1. **¿Qué son las Listas de Control de Acceso en redes y cuál es su propósito principal?**

Son un conjunto de reglas que controlan el tráfico que puede ingresar o salir de una red. Su propósito principal es filtrar y regular el acceso a recursos en la red, permitiendo o denegando paquetes basados en criterios específicos como direcciones IP, protocolos, puertos, etc.

1. **¿Cuáles son las principales diferencias entre las ACL estándar y extendidas en IPv4**
   * **ACL estándar:**
     + Filtran el tráfico basándose únicamente en la dirección IP de origen.
     + Se identifican con números entre 1-99 o 1300-1999.
     + Menos flexibles y más genéricas.
   * **ACL extendidas:**
     + Permiten filtrar tráfico basándose en la dirección IP de origen, dirección de destino, protocolo y puertos.
     + Se identifican con números entre 100-199 o 2000-2699.
     + Más específicas y versátiles.
2. **¿Cómo se define una ACL en IPv6 y qué aspectos clave la diferencian de las ACLs en IPv4?**

En IPv6, las ACLs se configuran basándose en nombres y utilizan prefijos en lugar de wildcards para definir rangos de direcciones. Las diferencias clave incluyen:

* + - Soporte directo para prefijos y direcciones IPv6 (no usan wildcards).
    - Incluyen reglas implícitas para el tráfico necesario, como Neighbor Discovery (ND).
    - Usan nombres en lugar de números, lo que facilita su identificación.

1. **¿Qué significa que las ACLs en IPv6 sean "basadas en nombres" y no en números?**

Las ACLs en IPv6 son identificadas por nombres descriptivos en lugar de números. Esto permite una gestión más clara y organizada, especialmente en redes complejas, ya que el nombre puede reflejar su propósito (por ejemplo, "ACL-HTTPS-Only").

1. **¿Cual es la diferencia entre direcciones link-local, global y multicast en IPv6 y cómo afectan la configuración de las ACLs.?**
   * **Link-local:** Solo funcionan dentro de un enlace físico. No suelen necesitar ACLs porque no se enrutan.
   * **Global:** Direcciones únicas en toda la red global, ideales para aplicar reglas de ACL.
   * **Multicast:** Usadas para comunicación en grupo. Las ACLs deben permitir tráfico multicast específico, como el tráfico de ND o protocolos de enrutamiento.
2. **¿Cómo se utiliza el prefijo de subred en IPv6 para definir un rango de direcciones en una ACL?**

El prefijo define un rango de direcciones. Por ejemplo, 2001:db8::/64 incluye todas las direcciones con el mismo prefijo de 64 bits, lo que simplifica la configuración de rangos en una ACL.

1. **¿Qué pasos se deben seguir para crear y aplicar una ACL en IPv6? Proporcione un ejemplo básico.**
   1. **Definir la ACL:**

ipv6 access-list ALLOW-HTTPS

permit tcp any any eq 443

deny ipv6 any any

* 1. **Aplicar la ACL:**

interface GigabitEthernet0/0

ipv6 traffic-filter ALLOW-HTTPS in

1. **Explique cómo funcionan las reglas implícitas de "permitir tráfico ND (Neighbor Discovery)" en ACLs de IPv6.**

Las ACLs en IPv6 incluyen reglas implícitas para Neighbor Discovery Protocol (NDP), permitiendo mensajes ICMPv6 requeridos para el funcionamiento básico de IPv6, como detección de vecinos y resolución de direcciones.

1. **Compare el uso de "wildcards" en IPv4 con las máscaras de prefijo utilizadas en IPv6.**
   * IPv4 usa wildcards (0.0.0.255) para definir rangos específicos.
   * IPv6 utiliza máscaras de prefijo (/64), lo que es más directo y fácil de interpretar.
2. **¿Qué papel juegan los protocolos ICMPv6 en las ACLs de IPv6? ¿Cómo se gestionan en comparación con ICMP en IPv4?**

ICMPv6 maneja funcionalidades esenciales como ND, mensajes de router y diagnóstico. Las ACLs deben permitir mensajes ICMPv6 clave, como echo request y router advertisement.

1. **Investigue cómo se manejan las conexiones entrantes y salientes en IPv6 con respecto a las ACLs.**

Las ACLs pueden definir reglas específicas para tráfico entrante (in) o saliente (out). Por ejemplo:

ipv6 access-list OUTBOUND

permit tcp any any eq 80

deny ipv6 any any

1. **Explique cómo las ACLs en IPv6 manejan el tráfico basado en la clase de tráfico (por ejemplo, tráfico de voz, video, datos).**

Las ACLs pueden priorizar o restringir tráfico por clases, como video o voz, utilizando etiquetas QoS (calidad de servicio) en IPv6.

1. **¿Qué comandos se utilizan para verificar el funcionamiento de una ACL en IPv6? Proporcione ejemplos prácticos.**
   1. **Ver ACL aplicada:**

show ipv6 access-list

* 1. **Ver estadísticas:**

show ipv6 access-list [nombre]

1. **Investigue y compare cómo se manejan las direcciones de broadcast en IPv4 frente a las direcciones multicast en IPv6 dentro de las ACLs.**
   * IPv4 usa direcciones de broadcast (255.255.255.255).
   * IPv6 usa multicast para propósitos similares. Por ejemplo, FF02::1 alcanza todos los nodos en el enlace.
2. **¿Qué desafíos específicos plantea la configuración de ACLs en una red dual-stack (IPv4 e IPv6) y cómo se pueden abordar?**
   * **Doble configuración:** Las ACL deben configurarse para IPv4 e IPv6.
   * **Solución:** Usar herramientas de gestión unificadas para aplicar reglas consistentes.
3. **Describa un caso práctico donde las ACLs en IPv6 sean utilizadas para segmentar y proteger el tráfico de una red.**
   * Un departamento financiero podría tener acceso solo a un servidor interno mediante:

ipv6 access-list FINANCE

permit tcp 2001:db8:1::/64 host 2001:db8:2::1 eq 443

deny ipv6 any any

1. **Diseñe una regla básica de configuración de una ACL en IPv6 que permita solo el acceso HTTPS desde una red específica y bloquee todo lo demás.**

ipv6 access-list HTTPS-ONLY

permit tcp 2001:db8:1::/64 any eq 443

deny ipv6 any any

***Fuentes:***

<https://www.sapalomera.cat/moodlecf/RS/2/course/module9/9.5.2.2/9.5.2.2.html>

<https://support.hpe.com/techhub/eginfolib/networking/docs/switches/YA-YB/16-02/5200-1665_YAYB_IPv6/content/ch06.html>

<https://info.support.huawei.com/hedex/api/pages/EDOC1100413634/FEN1022J/02/resources/en-us_topic_0000001225351288.html>