# 3. Marco Teórico

## Conceptos de Protocolos de Enrutamiento

**¿Qué es un protocolo de enrutamiento y cómo funciona?**

Un protocolo de enrutamiento es un conjunto de normas que utilizan los dispositivos de red para decidir cómo enviar un paquete de datos hasta su destino final. En esencia, estos protocolos se encargan de determinar el camino que recorrerán los datos dentro de una red. Existen dos tipos principales de enrutamiento: estático y dinámico.

**El enrutamiento estático** El enrutamiento estático implica que el administrador configure manualmente las rutas en cada dispositivo de la red. Esta técnica resulta útil en redes pequeñas con pocos dispositivos, pero se vuelve complicada y propensa a errores conforme la red crece.

**El enrutamiento dinámico**En cambio, el enrutamiento dinámico se basa en algoritmos que calculan automáticamente la mejor ruta para los datos. Los dispositivos intercambian información sobre el estado actual de la red y, con base en ella, eligen el camino más eficiente para el envío de los paquetes. Este tipo de enrutamiento es más adecuado para redes grandes, ya que ofrece mayor escalabilidad y tolerancia a fallos.

Además, los protocolos de enrutamiento se dividen en dos grandes grupos: los internos, que operan dentro de una misma red o sistema autónomo, y los externos, que se utilizan para comunicar diferentes sistemas autónomos entre sí.

# Clasificación (Interior / Exterior)

## Protocolos de enrutamiento interno

Los protocolos de enrutamiento interno se utilizan dentro de una sola red autónoma. Una red autónoma es un grupo de dispositivos que comparten una misma política de enrutamiento. Los protocolos de enrutamiento interno son comúnmente utilizados en redes de tamaño medio a grande.

Algunos ejemplos de protocolos de enrutamiento interno incluyen:

* **OSPF (Open Shortest Path First)**: Es un protocolo de enrutamiento de estado de enlace que utiliza un algoritmo Dijkstra para calcular las rutas más cortas en una red. OSPF es ampliamente utilizado en redes empresariales.
* **RIP (Routing Information Protocol)**: Es un protocolo de enrutamiento de vector de distancia que mantiene una tabla de enrutamiento basada en el número de saltos entre los dispositivos. RIP es un protocolo de enrutamiento antiguo que todavía se utiliza en redes pequeñas y simples.
* **EIGRP (Enhanced Interior Gateway Routing Protocol)**: Es un protocolo de enrutamiento de estado de enlace propietario de Cisco que se utiliza en redes empresariales. EIGRP utiliza un algoritmo DUAL (Diffusing Update Algorithm) para calcular las rutas más eficientes en la red.

## Protocolos de enrutamiento externo

Los protocolos de enrutamiento externo se utilizan para comunicar dos o más redes autónomas. Estos protocolos de enrutamiento se utilizan para compartir información de enrutamiento entre diferentes redes. Algunos ejemplos de protocolos de enrutamiento externo incluyen:

* **BGP (Border Gateway Protocol)**: Es un protocolo de enrutamiento de vector de distancia que se utiliza para interconectar diferentes sistemas autónomos. BGP es utilizado principalmente por los proveedores de servicios de Internet para intercambiar información de enrutamiento entre diferentes redes.
* **IS-IS (Intermediate System to Intermediate System)**: Es un protocolo de enrutamiento de estado de enlace que se utiliza para redes empresariales y proveedores de servicios de Internet. IS-IS utiliza un algoritmo Dijkstra para calcular las rutas más cortas en una red.
* [¿Qué es un protocolo de enrutamiento y cómo funciona? - eClassVirtual - Cursos Cisco en línea](https://eclassvirtual.com/que-es-un-protocolo-de-enrutamiento-y-como-funciona/)

# Protocolo RIP

## ¿Qué es el protocolo RIP

El Protocolo de Información de Encaminamiento/Enrutamiento (**RIP**) es un protocolo de vector distancia que utiliza el conteo de saltos como su métrica principal. RIP define cómo los routers deben compartir información cuando mueven el tráfico entre un grupo interconectado de redes de área local (LAN).

El Protocolo de información de enrutamiento se diseñó originalmente para el Xerox PARC Universal Protocol (PUP) y se llamó GWINFO en el conjunto de protocolos Xerox Network Systems (XNS) en 1981. RIP, que se definió en [RFC 1058](https://tools.ietf.org/html/rfc1058) en 1988, es conocido por ser fácil de configurar y fácil de usar. en pequeñas redes.

## ¿Cómo funciona **RIP?**

RIP utiliza un algoritmo de vector distancia para decidir en qué ruta colocar un paquete para llegar a su destino. Cada router RIP mantiene una tabla de routing, que es una lista de todos los destinos que el router sabe cómo llegar. Cada router transmite su tabla de routing completa a sus vecinos/neighbors más cercanos cada 30 segundos. En este contexto, los vecinos son los otros routers a los que un router está conectado directamente, es decir, los otros routers en los mismos segmentos de red que el router seleccionado. Los vecinos, a su vez, pasan la información a sus vecinos más cercanos, y así sucesivamente, hasta que todos los hosts RIP dentro de la red tengan el mismo conocimiento de las rutas de routing . Este conocimiento compartido se conoce como **convergencia**.

Si un router recibe una actualización en una ruta y la nueva ruta es más corta, actualizará la entrada de la tabla con la longitud y la dirección del siguiente salto de la ruta más corta. Si la nueva ruta es más larga, esperará un período de “*retención*” para ver si las actualizaciones posteriores también reflejan el valor más alto. Solo actualizará la entrada de la tabla si se ha determinado que la nueva ruta más larga es estable.

Si un router falla o se corta una conexión de red, la red descubre esto porque ese router deja de enviar actualizaciones a sus vecinos o deja de enviar y recibir actualizaciones a lo largo de la conexión cortada. Si una ruta determinada en la tabla de routing no se actualiza en seis ciclos de actualización sucesivos (es decir, durante 180 segundos), un router RIP descartará esa ruta y permitirá que el resto de la red conozca el problema a través de sus propias actualizaciones periódicas.

**Versiones de RIP**

Existen tres versiones del Protocolo de información de enrutamiento: **RIPv1**, **RIPv2** y **RIPng**.

RIPv1, estandarizado en 1988, también se denomina **Protocolo de enrutamiento con clase** porque no envía información de máscara de subred en sus actualizaciones de routing. Por otro lado, RIPv2, estandarizado en 1998, se llama **Protocolo de enrutamiento sin clas**e porque envía información de máscara de subred en sus actualizaciones de routing. **RIPng es una extensión de RIPv2** que se creó para admitir IPv6.

En RIPv1, las rutas se deciden en función del destino de IP y el conteo de saltos. RIPv2 avanzó este método y comenzó a incluir máscaras de subred y puertas de enlace. Además, la tabla de routing en RIPv1 se transmite a todas las estaciones de la red conectada, mientras que RIPv2 envía la tabla de routing a una dirección de multidifusión en un esfuerzo por reducir el tráfico de red. Además, **RIPv2 usa autenticación para seguridad**, una característica que falta en RIPv1.

## Configuración de RIP

**RIP opera en la capa de aplicación** del modelo OSI El proceso de configuración para el *Protocolo de información de enrutamiento* es bastante simple. Una vez que se han asignado las direcciones IP a las computadoras e interfaces de los routers involucrados, los desarrolladores pueden emitir el comando **RIP** del router, que le indica al router que habilite el *RIP*, seguido del comando *network*, que permite a los usuarios identificar las redes con las que quieren trabajar. Sólo es necesario especificar las redes directamente asociadas con el router.

Los usuarios también pueden configurar cualquier puerto para realizar las siguientes acciones:

* Evitar que se envíen o reciban paquetes RIP.
* Recibir paquetes en varios formatos.
* Enviar paquetes formateados para cada una de las diferentes versiones de RIP a la dirección de difusión RIPv1.

## cracterísticas de RIP

RIP utiliza un conteo de saltos modificado como una forma de determinar la distancia de la red. *Modificado* refleja el hecho de que los ingenieros de redes pueden asignar rutas de mayor costo. De manera predeterminada, si el vecino de un router posee una red de destino y puede entregar paquetes directamente a la red de destino sin utilizar ningún otro router, esa ruta tiene un salto. En la terminología de gestión de red, esto se describe como un costo de uno.

**RIP permite solo 15 saltos en una ruta**. Si un paquete no puede llegar a un destino en 15 saltos, el destino se considera **inalcanzable**. A las rutas se les puede asignar un costo más alto (como si involucraran saltos adicionales) si la empresa desea limitar o desalentar su uso. Por ejemplo, a un enlace de respaldo satelital se le puede asignar un costo de 10 para obligar al tráfico a seguir otras rutas cuando esté disponible.

# Ventajas y desventajas de RIP

## Las ventajas de RIP incluyen:

* Configuración factible
* Fácil de comprender
* Predominantemente libre de bucles
* Garantizado para admitir casi todos los routers
* Promueve el equilibrio de carga.

## Las desventajas de RIP incluyen:

* No siempre libre de bucles
* Solo se admite el equilibrio de carga de igual costo
* Puede producirse congestión
* Ancho de banda intensivo e ineficiente
* Las grandes redes conducen a una lenta convergencia

Al utilizar RIP, los usuarios pueden encontrarse con varias limitaciones. Por ejemplo, el ***Routing Information Protocol*** aumenta el tráfico de red debido a las comprobaciones y actualizaciones que realiza en los routers vecinos cada 30 segundos. Además, dado que RIP solo actualiza los routers vecinos, las actualizaciones para routers no vecinos pueden olvidarse ya que la información no es accesible de inmediato.

[¿Qué es Routing Information Protocol (RIP) y cómo funciona? » Redes](https://ccnadesdecero.es/routing-information-protocol-rip/#1_Que_es_Protocolo_de_Informacion_de_Encaminamiento)

# Protocolo OSPF

OSPF (Open Shortest Path First) es un protocolo de enrutamiento dinámico que encuentra y reconstruye rutas automáticamente cuando hay cambios en la red. Analiza constantemente el estado de todas las rutas disponibles y utiliza un algoritmo para elegir la mejor. Gracias a esto, **OSPF es particularmente eficaz en redes con mucho tráfico**, donde es necesario transmitir grandes volúmenes de datos sin interrupciones y sin retrasos.

### DIFERENCIA DE LOS OTROS MODELOS

* **RIP está limitado a 15 nodos y envía actualizaciones de ruta cada 30 segundos**. OSPF envía actualizaciones solo cuando hay cambios en la topología, lo que reduce la carga en la red y ahorra recursos.
* **EIGRP es un protocolo propietario de Cisco**, mientras que OSPF es un estándar abierto compatible con la mayoría de los fabricantes de equipos de red. OSPF se puede implementar en equipos de diferentes fabricantes, lo que lo hace más flexible para escalar.

OSPF se puede comparar con un GPS: cuando el enrutador tiene un mapa completo de la red, puede construir fácilmente una ruta a cualquier punto. Esto es eficaz porque la probabilidad de que ocurran errores o bucles en esta situación es mínima. Sin embargo, a medida que aumenta el número de rutas, se necesita más tiempo y recursos para encontrar la ruta óptima, como al trazar una ruta en un GPS: buscar una ruta desde Madrid a Barcelona toma más tiempo que buscar una ruta desde Madrid a Alcalá de Henares.

