Unidad 05 — Control de tráfico y publicaciones

Esta unidad cubre las herramientas que un router usa para decidir qué tráfico dejar pasar y qué rutas enseñar o aprender por los protocolos de ruteo dinámico. Las ACL (Access Control Lists) filtran tráfico IP en base al contenido de los paquetes; las distribute-list usan esas mismas ACL para filtrar los prefijos que un protocolo de ruteo publica o recibe; las prefix-list son una alternativa más flexible pensada específicamente para filtrar rangos de prefijos; y los route-map son la herramienta más general, capaz de combinar condiciones (match) con acciones (set) para aceptar, rechazar o modificar atributos de una ruta.

Conceptos clave

ACL estándar

Rango 1–99 (y 1300–1999 extendido). Filtra únicamente por IP origen . Sintaxis: access-list {permit|deny} source [wildcard] .

ACL extendida

Rango 100–199 (y 2000–2699 extendido). Filtra por protocolo, IP origen, IP destino y puerto. Sintaxis: access-list {permit|deny} protocol source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [log] .

ACL nombrada

Se identifica por nombre en vez de número: ip access-list {standard|extended} , y las líneas de permit/deny se ingresan como subcomandos.

Wildcard mask

Máscara inversa a la de subred: bit en 0 = chequea ese bit, bit en 1 = no chequea (no importa su valor).

Deny implícito

Toda ACL termina con un deny any (o equivalente) implícito: si ninguna línea hizo match, el tráfico se descarta.

Distribute-list

Filtra los prefijos que un protocolo de ruteo dinámico enseña o aprende, usando una ACL como criterio. Máximo una distribute-list de entrada y una de salida en configuración global por proceso de ruteo (además puede haber una in y una out por interfaz).

Prefix-list

Alternativa a las ACL pensada para filtrar prefijos, identificada por nombre y con sentencias numeradas (número de secuencia) evaluadas en orden creciente. Última línea implícita: deny 0.0.0.0/0 le 32 .

Atributos ge / le

ge (greater equal): la máscara del prefijo evaluado debe ser igual o más específica que el valor indicado. le (less equal): debe ser igual o menos específica que el valor indicado.

Route-map

Secuencia ordenada de declaraciones (statements), cada una con condiciones match y acciones set , y un resultado permit / deny . Si no hay match en ninguna declaración, se aplica un deny implícito final (igual que en una ACL).

Puntos clave para repasar

- ACL estándar: rango 1–99. Solo IP origen. ip access-group {in|out}
- ACL extendida: rango 100–199. Protocolo + origen + destino + puerto + established/log
- ACL nombrada: ip access-list {standard|extended} , subcomandos permit/deny
- Lógica del router: ACL IN → ruteo → ACL OUT ; Deny en cualquiera de las dos → descarte
- Wildcard: 0 = chequea el bit, 1 = no chequea
- Toda ACL termina con un deny any implícito
- Distribute-list: filtra rutas de un protocolo dinámico usando una ACL. Máximo 1 in + 1 out global por proceso (más 1 in + 1 out por interfaz)
- Prefix-list: ip prefix-list [seq n] {deny|permit} red/máscara [ge n] [le n] . Deny implícito final: 0.0.0.0/0 le 32
- ge = máscara igual o más específica · le = máscara igual o menos específica que el valor indicado
- Route-map: secuencia de match (condición) + set (acción) → permit/deny. Match implícito descarta si nada coincide (ídem ACL). Secuencias por defecto: 10, 20, 30...
- Flexibilidad creciente: distribute-list (solo filtra, usa ACL) < prefix-list (filtra por rango de prefijos, más eficiente) < route-map (filtra y modifica atributos, la más general)