Redes 2

Resumen de repaso — las 8 unidades

Conceptos clave y puntos de repaso condensados a partir del material del curso.
Para el detalle completo con diagramas y ejemplos, ver el sitio de repaso online.

Unidad 00 — Repaso

Antes de entrar en los protocolos específicos de Redes 2 (BGP, MPLS, redundancia, QoS), conviene repasar la base común a todos ellos: cómo arma un router su tabla de ruteo , con qué criterios elige entre rutas cuando tiene varias opciones, cómo se subnetea una red, y cómo funciona NAT/PAT para traducir direcciones entre redes privadas y públicas. Estos conceptos son transversales: la Distancia Administrativa y el orden de los criterios de selección de rutas reaparecen en todas las unidades siguientes.

Conceptos clave

Routing (enrutamiento)

Aprendizaje y actualización de la topología lógica de la red. Cada router intercambia información con los demás y la registra en una o varias tablas (tabla topológica, tabla de ruteo, etc.).

Switching / Forwarding (conmutación)

Recepción de paquetes que ingresan por una interfaz de entrada y su retransmisión por la interfaz de salida correspondiente, en base a lo que indica la tabla de ruteo.

Los tres análisis del router

Para rutear un paquete el router hace: 1) interpretación del esquema de direccionamiento (TCP/IP, IPX, etc.), 2) búsqueda en la tabla de ruteo de un registro para esa dirección (o se usa la ruta por defecto, si existe), y 3) selección de la interfaz de salida según el esquema de métricas.

Distancia Administrativa (DA)

Valor numérico que indica la confiabilidad del protocolo (o método) por el que se aprendió una ruta. A menor DA, mayor confiabilidad. Es el criterio de desempate entre rutas de igual especificidad aprendidas por medios distintos.

Métrica

Parámetro (o conjunto de parámetros) que mide la conveniencia de una ruta frente a otras hacia el mismo destino. Depende del protocolo: RIP usa saltos, EIGRP combina ancho de banda y retardo mínimos, OSPF usa costo (según ancho de banda), IS-IS usa costo configurable, y BGP evalúa un conjunto de atributos en orden específico.

Ruta más específica

Independientemente del protocolo por el que se haya aprendido, ante rutas con distinto prefijo hacia un destino, gana siempre la de prefijo más largo (más específica).

Subneteo

Proceso de dividir una red en subredes más pequeñas incrementando la longitud de la máscara, es decir, tomando bits del campo de host para asignarlos a la parte de red y generar prefijos más específicos.

NAT (Network Address Translation)

Mecanismo que traduce direcciones IP al atravesar la frontera entre una red interna/privada (Inside) y una red externa/pública (Outside), habitualmente Internet.

PAT (Port Address Translation)

Variante de NAT dinámico con sobrecarga: traduce muchas direcciones internas a una única (o pocas) direcciones públicas, distinguiendo cada traducción por el puerto de capa 4 de origen.

Inside Local / Inside Global

Inside Local es la IP real de un host dentro de la red privada (cómo se ve a sí mismo). Inside Global es la IP con la que ese mismo host se ve representado hacia Internet (la que asigna el NAT).

Outside Local / Outside Global

Outside Local es cómo perciben los hosts internos a un host externo (puede diferir de la real si el NAT también traduce direcciones de destino). Outside Global es la dirección real de ese host tal como existe en la red externa.

Puntos clave para repasar

- Ruta más específica
- Distancia Administrativa (DA) menor
- Métrica menor (si empatan especificidad y DA → hasta 6 rutas en balance de carga)
- Subredes: 2^(máscara nueva − máscara original) · Hosts por subred: 2^(32 − prefijo)
- Rangos que se solapan pero con prefijo distinto = destinos distintos → todas se instalan
- Mismo destino exacto → gana menor DA, luego menor métrica, luego balance de carga (hasta 6 rutas)
- NAT estático: uno a uno, para exponer servidores internos (relación fija, consume una IP pública por host)
- NAT dinámico sin sobrecarga: pool de IPs públicas, traducción sólo si la conexión se inicia desde adentro
- PAT (NAT dinámico con sobrecarga): identifica traducciones por IP + puerto de origen; keyword overload
- Inside Local/Global: cómo se ve un host interno desde adentro / desde afuera. Outside Local/Global: cómo se ve un host externo desde adentro / en la realidad