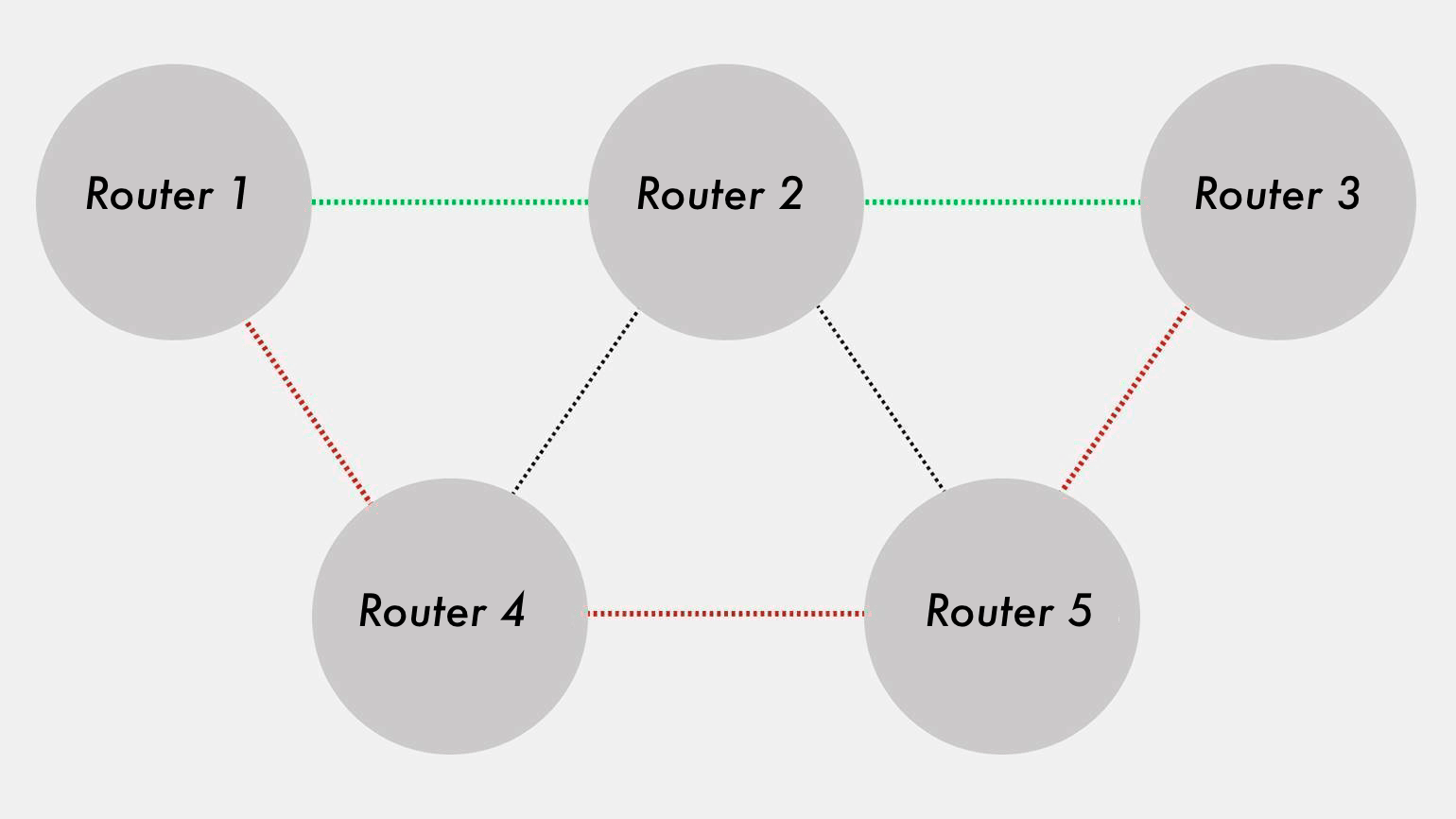
Por lo tanto, **OSPF se utiliza normalmente dentro de la red de una organización y no es adecuado para el enrutamiento en Internet**. Sin embargo, puede conectarse a redes externas a través de enrutadores de borde (ASBR) para intercambiar información entre la red interna y los proveedores externos.

Principio de Funcionamiento de OSPF

Cada enrutador configurado con el protocolo OSPF intercambia información con los dispositivos vecinos sobre las rutas disponibles y su costo (OSPF Cost). El intercambio de datos se lleva a cabo según el principio de “*todos con todos*“. La información recibida se guarda en la base de datos LSDB y, sobre su base, los enrutadores determinan los vecinos y calculan las rutas.

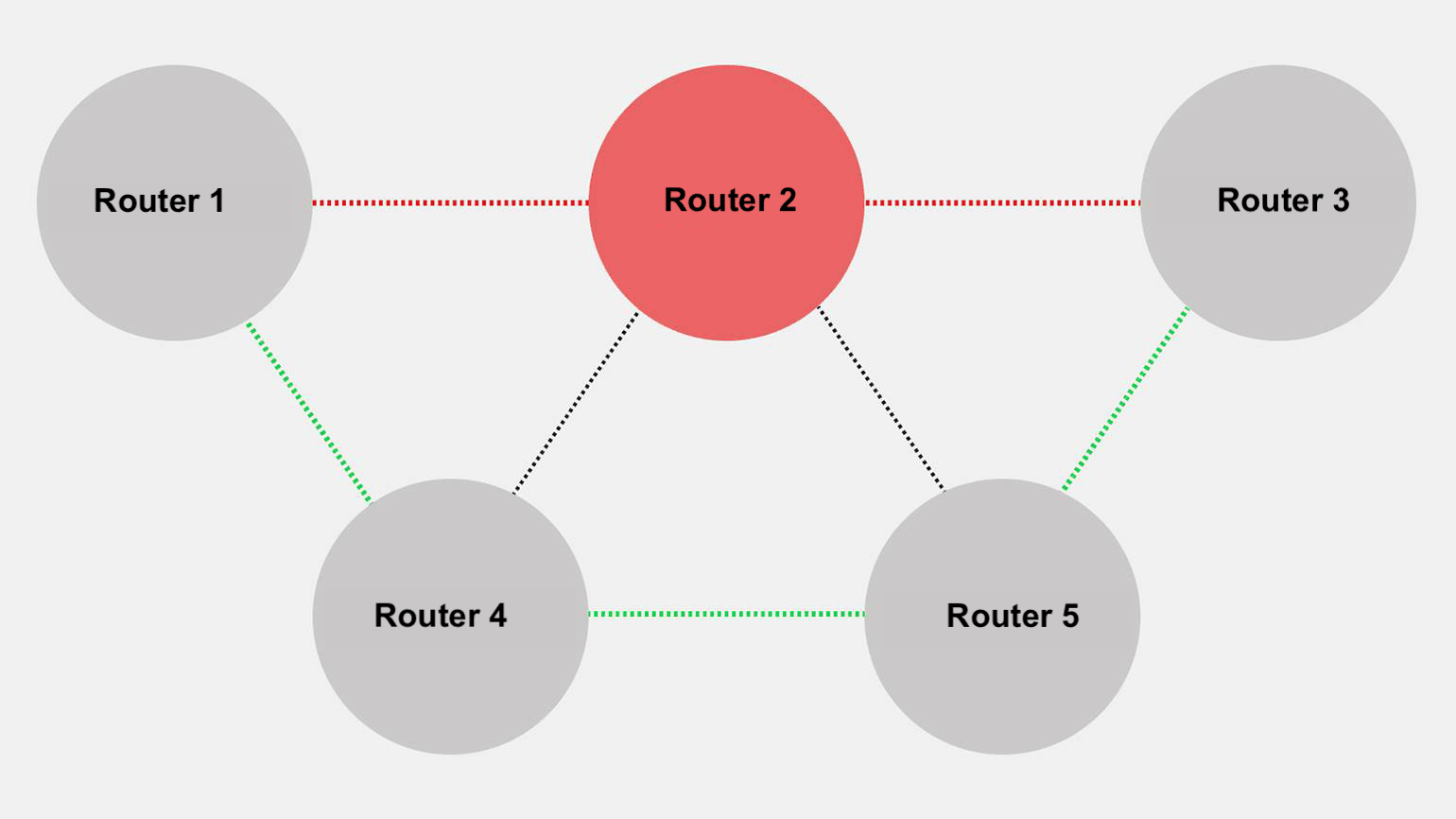
Imagine una red de cinco enrutadores, como en la imagen de abajo. Supongamos que el costo de la transmisión de datos a través de cada interfaz es el mismo. Necesitamos elegir la ruta más rápida para transmitir datos desde el primer enrutador al tercero. La ruta óptima pasará por el segundo enrutador, ya que la participación del cuarto enrutador agregará un nodo adicional y aumentará la demora en la transmisión de datos.

Con el mismo costo de transmisión de datos a través de cada interfaz, la ruta óptima es la que pasa por la menor cantidad de enrutadores entre el remitente y el receptor



Al mismo tiempo, cada enrutador en OSPF elige de forma autónoma una ruta específica, y los mensajes sobre las rutas de red disponibles sirven solo como información de referencia. Por ejemplo, si el segundo enrutador está sobrecargado, el primer enrutador puede enviar datos a través del enrutador 4, en las condiciones actuales, dicha ruta puede resultar óptima.

Con el mismo costo de transmisión de datos a través de cada interfaz, la ruta óptima puede cambiar si uno de los enrutadores está sobrecargado, no está disponible o cambia el ancho de banda de la red



## Tipos de Interfaces

El protocolo OSPF utiliza dos tipos principales de interfaces para intercambiar información con routers vecinos: **Broadcast** y **Point-to-point**.

* **La interfaz OSPF Broadcast**se utiliza en redes de difusión, como Ethernet, donde un router puede intercambiar datos con varios vecinos simultáneamente. Para optimizar el proceso en tales redes, se elige un Router designado (DR). DR recopila información sobre todos los dispositivos en su área de responsabilidad y la reenvía a otros routers, lo que reduce el número de intercambios directos.
* **La interfaz OSPF Point-to-point** se utiliza a menudo en redes WAN para conectar dos routers. El intercambio de datos en esta interfaz se lleva a cabo sin DR, lo que simplifica el proceso y reduce el volumen de mensajes.

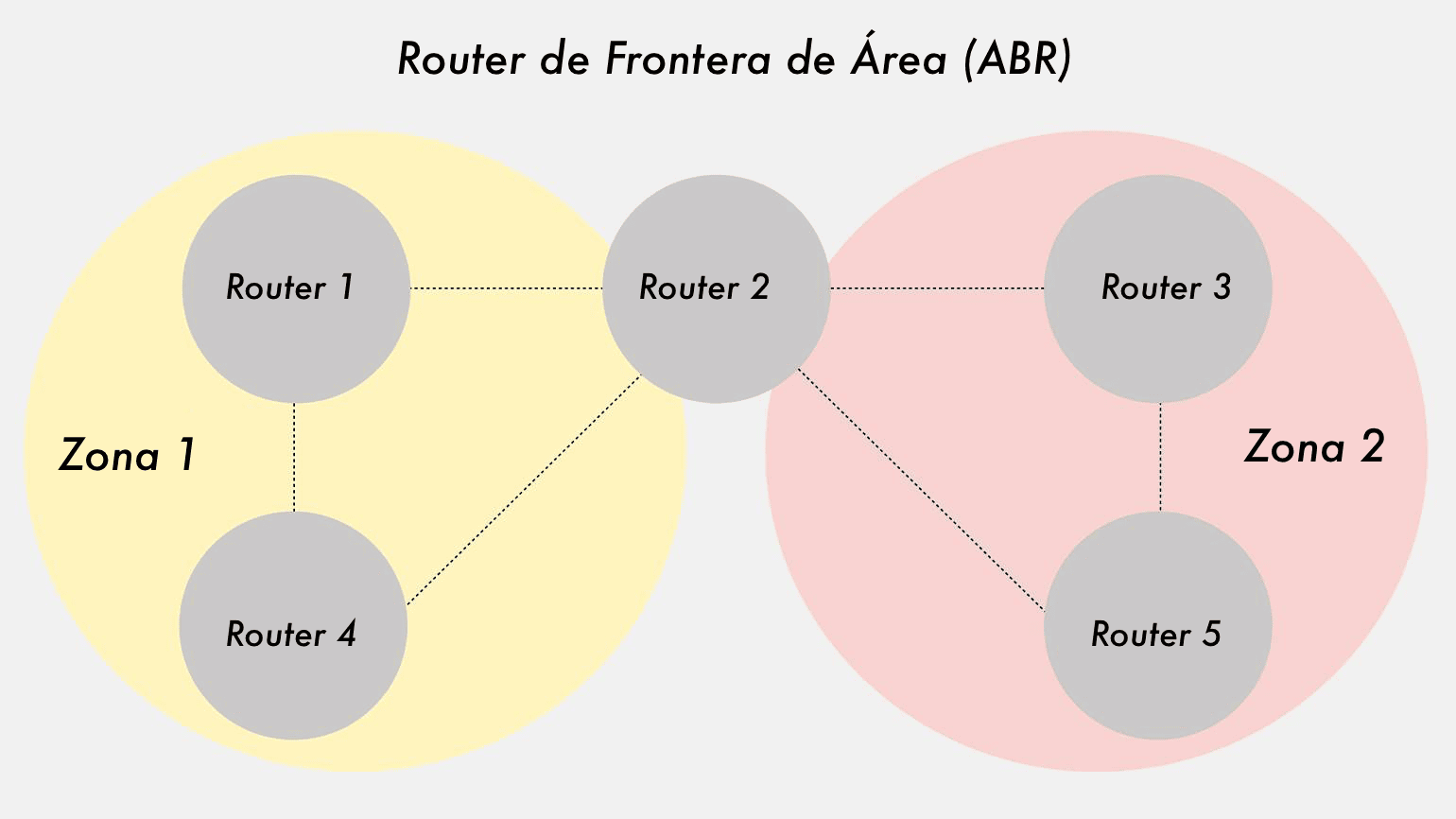
La combinación de diferentes tipos de interfaces proporciona un enrutamiento y una gestión de red confiables. En las redes de difusión, Broadcast ayuda a reducir el volumen de tráfico, y la interfaz Point-to-Point proporciona una comunicación simple y eficaz entre dos dispositivos.

