluadas las listas de control de acceso
- Los tipos de listas de acceso y cómo se crean y modifican
- La función que cumple la máscara en las listas de acceso
- Crear listas de acceso estándar y extendidas
- Dóndese aplican las listas de acceso según el tipo
- Cómo se verifican las listas de acceso