Unidad 01 — Topologías y enrutamiento

Esta unidad recorre el diseño estructurado de redes IP (modelo jerárquico de tres capas), la clasificación de los protocolos de ruteo (classful/classless, IGP/EGP, vector distancia/estado de enlace), el ruteo estático, y en profundidad los tres protocolos de estado de enlace y vector distancia más usados a nivel de campus y proveedor: RIP , OSPF e IS-IS . Cierra con IPv6 : formato, tipos de direcciones y autoconfiguración (SLAAC/EUI-64). Es la unidad más extensa del curso y la más preguntada en los exámenes, especialmente el cálculo de costo OSPF, la elección de DR/BDR, los tipos de LSA, las áreas especiales, la comparación OSPF/IS-IS y los cálculos de direccionamiento IPv6.

Conceptos clave

ABR (Area Border Router)

Router OSPF con interfaces en al menos dos áreas distintas (una de ellas puede ser el área 0). Mantiene una link-state database por cada área a la que está conectado y resume rutas entre ellas.

ASBR (Autonomous System Boundary Router)

Router OSPF con al menos una interfaz hacia otro sistema autónomo (u otro protocolo). Redistribuye rutas externas hacia OSPF mediante LSA tipo 5 (o tipo 7 si el área es NSSA).

DR / BDR

En redes de acceso múltiple (broadcast), el Router Designado (DR) y su respaldo (BDR) concentran las adyacencias para reducir el tráfico de n(n-1)/2 a 2(n-1). Se eligen por prioridad (default 1, 0 = no elegible) y, en caso de empate, por Router ID más alto. La elección no es preemptiva.

LSA (Link State Advertisement)

Mensaje mediante el cual los routers de estado de enlace anuncian el estado de sus enlaces. Existen varios tipos (1, 2, 3, 4, 5, 7…) según su alcance y origen.

Áreas especiales OSPF

Stub (no acepta LSA tipo 5, externo, usa ruta default), Totally Stubby (tampoco acepta LSA 3/4 de resumen, solo default) y Backbone/Área 0 (acepta todos los tipos de LSA e interconecta todas las demás áreas).

Niveles IS-IS (L1 / L1L2 / L2)

IS-IS no tiene un área backbone fija como el área 0 de OSPF. En su lugar organiza la jerarquía en niveles: L1 (intra-área, análogo a router interno), L1/L2 (frontera entre áreas, análogo a ABR) y L2 (backbone virtual formado por todos los routers L2/L1L2, análogo a routers de backbone).

NET (Network Entity Title)

Dirección que identifica a un router IS-IS (no usa IP): AFI (1 byte, habitualmente 49) + Area ID + System ID (6 bytes, único por router) + NSEL (1 byte, siempre 00). Ej: 49.0001.1921.6800.1001.00 .

SLAAC / EUI-64

Mecanismo de autoconfiguración stateless de IPv6: el router anuncia el prefijo /64 vía Router Advertisement, y el host arma el Interface ID de 64 bits a partir de su MAC (EUI-64): separa

la MAC en dos mitades de 24 bits, inserta FFFE en el medio e invierte el bit U/L (7° bit) del primer byte.

Puntos clave para repasar

- Modelo jerárquico: Acceso → Distribución → Core/Backbone
- Classful (no manda máscara): RIPv1, IGRP · Classless (manda máscara, VLSM): RIPv2, EIGRP, OSPF, IS-IS, BGP
- IGP (dentro de un AS) vs EGP (entre AS) · Vector distancia (RIP, EIGRP) vs Estado de enlace (OSPF, IS-IS)
- Ruteo estático: ip route network mask {address|interface} [distance]
- RIP: vector distancia, métrica=saltos (máx 15), updates cada 30s, balancea hasta 6 caminos
- Costo OSPF = BWref (default 100 Mbps) / BWenlace (Mbps) , redondeo hacia arriba, mínimo 1
- OSPF: Hello=10s · Dead=40s · SPF delay=5s · Área 0 obligatoria
- DR/BDR: reduce adyacencias de n(n-1)/2 a 2(n-1); prioridad default 1 (0=no elegible); empate→Router ID; no preemptivo; no aplica en punto a punto
- LSA: Tipo 1 (router, intra-área) · Tipo 2 (network, DR, intra-área) · Tipo 3/4 (summary inter-área; 4=ABR→ASBR) · Tipo 5 (externo AS) · Tipo 7 (NSSA)
- Áreas especiales: Stub (no LSA 5, usa default) · Totally Stubby (tampoco LSA 3/4) · Backbone (acepta todo)
- IS-IS: IS=router, ES=host, LSP=LSA, NET=AFI(49).AreaID.SystemID(6B).NSEL(00)
- IS-IS niveles: L1 (intra-área, ~router interno) · L1/L2 (frontera, ~ABR) · L2 (backbone virtual, ~backbone)
- Métrica IS-IS: narrow 6 bits (máx 63) · wide 24 bits (máx 16.777.215) · default 10 · no depende del ancho de banda
- IS-IS corre directo sobre capa 2 (no usa IP) · OSPF corre sobre IP, protocolo 89
- IPv6: 128 bits, 8 bloques hex de 16 bits · comprimir un único grupo de ceros con :: (nunca dos veces)
- GUA 2000::/3 · ULA FC00::/7 (~10.0.0.0/8) · Link-local FE80::/10 · Multicast FF00::/8 (no hay broadcast)
- EUI-64: separar MAC en 2 mitades de 24 bits, insertar FFFE en el medio, invertir bit U/L del primer byte