### **Zonas OSPF**

A medida que la red crece, aumenta el número de dispositivos configurados con el protocolo OSPF. Como resultado, la base de datos del estado de las interfaces (LSDB) se amplía y ocupa más espacio, aumenta el número de rutas de red disponibles y el algoritmo para encontrar la ruta más corta se complica. En estas redes, incluso la desconexión temporal de un router provoca una mayor carga en el equipo.

Para solucionar este problema, OSPF utiliza la división de la red en zonas (áreas). Esto reduce la frecuencia de actualización de la base de datos del estado de las interfaces y mejora el rendimiento de la red. Cada interfaz de un router puede pertenecer solo a una zona, y los routers de frontera de zona (ABR – area border routers) son responsables del intercambio de datos entre las zonas.

Anteriormente, cuando el rendimiento de los routers era limitado, existía la regla de incluir no más de 50 dispositivos en una zona para minimizar la carga en la red. Hoy en día, una zona puede incluir miles de routers, por lo que el zonificado se utiliza más para facilitar la gestión que para resolver problemas de escalabilidad.



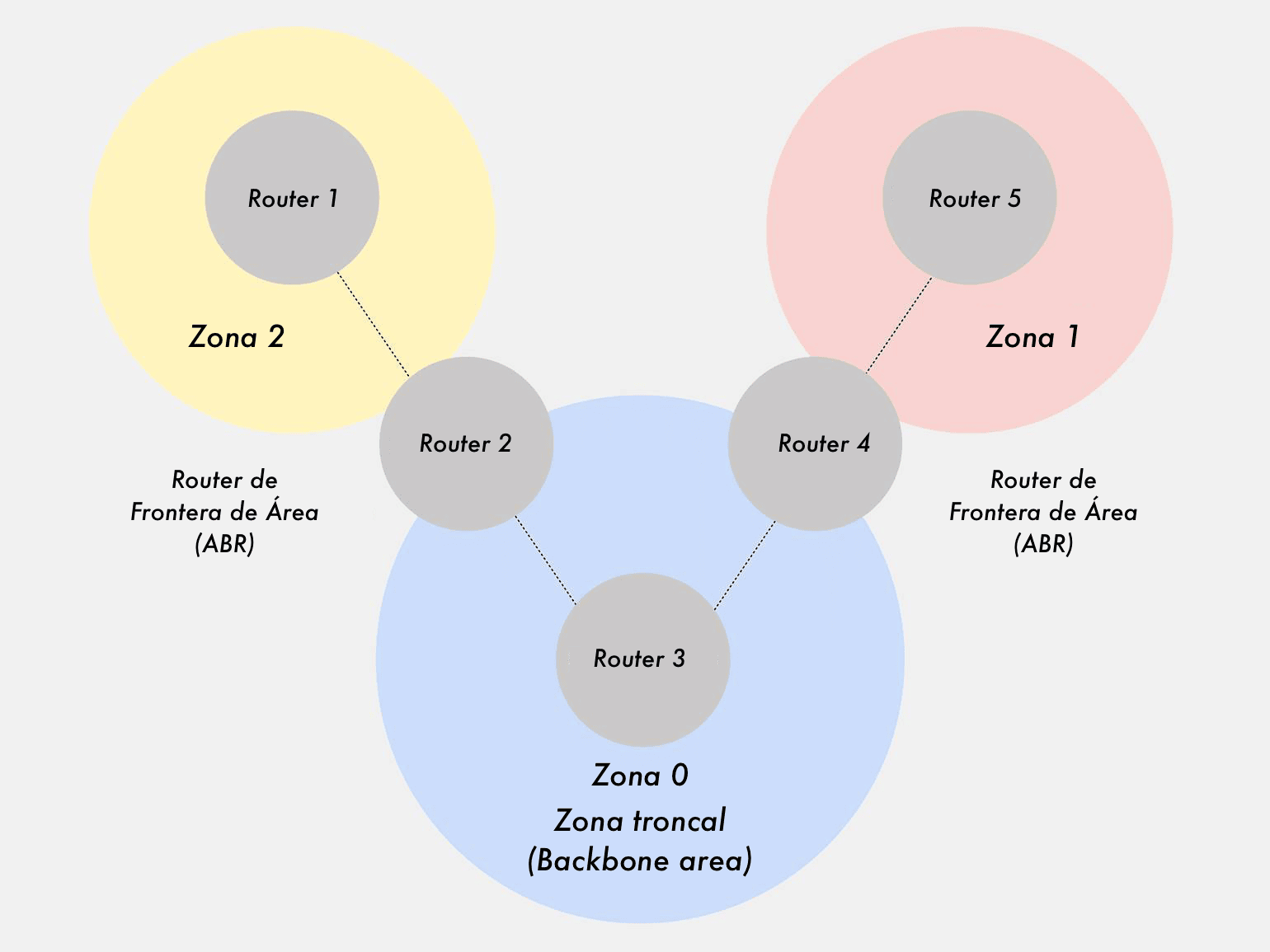
### Diagrama Router de Frontera de Área (ABR)

La zona más importante en OSPF es Backbone area, también conocida como zona troncal o zona 0. Conecta todas las demás zonas de la red OSPF. Toda la información de enrutamiento se transmite a través de Backbone area, lo que garantiza un enrutamiento centralizado sin bucles de red.

Además de Backbone area, existen otros tipos de zonas en OSPF:

* **Standard area:** estas zonas intercambian información de enrutamiento completa tanto dentro de la zona como a través de Backbone Area.
* **Stub area:** estas zonas limitan la cantidad de información sobre las rutas externas, lo que reduce la carga en los routers.
* **Totally stubby area:** es una versión más estricta de Stub Area, que además filtra las rutas, lo que reduce aún más la cantidad de información transmitida.
* **NSSA (Not-so-stubby area):** es una zona híbrida que puede aceptar rutas externas limitadas, lo que la hace más flexible al construir la red.

Imagina una red con tres zonas: zona 0, zona 1 y zona 2. Para transmitir datos de la zona 1 a la zona 2, deben pasar a través de la zona 0 (Backbone area) y viceversa. Incluso si un router tiene interfaces que pertenecen a las zonas 1 y 2, la transmisión directa de datos es imposible, los datos siempre pasarán a través de Backbone.

Ilustración de zonas OSPF

# Tipos de Paquetes

En OSPF hay cinco tipos de paquetes, cada uno de los cuales juega un papel específico en la transmisión y actualización de los datos. Anteriormente nos familiarizamos con los paquetes **Hello**, que son necesarios para establecer y mantener la comunicación entre los routers. Ahora veremos el resto.

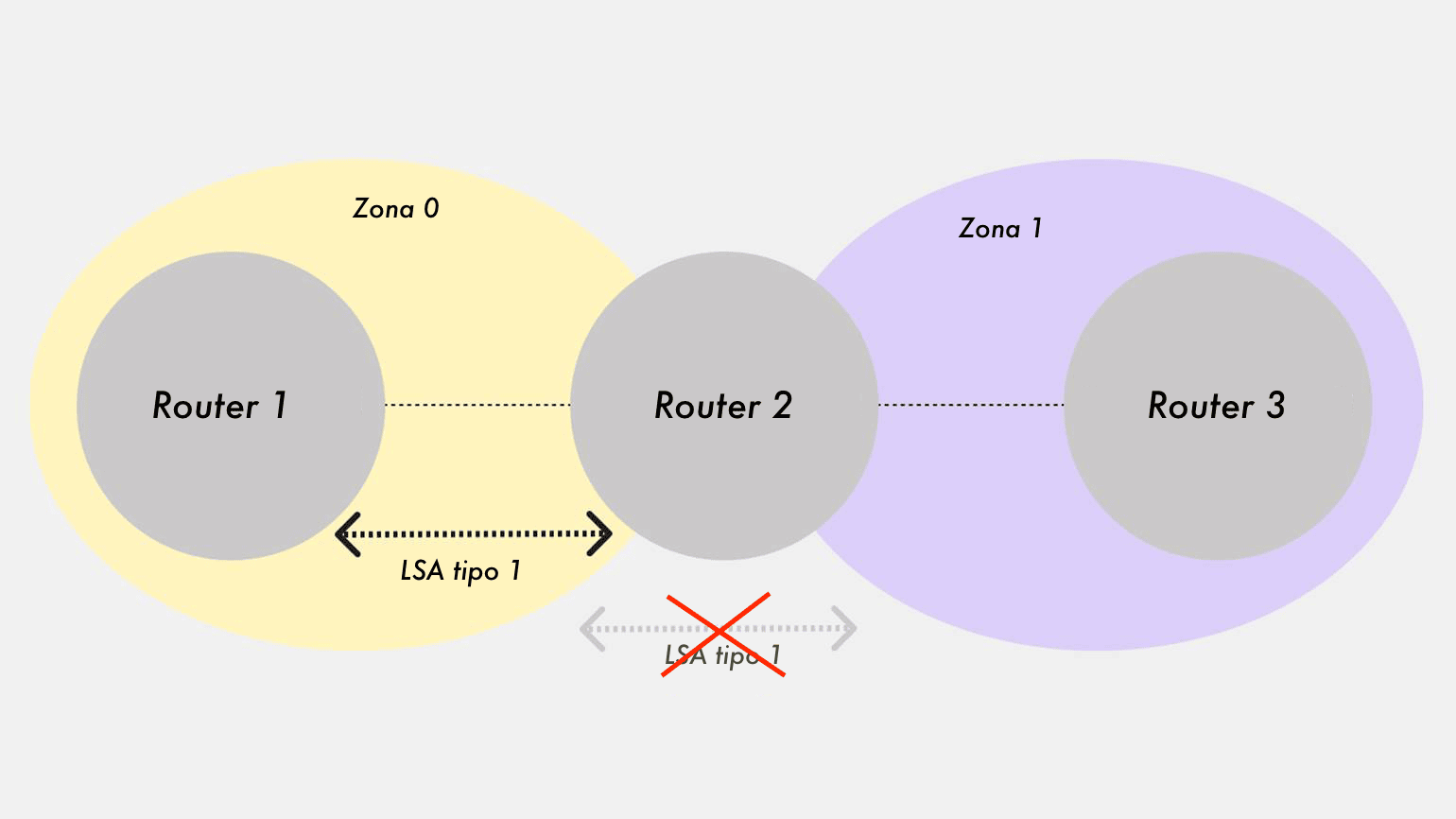
**Database description packet:** paquete de descripción de la base de datos. Al establecer la vecindad, los routers comienzan a intercambiar paquetes *Database description*. Estos paquetes contienen información sobre la topología que se almacena en la base de datos de los routers. En las redes grandes, puede ser necesario utilizar varios paquetes para transmitir la topología. En este caso, el proceso se organiza según el esquema “pregunta-respuesta”: un router se convierte en maestro y el otro en esclavo. El router esclavo transmite paquetes después de recibir datos del maestro.