Unidad 02 — Redistribución de rutas

Cuando conviven más de un protocolo de ruteo en la misma red (por ejemplo durante una migración, o porque distintas áreas administrativas usan protocolos distintos), cada protocolo desconoce por defecto las rutas del otro. La redistribución permite que un router que hable dos protocolos "inyecte" en uno la información aprendida por el otro. Puede hacerse en un solo sentido (redistribución simple) o en los dos sentidos (redistribución doble), y esta última, si se realiza en más de un punto de interconexión entre las mismas dos redes, puede provocar loops de ruteo — uno de los puntos más preguntados en los exámenes.

Conceptos clave

Redistribución simple

La información conocida por un protocolo se difunde por otro, en un solo sentido. Permite conectividad unidireccional: el host del lado que recibe la redistribución puede llegar al otro lado, pero no al revés.

Redistribución doble

El mecanismo se aplica en los dos sentidos (cada protocolo redistribuye al otro). La conectividad pasa a ser total entre ambas redes.

Loop de ruteo por doble redistribución

Si la doble redistribución entre las mismas dos redes se configura en más de un router (dos puntos de interconexión), un router puede aprender una ruta tanto directamente por su protocolo de origen como, con retraso, por el protocolo redistribuido desde el otro punto. Si esa segunda versión resulta preferida por la métrica/distancia administrativa, se forma un loop.

Distancia Administrativa (D.A.)

Valor que usa el router para elegir entre rutas al mismo destino aprendidas por protocolos distintos: gana la de menor D.A. EIGRP interno (90) es más confiable por defecto que OSPF (110).

auto-summary (EIGRP)

EIGRP es classful por defecto: resume automáticamente en los límites de clase (A/B/C), perdiendo especificidad de subredes. no auto-summary desactiva ese resumen automático.

Ruta externa tipo 2 (E2 / EX)

Ruta redistribuida hacia OSPF (E2) o EIGRP (EX): conserva el costo/métrica que tenía en el momento de ser redistribuida y no lo recalcula al atravesar la red de destino.

Forward metric

En una ruta OSPF externa tipo 2, es el costo interno OSPF hasta el ASBR que redistribuyó la ruta. Solo se usa como desempate entre rutas E2 hacia el mismo destino con igual métrica externa.

Puntos clave para repasar

- Redistribución simple = conectividad en un solo sentido. Redistribución doble = conectividad total.

- Doble redistribución en un solo router: sin riesgo de loop. En dos o más puntos de interconexión entre las mismas redes: riesgo de loop de ruteo.
- Todo redistribute requiere (o toma por defecto) una métrica semilla en el protocolo destino — la métrica original casi siempre se pierde al cruzar de un protocolo a otro.
- EIGRP es classful por defecto (auto-summary encendido): corregir con no auto-summary en cada router para anunciar subredes específicas en vez de resúmenes por clase.
- Fórmula simplificada de métrica EIGRP: metric = 256 × (10^7/bandwidth + delay)
- OSPF E2 (type extern 2): la métrica no cambia al atravesar la red OSPF; forward metric = costo interno hasta el ASBR, solo para desempate.
- Comandos típicos: redistribute rip metric 200 · redistribute ospf 100 metric 7 · redistribute static metric 5 · default-information originate metric 250

Unidad 03 — BGP (Border Gateway Protocol)

BGP es el protocolo de ruteo que sostiene Internet: conecta Sistemas Autónomos (AS) entre sí. A diferencia de los IGP vistos antes (RIP, OSPF, IS-IS), BGP es un protocolo exterior (EGP) , de tipo path vector , diseñado para escalar a redes enormes y para decidir la mejor ruta en base a atributos configurables en vez de una métrica única.