**Link state request packet:** paquete de solicitud de estado de interfaz. Si la base de datos de un router está desactualizada, puede solicitar actualizaciones a los routers vecinos. Para ello, se utiliza el paquete Link State Request, que permite al router obtener solo los datos que faltan o están desactualizados en su propia base de datos.

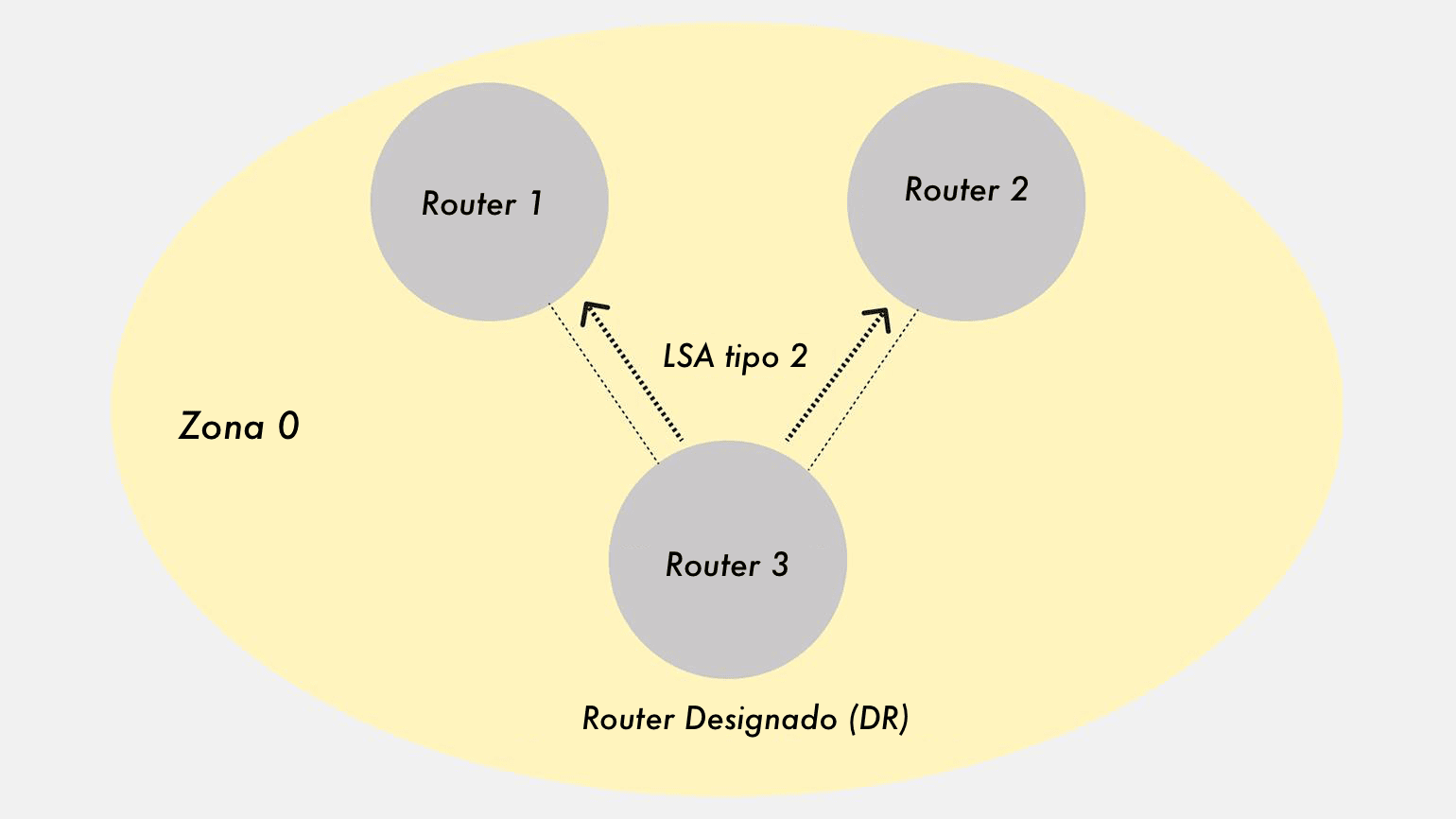
**Link state update packet (LSU):** paquete de actualización de estado de interfaz. Este paquete contiene mensajes LSA que los routers utilizan para mantener la actualidad de los datos en la base, transmitiendo cambios en la topología de la red y actualizando las rutas.

**Link state acknowledge packet (LSAck):** paquete de confirmación de estado de interfaz. Cuando un router recibe un paquete con una actualización, envía LSAck para confirmar la recepción de los datos. Esto garantiza la entrega de la información y previene la pérdida de paquetes.

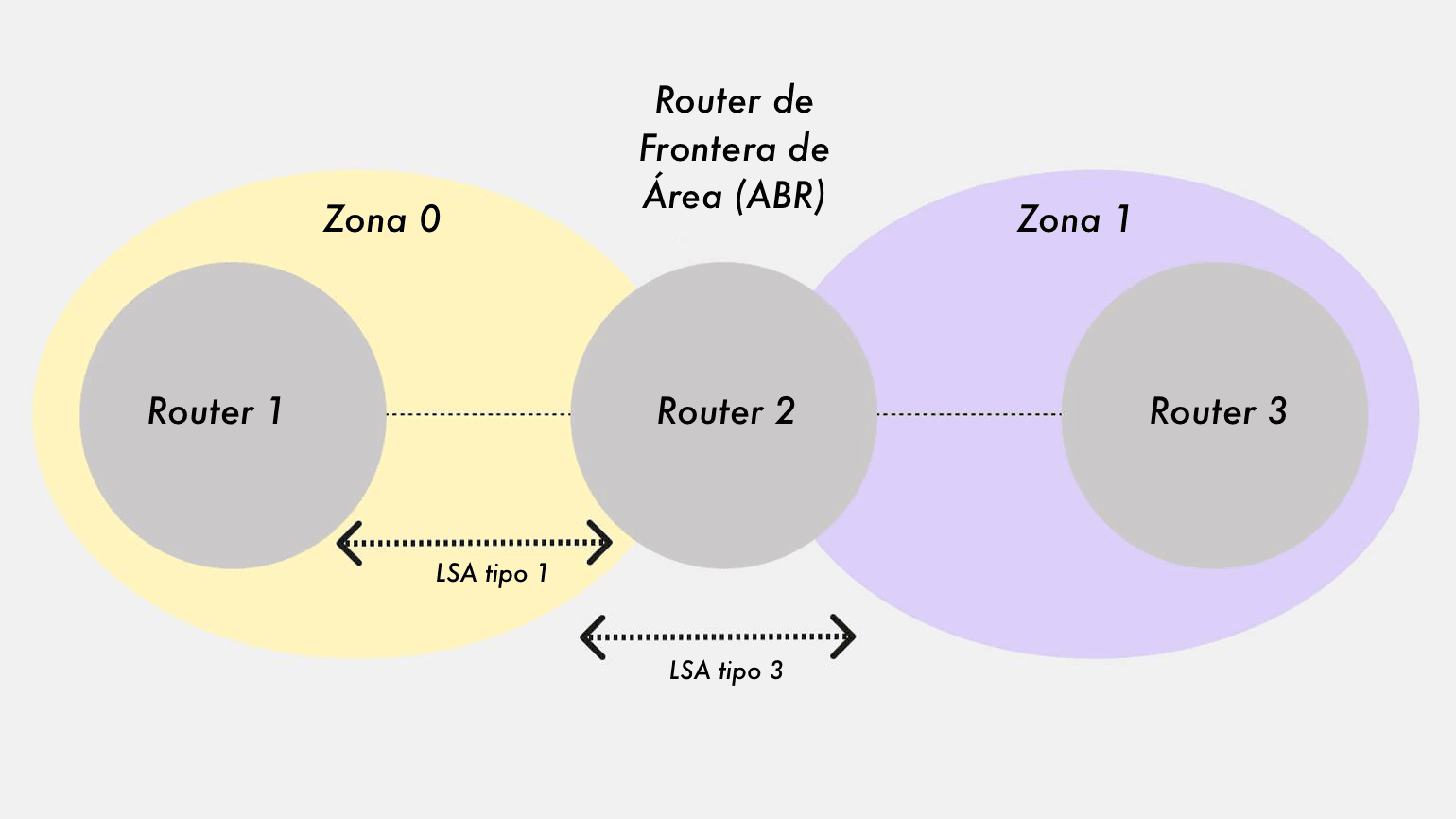
**LSA tipo 1: Router LSA – Anuncio de router.** Cada router genera paquetes LSA tipo 1 que contienen información sobre el estado de sus interfaces. Estas LSA se distribuyen solo dentro de su zona y no salen de ella. Los paquetes incluyen el identificador del router, el estado de las interfaces y la dirección IP. Por ejemplo, si un router detecta que una de sus interfaces está desactivada, creará un LSA tipo 1 para notificar a los demás dispositivos de la zona sobre el cambio.

Ilustración de LSA tipo 1

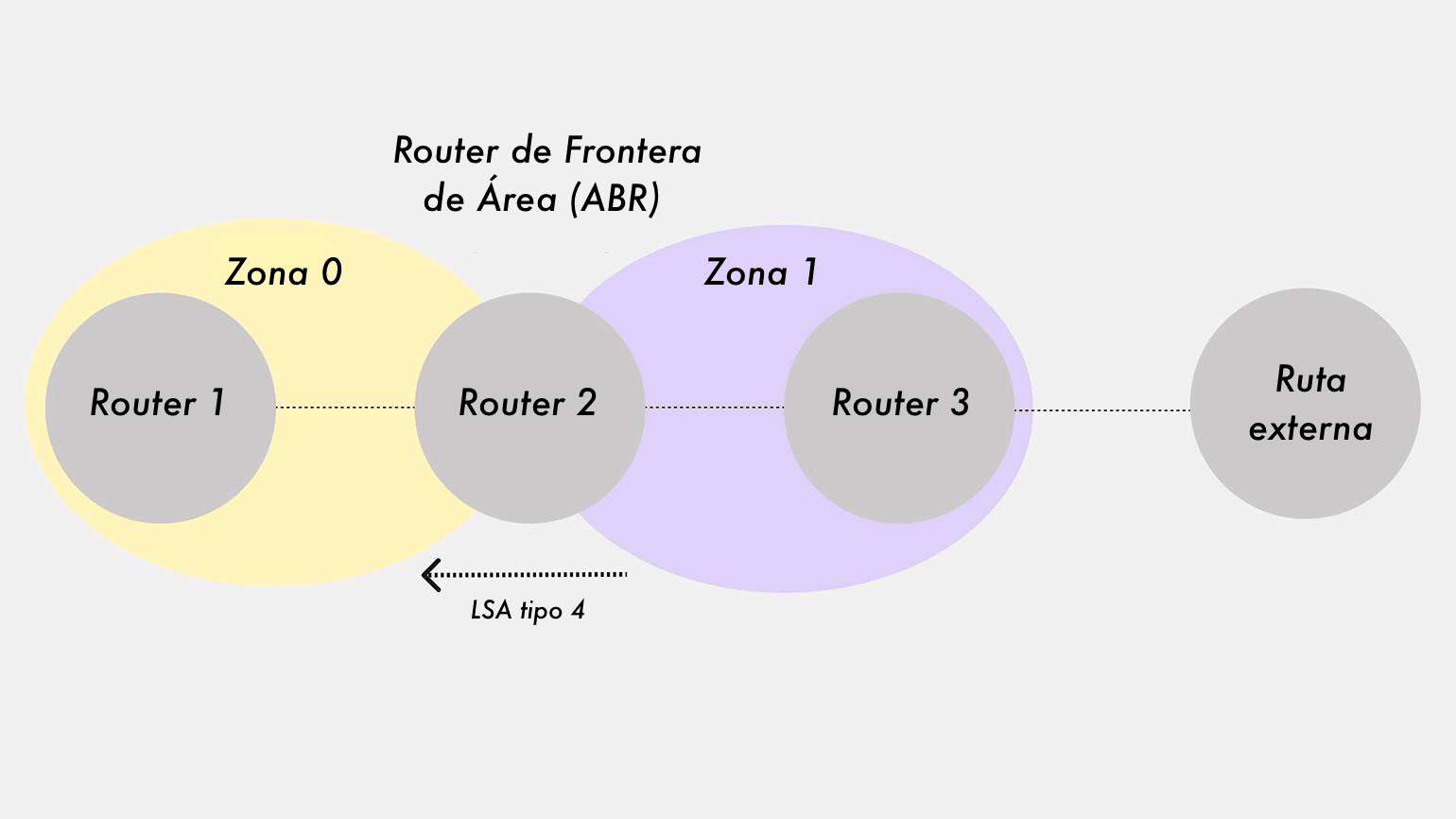
**LSA tipo 2: Network LSA – Anuncio de red.** DR crea Network LSA y la distribuye entre todos los routers de la zona. Contiene información sobre todos los routers de la subred, así como datos sobre DR y BDR. Al igual que LSA tipo 1, este tipo no sale de la zona. Por ejemplo, si hay varios routers en una red local, Network LSA transmitirá información sobre qué routers están conectados a DR y BDR, para que todos los dispositivos conozcan el estado actualizado de la red.

Ilustración de LSA tipo 2

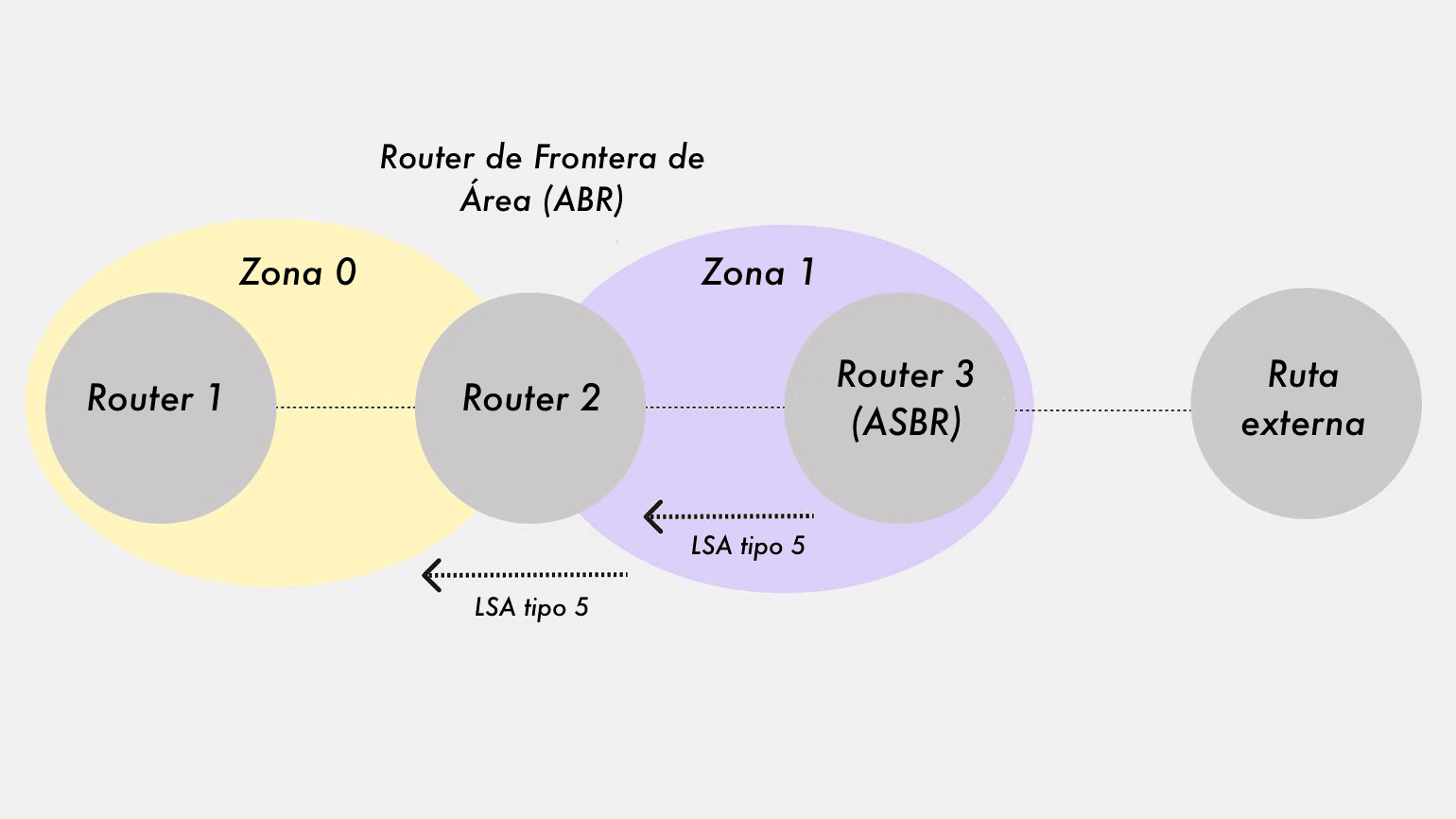
**LSA tipo 3: Summary LSA – Anuncio resumido de rutas entre zonas.** Este tipo de mensaje es creado por un Router de frontera (ABR) y anuncia rutas para otras zonas. Si un router de la zona 0 necesita transmitir datos a la zona 1, ABR creará un Summary LSA con la ruta a la zona 1 y lo transmitirá a la zona 0. Después de esto, el router de la zona 0 sabrá cómo llegar a los dispositivos de la zona 1.

Ilustración de LSA tipo 3

**LSA tipo 4: Summary ASBR LSA – Anuncio resumido de la ruta más allá de OSPF.** Este tipo de LSA lo genera un router de frontera si hay una ruta externa en una de las zonas. Summary ASBR LSA informa la ruta al router que gestiona esta ruta externa. Por ejemplo, si un router de la zona 0 gestiona la conexión a Internet, ABR creará un LSA tipo 4 y lo transmitirá a otras zonas para que conozcan la ruta a este router para transmitir datos más allá de OSPF.

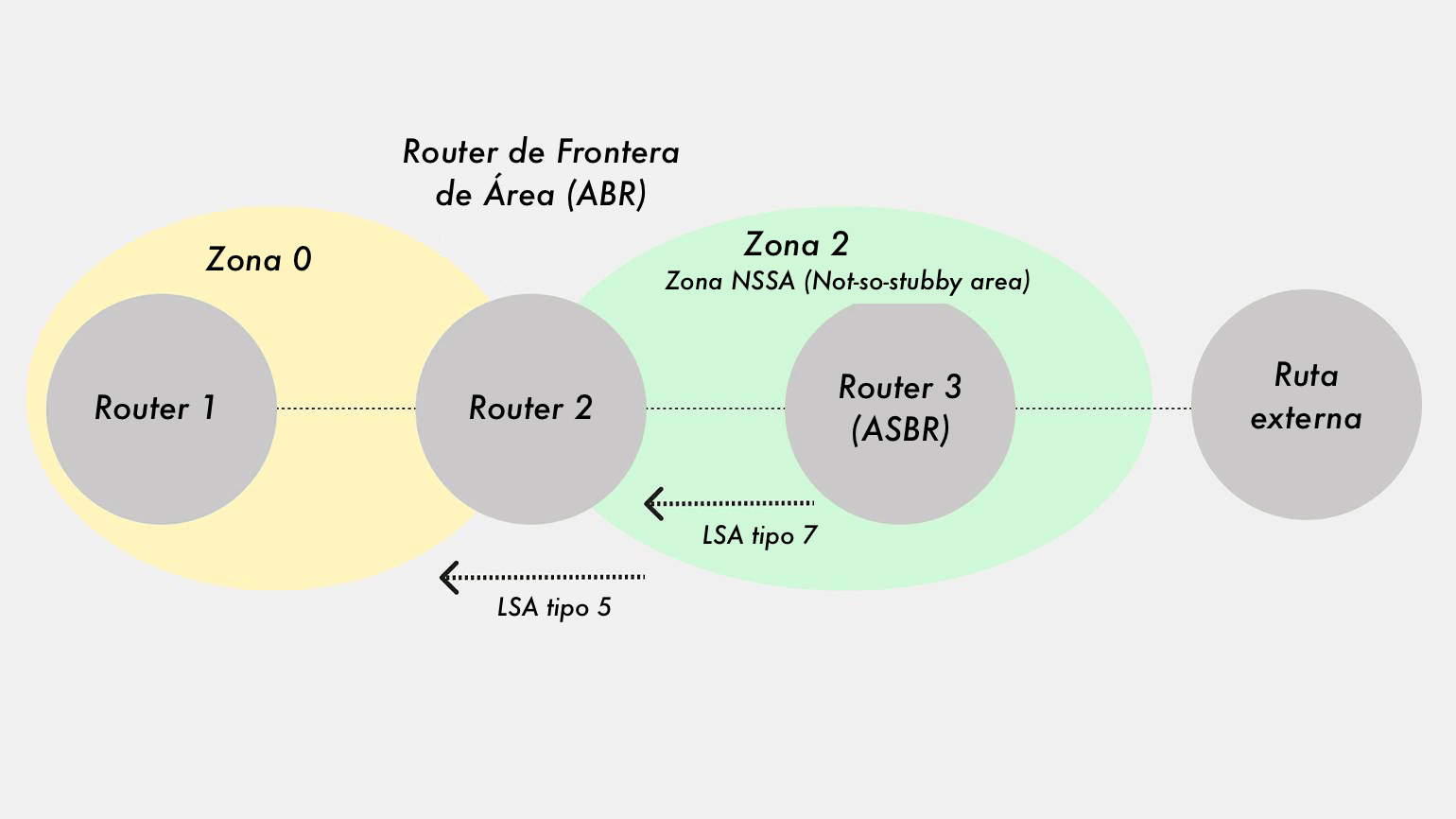
Ilustración de LSA tipo 4

**LSA tipo 5: Autonomous system external LSA – Anuncio de la presencia de una ruta más allá de OSPF.** Estos anuncios los generan los routers de frontera del sistema autónomo (ASBR), que están conectados a redes externas. Autonomous system external LSA se transmite a todas las zonas, excepto a Stub, Totally stubby y NSSA. Si un router de la zona 0 está conectado a Internet y recibe rutas del proveedor, generará un LSA tipo 5. Luego, este mensaje se transmite a otras zonas para que los routers conozcan la ruta a la ruta externa de Internet.