Conceptos clave

Sistema Autónomo (AS)

Conjunto de redes bajo una misma administración, identificado por un número único (1–65535 en AS de 16 bits, privados 64512–65535; desde 2007 existen AS de 32 bits, 1 a 4.294.967.295).

iBGP / eBGP

iBGP corre entre routers del mismo AS; eBGP corre entre routers de AS distintos . Las vecindades BGP siempre son punto a punto, sobre TCP puerto 179.

AS-Path

Lista de AS por los que pasó la ruta. Detecta loops (repetición no contigua descarta la ruta) y permite prepends (repetición contigua del propio AS para empeorar artificialmente una ruta). Well-known mandatory.

MED (Multi Exit Discriminator)

Influye en vecinos eBGP directos para indicarles por qué enlace enviar el tráfico. No se transfiere a otros AS (optional non-transitive). Gana el valor menor .

Local Preference (LP)

Se intercambia solo dentro del mismo AS. Define la salida preferida del AS. Well-known discretionary. Gana el valor más alto .

Weight

Atributo propietario de Cisco, local al router (no se anuncia ni siquiera dentro del AS). Gana el valor más alto . Se evalúa antes que Local Preference.

Origin

Indica cómo se originó la ruta: IGP (i) > EGP (e) > Incomplete (?), en orden de preferencia. Well-known mandatory.

Route Reflector (RR)

Router iBGP que redistribuye rutas aprendidas de un vecino iBGP a sus clientes reflectores, rompiendo de forma controlada la regla del horizonte dividido de BGP. Evita el full-mesh iBGP.

Puntos clave para repasar

- Puerto TCP 179 · AS 16 bits 1–65535 (privados 64512–65535) · AS 32 bits desde 2007
- iBGP = mismo AS · eBGP = AS distintos
- Orden de selección: Weight > LP > local (network/redistribute) > AS-Path > Origin > MED > eBGP>iBGP > costo IGP > más antigua > menor Router ID

- Weight: local al router, gana el mayor. LP: dentro del AS, gana el mayor. MED: entre AS vecinos, gana el menor.
- Origin: IGP(i) > EGP(e) > Incomplete(?)
- Sincronización: no anunciar por eBGP lo aprendido por iBGP sin verlo en el IGP (previene black holes)
- Horizonte dividido en BGP: no reenviar por iBGP lo aprendido por iBGP (previene loops internos)
- Route Reflector: rompe el horizonte dividido a propósito para evitar full-mesh iBGP. Sin RR: N(N-1)/2 sesiones. Con M RR: (N-M)×M

Unidad 04 — Redundancia en redes de datos

El objetivo de la redundancia es asegurar la continuidad del funcionamiento ante un fallo simple (un fallo en un punto específico de la red), previendo caminos alternativos que se utilicen automáticamente si los actuales dejan de estar disponibles. Este curso analiza la redundancia en tres niveles : dentro de la LAN (protocolos de primer salto redundante: HSRP, VRRP, GLBP), entre Sistemas Autónomos (multihoming con BGP) y en sistemas de servidores (Round Robin de DNS, Anycast, Server Load Balancing).

Conceptos clave

HSRP (Hot Standby Router Protocol)

Mecanismo propietario de Cisco (1994, RFC 2281) que provee una salida redundante a los hosts de una LAN mediante una IP y una MAC virtuales compartidas por un router activo y uno standby.

VRRP (Virtual Router Redundancy Protocol)

Mecanismo creado por IETF en 1999 (RFC 3768), similar a HSRP pero de múltiples proveedores (no propietario), con temporizadores más rápidos por defecto.

GLBP (Gateway Load Balancing Protocol)

Mecanismo de Cisco (2005) que permite balance de carga real del default gateway sin necesidad de definir múltiples grupos (a diferencia de MHSRP), usando los roles AVG y AVF.

AVG y AVF (terminología GLBP)

AVG (Active Virtual Gateway): responde las solicitudes ARP a la IP virtual y asigna a cada router del grupo una MAC virtual distinta. AVF (Active Virtual Forwarder): router responsable de reenviar el tráfico dirigido a una de esas MAC virtuales (hasta 4 AVF por grupo).

MHSRP (Multi-group HSRP)

Balanceo de carga mediante dos (o más) grupos HSRP independientes en la misma LAN: un router es activo en un grupo y standby en el otro, y viceversa. Distintos hosts usan distinta IP virtual como default gateway.

Multihoming

Redundancia de proveedores de acceso a Internet mediante BGP, empleando un número de Sistema Autónomo público para identificar el origen de las publicaciones de direcciones propias.

Round Robin de DNS

Tener más de un registro DNS para un mismo nombre, devolviendo la lista en distinto orden en cada consulta. No detecta fallos de servidor ni asegura balance real de carga.

Anycast

Replicar servidores con el mismo direccionamiento IP; el cliente accede por el camino de menor métrica. Requiere dejar de anunciar la ruta ante una caída, y solo sirve para servicios resolubles con un solo paquete (falta de persistencia), típicamente DNS.

SLB (Server Load Balancing)

Granja de servidores reales detrás de un balanceador de carga accesible mediante una única IP virtual, que reparte el tráfico entre ellos.

Puntos clave para repasar

- HSRP (Cisco, RFC 2281): hello 3s / hold 10s. MAC virtual 0000.0C07.ACxx . Prioridad más alta = activo. standby preempt para recuperar el rol. standby track decrementa la prioridad (10 por defecto) si cae el uplink monitoreado.
- VRRP (IETF, RFC 3768): hello 1s por defecto. Hold = 3×Advertisement + tiempo skew (inversamente proporcional a la prioridad).
- GLBP (Cisco, 2005): hello 3s, multicast 224.0.0.102, UDP 3222. AVG asigna MAC virtuales; hasta 4 AVF por grupo; hasta 1024 grupos. Algoritmos: Round-Robin, Por Peso, Dependiente del Host. Único que balancea carga sin necesitar múltiples grupos ni default gateways distintos.
- MHSRP: balanceo mediante 2+ grupos HSRP, cada router activo en uno y standby en otro.
- HSRP/VRRP solo protegen el tráfico saliente de la LAN; el entrante depende de los anuncios de rutas del IGP.
- Multihoming BGP — 3 alternativas de recepción: solo default · partial routing (default + rutas de clientes por AS-Path) · full routing table.
- Tráfico saliente: se controla con route-map + prefix-list / as-path access-list en cada neighbor.
- Tráfico entrante: distinta especificidad por punto de ingreso (con sumarización de respaldo), o prepends selectivos por rango de direcciones.
- Round Robin DNS: no detecta caídas de servidor. Anycast: requiere dejar de anunciar la ruta al caer, sin persistencia (solo servicios de 1 paquete, ej. DNS). SLB: granja de servidores tras una IP virtual y un balanceador.
- Stateless Backup (redundancia de balanceadores) se implementa con HSRP en switches de capa 3.

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)

Unidad 06 — MPLS (Multi Protocol Label Switching)

El ruteo IP tradicional busca el prefijo más largo en cada salto, lo que consume procesamiento y no da control fino sobre el camino que toma el tráfico. MPLS no reemplaza al ruteo IP, lo complementa : agrega una capa de conmutación por etiquetas entre capa 2 y capa 3, de forma que los routers del núcleo solo miran una etiqueta de 20 bits en vez de la tabla de ruteo completa. Esto habilita ingeniería de tráfico y VPNs de capa 2 y 3 sobre una misma infraestructura compartida.

Conceptos clave

Label (etiqueta)

Identificador de 20 bits, de significado local a cada router, que representa una FEC durante el reenvío.

FEC (Forwarding Equivalence Class)

Conjunto de paquetes tratados de la misma manera (mismo destino, misma QoS, misma VPN).

LSP (Label Switched Path)

Camino unidireccional predefinido a través de la red MPLS que une el router de ingreso (Ingress LER) con el de egreso (Egress LER).

LER / LSR

LER (Label Edge Router, = PE) agrega o quita etiquetas en el borde de la red. LSR (Label Switch Router, = P) solo conmuta etiquetas en el núcleo, sin conocer las rutas de los clientes.

LIB / LFIB

LIB: base de datos de etiquetas del plano de control (análoga a la RIB). LFIB: base de datos del plano de datos con la interfaz y next-hop de las mejores rutas (análoga a la FIB).