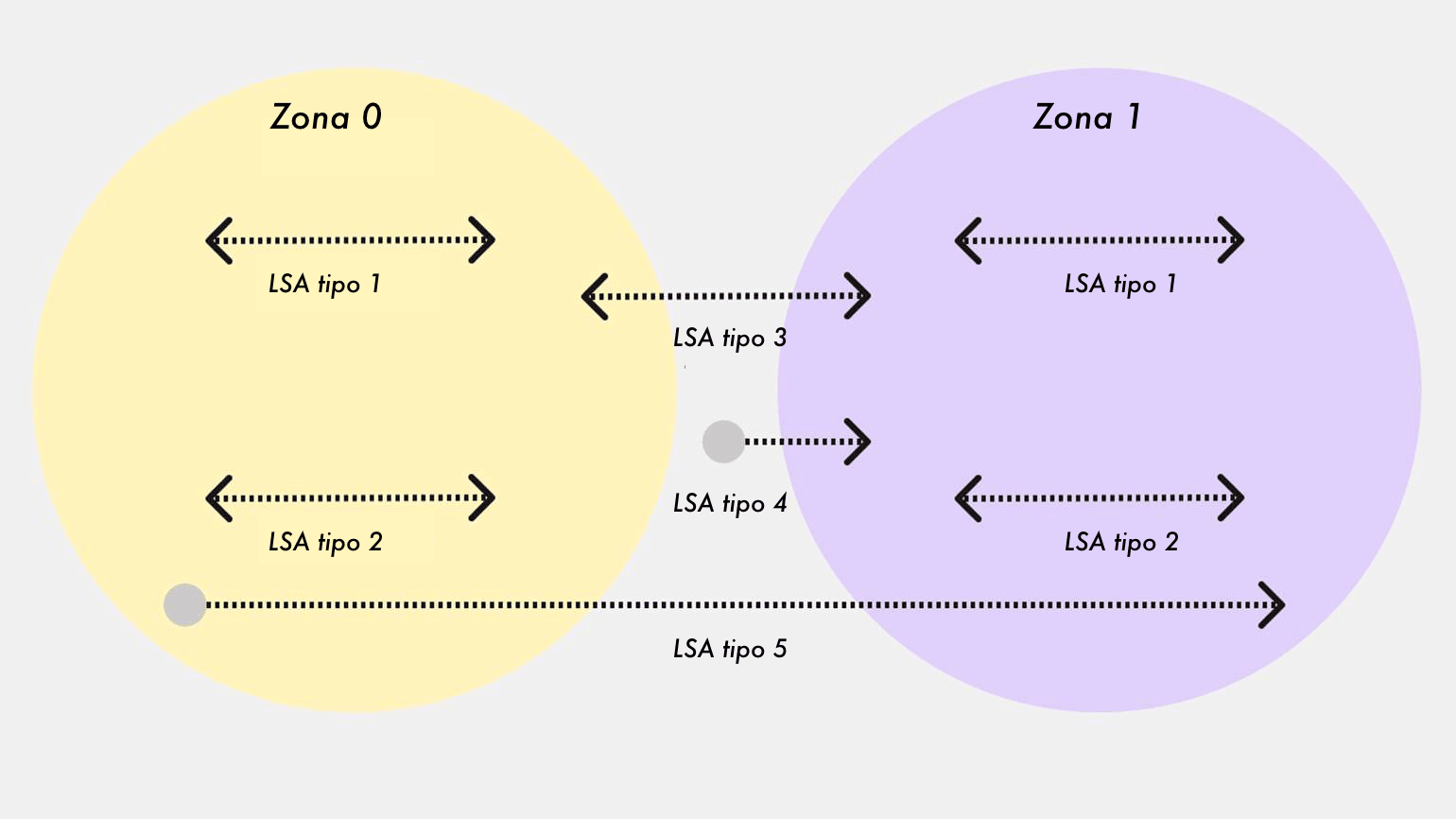
Ilustración de LSA tipo 5

**LSA tipo 6: Multicast OSPF LSA:** es un anuncio de multidifusión utilizado en OSPFv3. La multidifusión es una forma de transmitir datos simultáneamente a varios destinatarios de un grupo sin enviar copias a cada uno. Si los routers transmiten una transmisión de video a un grupo de multidifusión, utilizan una dirección de multidifusión para enviar datos a todos los participantes. LSA tipo 6 permite a los routers sincronizar rutas de multidifusión e intercambiar información sobre ellas.

**LSA tipo 7: NSSA external LSA:** es un anuncio de ruta desde fuera de OSPF en una zona NSSA. Este tipo de LSA se utiliza en zonas especializadas donde no está permitido el uso de LSA tipo 5 para distribuir rutas externas. Por ejemplo, una empresa puede tener una sucursal que está conectada a Internet a través de su propio router, que se encuentra en una zona NSSA. Para transmitir información sobre rutas externas de la sucursal a la red principal, se crea un LSA tipo 7. Cuando esta ruta sale de la zona NSSA y se transmite a otras zonas, se convierte en LSA tipo 5, lo que permite a los routers utilizar correctamente esta ruta externa.

Ilustración de LSA tipo 7

Los anuncios LSA garantizan el funcionamiento sin problemas del protocolo OSPF, permitiendo a los routers obtener información actualizada sobre las rutas y adaptarse rápidamente a los cambios en la red.

Interacción de los principales tipos de mensajes LSA en OSPF

[OSPF: Guía Completa para Principiantes en Redes » Blog Redes](https://ccnadesdecero.es/ospf-open-shortest-path-first/#Fundamentos_del_Protocolo_OSPF)

# Protocolo EIGRP

## Características Básicas

### ¿Qué es EIGRP?

El protocolo de routing de gateway interior mejorado (EIGRP – Enhanced Interior Gateway Routing Protocol) es un protocolo de routing vector distancia avanzado desarrollado por Cisco Systems. Como lo sugiere el nombre, **EIGRP es una mejora de otro protocolo de routing de Cisco**: el protocolo de routing de gateway interior (**IGRP**).

IGRP es un protocolo de routing vector distancia con clase anterior, que quedó obsoleto a partir del IOS 12.3.

EIGRP incluye características propias de los protocolos de routing de estado de enlace. EIGRP es apto para numerosas topologías y medios diferentes. En una red bien diseñada, EIGRP puede escalar para incluir varias topologías y puede proporcionar tiempos de convergencia extremadamente rápidos con un mínimo tráfico de red.

EIGRP se lanzó originalmente en 1992 como un protocolo exclusivo disponible solamente en los dispositivos de Cisco. En 2013, Cisco cedió una funcionalidad básica de EIGRP como estándar abierto al IETF, como una RFC informativa.

Esto significa que otros proveedores de redes ahora pueden implementar EIGRP en sus equipos para que interoperen con routers que ejecuten EIGRP, ya sean de Cisco o de otros fabricantes.

### Características de EIGRP

EIGRP se basa en el principio clave del protocolo de routing vector distancia, según el cual la información acerca del resto de la red se obtiene a partir de vecinos conectados directamente.

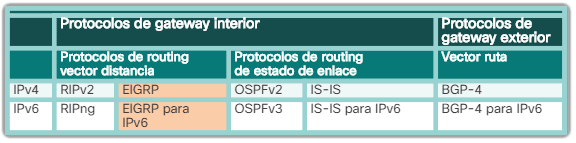
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/Tipos-de-protocolos-de-routing.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/Tipos-de-protocolos-de-routing.png)

Imagen Tipos de protocolos de routing

* **Algoritmo de actualización difusa**

El algoritmo de actualización por difusión (DUAL), constituye el centro del protocolo de routing. DUAL garantiza rutas de respaldo y sin bucles en todo el dominio de routing.

Al usar DUAL, EIGRP almacena todas las rutas de respaldo disponibles a los destinos, de manera que se puede adaptar rápidamente a rutas alternativas si es necesario.

* **Establecimiento de adyacencias de vecinos**

EIGRP establece relaciones con routers conectados directamente que también están habilitados para EIGRP. Las adyacencias de vecinos se usan para rastrear el estado de esos vecinos.

* **Protocolo de transporte confiable**

El protocolo de transporte confiable (RTP) es exclusivo de EIGRP y se encarga de la entrega de los paquetes EIGRP a los vecinos.

* **Actualizaciones parciales y limitadas**

En lo que respecta a sus actualizaciones, en EIGRP se utilizan los términos “parcial” y “limitada”. **A diferencia de RIP, EIGRP no envía actualizaciones periódicas, y las entradas de ruta no vencen.**

El término “parcial” significa que la actualización solo incluye información acerca de cambios de ruta, como un nuevo enlace o un enlace que deja de estar disponible.

El término “limitada” se refiere a la propagación de las actualizaciones parciales que se envían solo a aquellos routers que se ven afectados por el cambio.

* **Balanceo de carga de mismo costo o con distinto costo**

EIGRP admite balanceo de carga de mismo costo y balanceo de carga con distinto costo, lo que permite a los administradores distribuir mejor el flujo de tráfico en sus redes.

2.1. Módulos dependientes de protocolo

EIGRP tiene la capacidad para enrutar varios protocolos diferentes, incluidos IPv4 e IPv6, mediante el uso de módulos dependientes de protocolo (PDM).

Los PDM son responsables de tareas específicas de los protocolos de capa de red. Un ejemplo de esto es el módulo de EIGRP, que es responsable de enviar y recibir paquetes EIGRP encapsulados en IPv4.

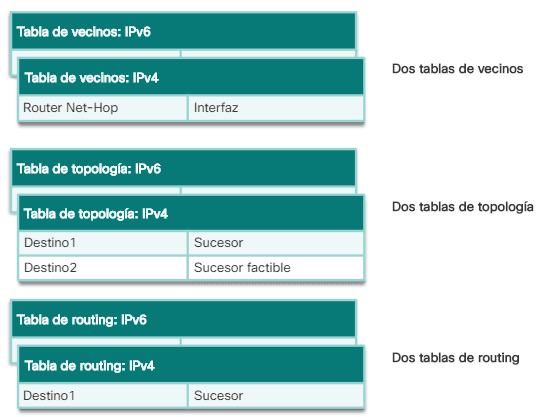
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/EIGRP-con-m%C3%B3dulos-dependientes-de-protocolo-PDM-1.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/EIGRP-con-m%C3%B3dulos-dependientes-de-protocolo-PDM-1.png)

Imagen EIGRP con módulos dependientes de protocolo (PDM)

Este módulo también es responsable de analizar los paquetes EIGRP y de informar a DUAL la nueva información recibida. EIGRP pide a DUAL que tome decisiones de routing, pero los resultados se almacenan en la tabla de routing IPv4.

Los PDM son responsables de las tareas específicas de routing de cada protocolo de capa de red, incluido lo siguiente:

* Mantener las tablas de vecinos y de topología de los routers EIGRP que pertenecen a esa suite de protocolos.
* Construir y traducir paquetes específicos del protocolo para DUAL.
* Conectar a DUAL con la tabla de routing específica del protocolo.
* Calcular la métrica y pasar esa información a DUAL.
* Implementar listas de filtrado y de acceso.
* Realizar funciones de redistribución hacia otros protocolos de routing y desde ellos.
* Redistribuir rutas descubiertas por otros protocolos de routing.

### Protocolo de transporte confiable

EIGRP utiliza el protocolo de transporte confiable (RTP) para la entrega y recepción de paquetes EIGRP.

**EIGRP se diseñó como un protocolo de routing independiente de capa de red** y; debido a este diseño, no puede usar los servicios de UDP o TCP. Esto permite que EIGRP se utilice para protocolos distintos de aquellos de la suite de protocolos TCP/IP, como **IPX y Apple Talk**. En la ilustración se muestra conceptualmente cómo opera RTP.

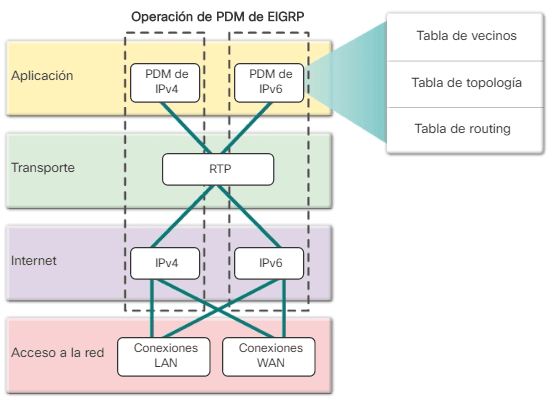
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/C%C3%B3mo-funciona-RTP.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/C%C3%B3mo-funciona-RTP.png)

Imagen EIGRP reemplaza a TCP con RTP

Si bien el término “confiable” forma parte de su nombre, RTP incluye entrega confiable y entrega poco confiable de los paquetes EIGRP, de manera similar a TCP y UDP respectivamente.

RTP confiable requiere que el receptor envíe un acuse de recibo al emisor. Los paquetes RTP poco confiables no requieren acuse de recibo.

RTP puede enviar paquetes EIGRP como unidifusión o multidifusión.

* Los paquetes de multidifusión EIGRP para IPv4 utilizan la dirección IPv4 de multidifusión reservada 224.0.0.10.
* Los paquetes de multidifusión EIGRP para IPv6 se envían a la dirección IPv6 de multidifusión reservada FF02::A.

## Autenticación

Al igual que otros protocolos de routing, EIGRP puede configurarse para autenticación. RIPv2, EIGRP, OSPF, IS-IS y BGP pueden configurarse para autenticar la información de routing.

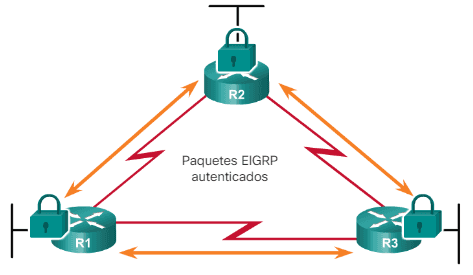
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/Autenticaci%C3%B3n-EIGRP.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/Autenticaci%C3%B3n-EIGRP.png)

Imagen Autenticación

Tipos de paquetes EIGRP

EIGRP utiliza **cinco tipos de paquetes distintos**, algunos en pares. Los tipos de paquetes EIGRP también reciben el nombre de “formatos de paquetes EIGRP” o “mensajes EIGRP”.

### Los cinco tipos de paquetes EIGRP incluyen:

* **Paquetes de saludo**: se utilizan para descubrir a los vecinos y para mantener las adyacencias de vecinos.
* **Paquetes de actualización**: propagan información de routing a vecinos EIGRP.
* **Paquetes de acuse de recibo**: se utilizan para acusar recibo de un mensaje EIGRP que se envió con entrega confiable.
* **Paquetes de consulta**: se utilizan para consultar rutas de vecinos.
* **Paquetes de respuesta**: se envían en respuesta a consultas EIGRP.

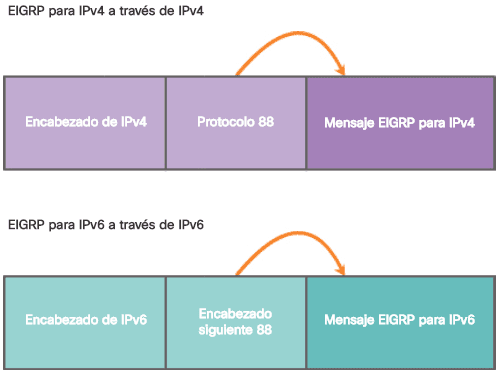
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/Encapsulaci%C3%B3n-de-paquetes-EIGRP.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/Encapsulaci%C3%B3n-de-paquetes-EIGRP.png)

Imagen Los mensajes EIGRP se envían a través de IP

Los mensajes EIGRP para IPv4 usan IPv4 como el protocolo de capa de red. El campo de protocolo IPv4 usa 88 para indicar que la porción de datos del paquete es un mensaje EIGRP para IPv4.

Los mensajes EIGRP para IPv6 se encapsulan en paquetes IPv6 que utilizan el campo de encabezado siguiente 88. Al igual que el campo de protocolo para IPv4, el campo de encabezado siguiente de IPv6 indica el tipo de datos transportados en el paquete IPv6.

## Paquetes de saludo EIGRP

EIGRP utiliza pequeños paquetes de saludo para descubrir otros routers con EIGRP habilitado en enlaces conectados directamente. Los routers utilizan los paquetes de saludo para formar adyacencias de vecinos EIGRP, también conocidas como “relaciones de vecinos”.

Los paquetes de saludo EIGRP se envían como transmisiones IPv4 o IPv6 de multidifusión y utilizan entrega RTP poco confiable. Esto significa que el receptor no responde con un paquete de acuse de recibo.

* La dirección de multidifusión EIGRP reservada para IPv4 es 224.0.0.10.
* La dirección de multidifusión EIGRP reservada para IPv6 es FF02::A.

En la mayoría de las redes, los paquetes de saludo EIGRP se envían como paquetes de multidifusión cada cinco segundos. Sin embargo, en redes multipunto multiacceso sin difusión (NBMA), como X.25, Frame Relay, e interfaces de modo de transferencia asíncrona (ATM) con enlaces de acceso de T1 (1,544 Mb/s) o más lentos, los paquetes de saludo se envían como paquetes de unidifusión cada 60 segundos.

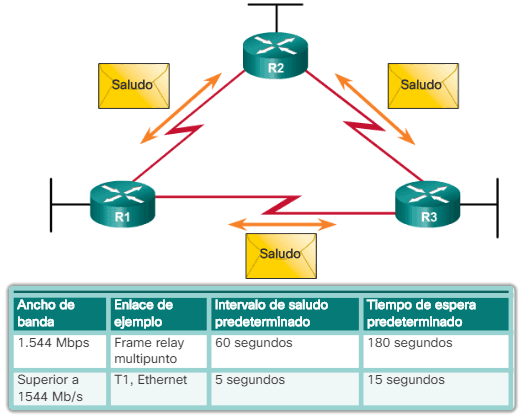
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/Paquetes-de-saludo-EIGRP.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/Paquetes-de-saludo-EIGRP.png)

Imagen  Intervalos de saludo y tiempos de espera predeterminados para EIGRP

## Paquetes de actualización EIGRP

EIGRP envía paquetes de actualización para propagar información de routing. Los paquetes de actualización se envían sólo cuando es necesario.

A diferencia de RIP, EIGRP (otro protocolo de routing vector distancia) no envía actualizaciones periódicas, y las entradas de ruta no vencen.

En cambio, EIGRP envía actualizaciones incrementales solo cuando se modifica el estado de un destino. Esto puede incluir cuando una nueva red está disponible, cuando una red existente deja de estar disponible, o cuando ocurre un cambio en la métrica de routing de una red existente.

En lo que respecta a sus actualizaciones, en EIGRP se utilizan los términos parcial y limitada. El término parcial significa que la actualización sólo envía información acerca de los cambios de ruta. El término “limitada” se refiere a la propagación de las actualizaciones parciales que se envían solo a aquellos routers que se ven afectados por el cambio.

Al enviar solo la información de routing necesaria únicamente a los routers que la necesitan, EIGRP minimiza el ancho de banda que se requiere para enviar actualizaciones EIGRP.

**Los paquetes de actualización EIGRP usan entrega confiable**, lo que significa que el router emisor requiere un acuse de recibo. **Los paquetes de actualización se envían como multicast** cuando son requeridos por múltiples routers, o como unicast cuando son requeridos por sólo un router.

En la Imagen 7, debido a que los enlaces son punto a punto, las actualizaciones se envían como unicast.

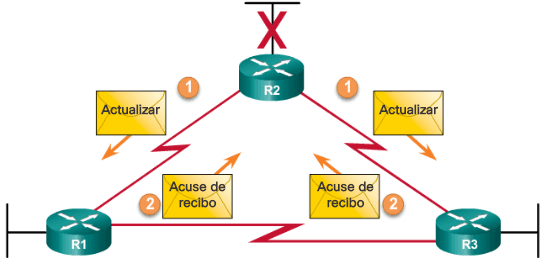
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/Mensajes-EIGRP-de-actualizaci%C3%B3n-y-de-acuse-de-recibo.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/Mensajes-EIGRP-de-actualizaci%C3%B3n-y-de-acuse-de-recibo.png)

Imagen Mensajes EIGRP de actualización y de acuse de recibo

## Paquetes de acuse de recibo EIGRP

EIGRP envía paquetes de acuse de recibo (ACK) cuando se usa el método de entrega confiable. Un acuse de recibo EIGRP es un paquete de saludo EIGRP sin ningún dato.

**RTP utiliza una entrega confiable para los paquetes EIGRP de actualización, consulta y respuesta**. Los paquetes de acuse de recibo EIGRP se envían siempre como transmisiones de unidifusión poco confiables. El sentido de la entrega poco confiable es que, de otra manera, habría un bucle interminable de acuses de recibo.

En la Imagen 7, el R2 perdió la conectividad a la LAN conectada a su interfaz Gigabit Ethernet. El R2 envía inmediatamente una actualización al R1 y al R3, donde se señala la ruta fuera de servicio. El R1 y el R3 responden con un acuse de recibo para que el R2 sepa que recibieron la actualización.

## Paquetes de consulta EIGRP

DUAL utiliza paquetes de consulta y de respuesta cuando busca redes y cuando realiza otras tareas. Los paquetes de consulta y respuesta utilizan una entrega confiable. Las consultas utilizan multicast o unicast, mientras que las respuestas se envíen siempre como unicast.

En la Imagen , R2 ha perdido la conectividad con LAN y envía consultas a todos los vecinos EIGRP y busca cualquier ruta posible hacia la LAN.

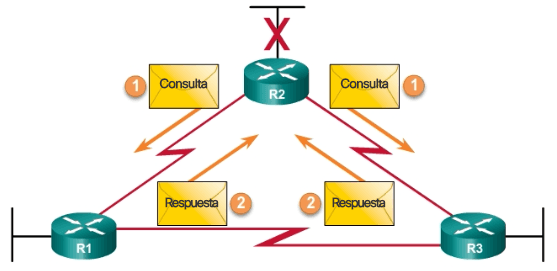
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/Mensajes-EIGRP-de-consulta-y-de-respuesta.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/Mensajes-EIGRP-de-consulta-y-de-respuesta.png)

Imagen Mensajes EIGRP de consulta y de respuesta

Debido a que las consultas utilizan entrega confiable, el router receptor debe devolver un paquete de acuse de recibo EIGRP. El acuse de recibo informa al emisor de la consulta que se recibió el mensaje de consulta. Para que el ejemplo sea más simple, se omitieron los acuses de recibo en el gráfico.

## Paquetes de respuesta EIGRP

Todos los vecinos deben enviar una respuesta, independientemente de si tienen o no una ruta a la red fuera de servicio. Debido a que las respuestas también usan entrega confiable, los routers como el R2 deben enviar un acuse de recibo.

Quizá no sea obvio por qué el R2 debería enviar una consulta para una red que sabe que está inactiva. En realidad, solo la interfaz del R2 que está conectada a la red está inactiva. Otro router podría estar conectado a la misma LAN y tener una ruta alternativa a la misma red. Por lo tanto, el R2 consulta por un router tal antes de eliminar completamente la red de su tabla de topología.

## Encapsulación de mensajes EIGRP

La porción de datos de un mensaje EIGRP se encapsula en un paquete. Este campo de datos se llama “**tipo, longitud, valor**” (TLV). Los tipos de TLV pertinentes a este curso son los parámetros de EIGRP, las rutas IP internas y las rutas IP externas.

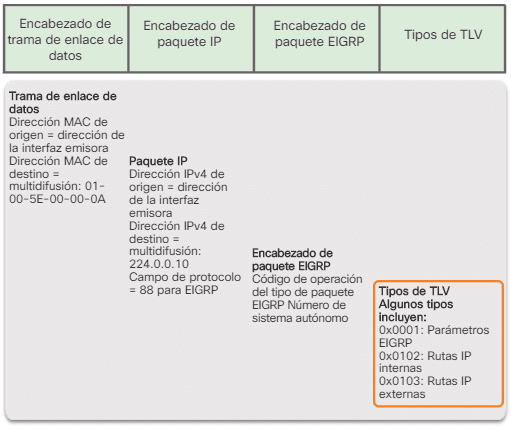
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/TLV-EIGRP.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/TLV-EIGRP.png)

Imagen Tipo/longitud/tipos de valores

El encabezado del paquete EIGRP se incluye con cada paquete EIGRP, independientemente de su tipo. Luego, el encabezado del paquete EIGRP y el TLV se encapsulan en un paquete IPv4.

En el encabezado del paquete IPv4, el campo de protocolo se establece en 88 para indicar EIGRP, y la dirección IPv4 de destino se establece en multidifusión 224.0.0.10. Si el paquete EIGRP se encapsula en una trama de Ethernet, la dirección MAC de destino también es una dirección de multidifusión, 01-00-5E-00-00-0A.

EIGRP para IPv6 usa un tipo de encapsulación similar. EIGRP para IPv6 se encapsula con un encabezado de IPv6. La dirección IPv6 de destino es la dirección de multidifusión FF02::A, y el campo de encabezado siguiente se establece en 88.