Puntos clave para repasar

- Encabezado (32 bits): Label(20) + Exp(3) + S(1) + TTL(8)
- PE = LER (borde, push/pop) · P = LSR (núcleo, solo swap)
- Etiquetas especiales: 0 Explicit Null IPv4 · 1 Alerta Router · 2 Explicit Null IPv6 · 3 Implicit Null (PHP)
- PHP: el penúltimo router (P) hace el POP, no el egress PE
- LIB = plano de control (todas las etiquetas) · LFIB = plano de datos (mejores rutas + next-hop)
- LDP requiere IGP ya configurado (asocia etiquetas a rutas existentes)
- RD: hace único el prefijo entre VPNs (prefijo vpnv4 = RD + IPv4). No decide import.
- RT: decide import/export de rutas entre VRFs (comunidad extendida BGP)
- VPN L3: doble etiqueta — exterior = LSP (la ven los P) · interior = VPN (solo la ven los PE, viaja por MP-BGP)

Unidad 07 — QoS (Quality of Service)

En redes IP tradicionales, todo el tráfico se trata como mejor esfuerzo (best effort) , sin garantías de entrega, retardo ni temporización. El tráfico de tiempo real (voz, video, juegos en línea) es sensible a la latencia , el jitter y la pérdida de paquetes ; el tráfico de mejor esfuerzo (correo, navegación web) tolera mucho mejor esas variaciones. QoS (Quality of Service) es la capacidad de una red de dar un servicio diferenciado a clases de tráfico seleccionadas, priorizando, garantizando ancho de banda y controlando el orden de entrega mediante un conjunto de mecanismos: clasificación, regulación de tráfico, encolamiento y gestión de congestión.

Conceptos clave

Ancho de banda

Cantidad máxima de datos que pueden transmitirse por una red en un tiempo determinado (Mbps, Gbps).

Latencia

Tiempo que tarda un paquete en ir desde el origen hasta el destino, medido en milisegundos.

Jitter (variación de retardos)

Variación en el tiempo de llegada de paquetes de un mismo flujo. Un jitter alto degrada la calidad de voz/video en tiempo real.

Pérdida de paquetes (Loss)

Paquetes que no llegan a destino, típicamente por congestión, expresada como % del total enviado.

Puntos clave para repasar

- Parámetros de calidad: Ancho de banda, Latencia, Jitter, Pérdida de paquetes
- IP Precedence (RFC 791): 3 bits, 8 niveles · 111 Network control … 000 Routine
- DSCP (RFC 2474/2475): 6 bits del byte ToS, 64 valores · EF=46 (voz) · AFxy (x=clase 1-4, y=drop Low/Med/High) · BE=0 (defecto)
- Policing: controla tasa de entrada/salida, descarta o remarca, sin buffer, no añade latencia
- Shaping: controla tasa de salida, retiene en buffer, puede añadir latencia, solo en egreso
- CAR (policing con Token Bucket): CIR (tasa comprometida) · Bc (ráfaga normal) · Be (ráfaga excedente) · zonas: 0-CIR garantizado, CIR-CIR+Bc normal burst, CIR+Bc-CIR+Bc+Be excess burst, >CIR+Bc+Be descarte
- Buffer de dejitter: uniformiza la salida de paquetes compensando el jitter; estático (fijo) vs dinámico (adaptativo); trade-off buffer grande = más latencia, buffer chico = más descarte
- Colas: FIFO (sin prioridad) · PQ (prioridad absoluta, riesgo starvation) · CQ (hasta 16 colas, % cíclico, en desuso) · WFQ (ponderada por precedencia) · LLQ = PQ (voz) + CBWFQ (resto) , la más usada en la práctica

- WRED: prevención de congestión (no es encolamiento), descarte aleatorio creciente entre umbral mínimo y máximo, ponderado por DSCP/precedencia
- Fragmentación + Intercalado: acota el tiempo de espera de la voz entre fragmentos de datos grandes
- VAD: ahorra ~35% del BW de voz detectando silencios
- SIP: UAC/UAS (endpoints) · Proxy (enruta) · Registrar (ubicación) · flujo REGISTER → INVITE → 180 Ringing → 200 OK → ACK → RTP → BYE
- QoS para VoIP: señalización SIP → DSCP CS3/AF31 + CBWFQ · media RTP → DSCP EF + LLQ