Encabezado de paquetes EIGRP

Todos los paquetes EIGRP incluyen el encabezado, como se muestra en la Imagen

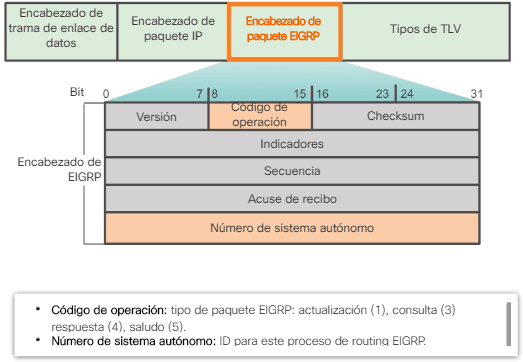
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/Encabezado-de-paquetes-EIGRP.png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/Encabezado-de-paquetes-EIGRP.png)

Imagen Encabezado de paquetes EIGRP

Los campos importantes incluyen el campo de código de operación y el campo de número de sistema autónomo. El código de operación especifica el tipo de paquete EIGRP de la siguiente manera:

* Actualizar
* Consulta
* Respuesta
* Saludo

El número de sistema autónomo especifica el proceso de routing EIGRP. A diferencia de RIP, se pueden ejecutar varias instancias de EIGRP en una red, y el número de sistema autónomo se usa para realizar el seguimiento de cada proceso EIGRP en ejecución.

# Tipos de TLV

## TLV de parámetros de EIGRP

El mensaje de parámetros de EIGRP incluye las ponderaciones que EIGRP usa para su métrica compuesta. Solo el ancho de banda y el retardo se ponderan de manera predeterminada. Ambos se ponderan de igual manera, por ello, tanto el campo K1 para el ancho de banda como el campo K3 para el retraso se establecen en uno (1). Los demás valores K se establecen en cero (0).

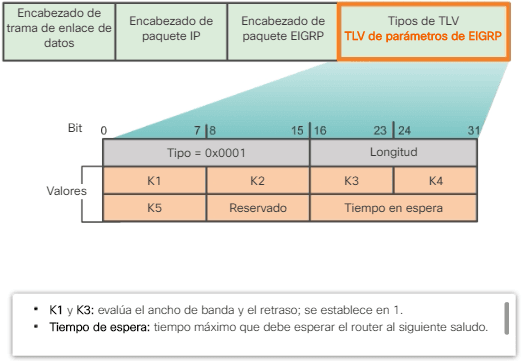
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/TLV-de-par%C3%A1metros-de-EIGRP..png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/TLV-de-par%C3%A1metros-de-EIGRP..png)

Imagen 11: TLV de parámetros de EIGRP.

El Tiempo de espera es la cantidad de tiempo que el vecino EIGRP que recibe este mensaje debe esperar antes de considerar que router que realiza la notificación se encuentra desactivado.

## TLV de rutas IP internas

El mensaje de IP internas se usa para anunciar las rutas EIGRP dentro de un sistema autónomo. Los campos importantes incluyen los campos de métrica (retraso y ancho de banda), el campo de máscara de subred (longitud de prefijo) y el campo de destino.

El retardo se calcula como la suma de retardos desde el origen hacia el destino en unidades de 10 microsegundos. El ancho de banda es el que cuenta con la configuración más baja en todas las interfaces de la ruta.

La máscara de subred se especifica como la duración de prefijo o el número de bits de la red en la máscara de subred. Por ejemplo, la longitud de prefijo para la máscara de subred 255.255.255.0 es 24, porque 24 es el número de bits de red.

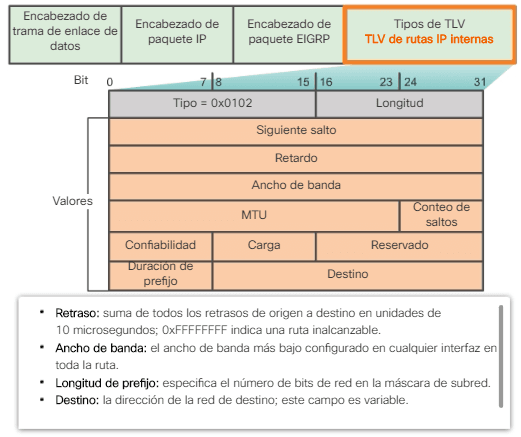
[[](https://ccnadesdecero.es/wp-content/uploads/2018/01/TLV-de-rutas-IP-internas..png)](https://ccnadesdecero.es/wp-content/uploads/2018/01/TLV-de-rutas-IP-internas..png)

Imagen TLV de rutas IP internas.

El campo Destino almacena la dirección de la red de destino. A pesar de que se muestran sólo 24 bits en esta figura, este campo varía en función del valor de la porción de red de la dirección de red de 32 bits.

Por ejemplo, la porción de red de 10.1.0.0/16 es 10.1; por lo tanto, el campo de destino almacena los primeros 16 bits. Como la longitud mínima de este campo es de 24 bits, el resto del campo se rellena con ceros. Si una dirección de red es más larga que 24 bits (192.168.1.32/27, por ejemplo), entonces el campo Destino se extiende otros 32 bits más (con un total de 56 bits) y los bits no utilizados se completan con ceros.

## TLV de rutas IP externas

El mensaje de IP externas se usa cuando las rutas externas se importan al proceso de routing EIGRP. Observe que la mitad inferior del TLV de rutas IP externas incluye todos los campos utilizados por el TLV de IP internas.

[Protocolo EIGRP: Definición y Características - CCNA desde Cero](https://ccnadesdecero.es/protocolo-eigrp-definicion-y-caracteristicas/)

Protocolo BGP

Si tiene que explicar qué es BGP a alguien nuevo en el entorno del proveedor de servicios, la mejor definición es que *BGP, o Protocolo de puerta de enlace de frontera, es el protocolo de routing que hace que Internet funcione*. El protocolo intercambia información de routing a través de Internet, utilizando routers y tablas de routing que se expresan en BGP.

BGP dirige paquetes entre sistemas autónomos (AS): redes administradas por una sola empresa o proveedor de servicios. El tráfico que se enruta dentro de una única red AS se conoce como BGP interno o iBGP. Más a menudo, BGP se utiliza para conectar un AS a otros sistemas autónomos, y luego se denomina BGP externo o eBGP.

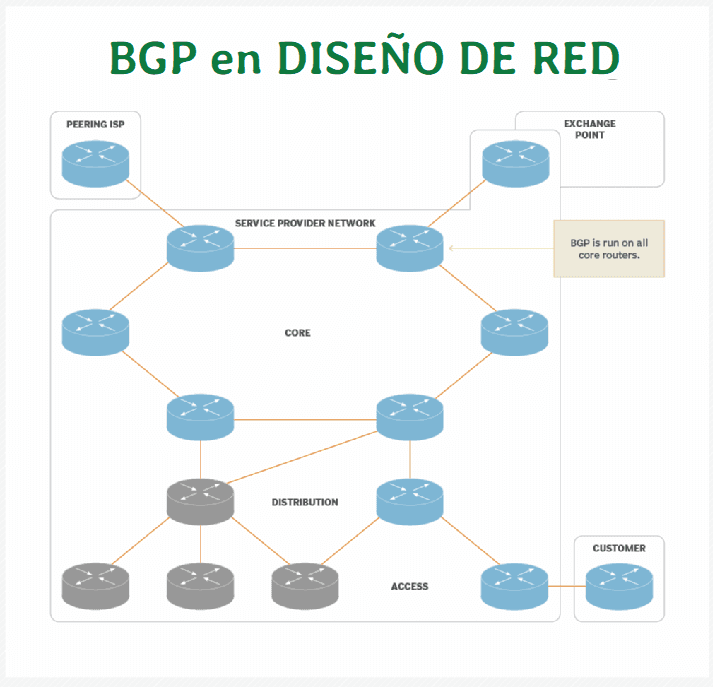
La función principal de BGP es intercambiar información de capacidad de alcance de la red con otros sistemas BGP. El Protocolo de puerta de enlace de frontera construye un gráfico de sistemas autónomos basado en la información intercambiada entre routers BGP.

Cómo funciona BGP

En la terminología BGP, un dominio de routing independiente, que casi siempre significa una red ISP, se denomina sistema autónomo. BGP siempre se usa como el protocolo de routingde elección entre diferentes ISP, lo que se conoce como BGP externo. Los ISP grandes también usan BGP como el protocolo de routing central dentro de sus propias redes, lo que se denomina BGP interno.

Para permitir la transferencia de información de routing entre ISP vecinos, BGP requiere acuerdos de pares, que comprenden los términos y condiciones necesarios para el intercambio de tráfico. El protocolo se adhiere a estos acuerdos, al tiempo que evalúa las tablas de routing y la información a lo largo de múltiples rutas entre los ISP. Lo hace utilizando un algoritmo de selección que determina la mejor ruta para dirigir el tráfico en función de comandos y atributos especificados. Sin embargo, el mejor camino no siempre es el más corto.

Debido a la complejidad inherente de BGP, los clientes y los ISP pequeños a menudo implementan BGP solo donde es necesario, por ejemplo, en puntos de interconexión y en un subconjunto mínimo de routers centrales, los que se encuentran entre los puntos de interconexión, como se muestra en el siguiente diagrama.

[[](https://ccnadesdecero.es/wp-content/uploads/2020/01/Uso-de-BGP.png)](https://ccnadesdecero.es/wp-content/uploads/2020/01/Uso-de-BGP.png)

# Uso de BGP

BGP ofrece estabilidad de red que garantiza que los routers puedan adaptarse rápidamente para enviar paquetes a través de otra re-conexión si una ruta de Internet se cae. BGP toma decisiones de routing basadas en rutas, reglas o políticas de red configuradas por un administrador de red. Cada router BGP mantiene una tabla de routing estándar utilizada para dirigir paquetes en tránsito. Esta tabla se usa junto con una tabla de routing separada, conocida como la *Routing Information Base* (RIB), que es una tabla de datos almacenada en un servidor en el router BGP. El RIB contiene información de ruta tanto de pares externos conectados directamente como de pares internos, y actualiza continuamente la tabla de routing a medida que ocurren cambios. BGP se basa en TCP/IP y utiliza la topología cliente-servidor para comunicar la información de enrutamiento, con el cliente-servidor iniciando una sesión BGP mediante el envío de una solicitud al servidor.

Problemas con el protocolo BGP

Border Gateway Protocol se creó originalmente en 1989 como una solución rápida para Internet, pero se ha mantenido como el protocolo principal para el tráfico de larga distancia. Desde entonces, sin embargo, las amenazas cibernéticas han evolucionado y BGP no ha seguido el ritmo.

El abuso del BGP se llama **BGP hijacking**, que es posible porque el protocolo se basa en confiar en las rutas anunciadas. Ha habido múltiples intentos de hacer una versión más segura de BGP, pero la implementación es extremadamente problemática. La mayoría de las nuevas versiones no pueden comunicarse con BGP estándar, lo que significa que todos los AS de todo el mundo tendrían que adoptar el nuevo protocolo simultáneamente.

Algunos incidentes de BGP que han tenido lugar en el pasado incluyen:

* En 2004, TTNet, un proveedor turco de servicios de Internet (ISP), anunció malas rutas BGP que afirmaban que eran el mejor destino para todo el tráfico en Internet. Los problemas solo duraron un día, pero muchas personas en todo el mundo no pudieron acceder a Internet.
* En 2008, un ISP paquistaní intentó bloquear el acceso de los usuarios paquistaníes a YouTube enrutando el tráfico a un agujero negro. La ruta se anunció accidentalmente a los routers vecinos que propagaron la ruta en todo el mundo. En este caso, YouTube estuvo inaccesible durante varias horas.
* Y, en 2018, los atacantes crearon deliberadamente malas rutas BGP para redirigir el tráfico destinado al servicio DNS de Amazon. Al redirigir el tráfico a ellos mismos, pudieron robar $100,000 de criptomonedas.