**Resumen segundo parcial telecomunicaciones**

**RIP (Routing information protocol)**

**¿Qué es RIP?**

El Protocolo de Información de Encaminamiento, Routing Information Protocol (RIP), es un protocolo de puerta de enlace interna o interior (Interior Gateway Protocol, IGP) utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol (IP) a las que se encuentran conectados. Su algoritmo de encaminamiento está basado en el vector de distancia, ya que calcula la métrica o ruta más corta posible hasta el destino a partir del número de "saltos" o equipos intermedios que los paquetes IP deben atravesar. El límite máximo de saltos en RIP es de 15, de forma que al llegar a 16 se considera una ruta como inalcanzable o no deseable.

Ejemplo de sintaxis de configuración en router Cisco

Router(config)#router rip

Router(config-router)#network 192.168.1.0

Router(config-router)#network 200.200.1.0

Router(config-router)#version 2

Router(config-router)#maximum-paths 6

Router(config-router)#no auto-summary

**Temporizadores RIP**

RIP utiliza unos temporizadores para que apoyen su funcionamiento, las cuales son:

**Temporizador periódico:** este controla la publicación de los mensajes de actualización regulares. Se debe ajustar el temporizador a 30 s, esto es para evitar se sincronicen y así sobrecargar el Internet si los routers se actualizan de forma simultánea. Cada router posee un temporizar periódico que se establece al azar a un número que va de 25 a 35 que va en decremento hasta llegar a 0 y envía un mensaje de actualización.

**Temporizador de caducidad (o timer de invalidación):** establece cuanto tiempo puede estar una ruta en la tabla de ruteo sin ser actualizada. Cuando un router recibe la información actualizada para una ruta, el temporizador establece 180 s para esa ruta en particular. Si pasados los 180 s asignados no se actualiza la ruta, se considera que está caducada y el número de saltos se pone 16 considerándose una ruta inalcanzable.

**Temporizador de Colección de Basura:** este temporizador controla el tiempo que pasa entre que una ruta es invalidada (o marcada como inalcanzable) y el tiempo que pasa hasta que se elimina la entrada de la tabla de ruteo. El valor predeterminado es de 240 s. Esto es 60 s más largo que el temporizador de caducidad. Entonces, por 60 s el router estará anunciando sobre la ruta inalcanzable a todos sus vecinos. El valor del temporizador debe setearse en un valor mayor que el temporizador de caducidad.

**Versiones**

En la actualidad existen dos versiones de RIP: RIPv1, RIPv2. También existe la versión RIpng, para IPv6.

**RIPv1**

La definición original, recogida en el RFC 1058, define RIP como un protocolo de enrutamiento con clase, es decir, basado en las clases de las direcciones IP. Por tanto, RIPv1 no soporta máscaras de tamaño variable (VLSM) ni direccionamiento sin clase (CIDR). Esto implica que las redes tratadas por este protocolo deben tener la máscara de red predefinida para su clase de dirección IP, lo que resulta poco eficiente. Además, RIPv1 tampoco incluye ningún mecanismo de autentificación de los mensajes, haciéndolo vulnerable a ataques cibernéticos.

**RIPv2**

Debido a las limitaciones de la versión 1, se desarrolla RIPv2 en 1993,2​ y se estandariza finalmente en 1998.3​ Esta versión soporta subredes, permitiendo así CIDR y VLSM. Además, para tener retrocompatibilidad con RIPv1, se mantuvo la limitación de 15 saltos si se está usando el protocolo OSPF o cualquier otro que sirva para direccionamiento en el enlace.

Se agregó una característica de "interruptor de compatibilidad"3​ para permitir ajustes de interoperabilidad más precisos. RIPv2 soporta autenticación

**RIPng**

RIP para IPv6.

**Ventajas**

* RIP es más fácil de configurar (comparativamente a otros protocolos).
* Implementa un algoritmo de encaminamiento más simple que otros protocolos, por lo que el cálculo de la "mejor" ruta (comparativamente en encaminadores de similares prestaciones) es más rápida.
* Es soportado por la mayoría de los fabricantes.
* El protocolo EIGRP de Cisco, patentado por ellos, salva la principal desventaja del nativo protocolo RIP porque valora la mejor métrica, además del número de saltos y otros criterios (ancho de banda, congestión, carga, retardo, fiabilidad, etc.), haciendo más eficiente la red

**Desventajas de RIP**

* Su principal desventaja consiste en que, para determinar la mejor métrica, únicamente toma en cuenta el número de saltos, descartando otros criterios (ancho de banda, congestión, carga, retardo, fiabilidad, etc.).
* El límite máximo de saltos es menor que el de otros protocolos (máximo 15 saltos), de forma que solo se puede utilizar en redes de tamaño mediano o pequeño.
* RIP tampoco está diseñado para resolver cualquier posible problema de enrutamiento. El RFC 1720 (STD 1) describe estas limitaciones técnicas de RIP como graves y el IETF está evaluando candidatos para reemplazarlo, dentro de los cuales OSPF es el favorito. Este cambio está dificultado por la amplia expansión de RIP y necesidad de acuerdos adecuados.
* El tiempo de convergencia es largo.
* Sólo se puede utilizar para redes pequeñas.

**Modo de operación**

El valor de AD de RIP es de 120, por ello tiene menor prioridad sobre los demás protocolos de encaminamiento.

Cuando RIP se inicia, envía un mensaje a cada uno de sus vecinos (en el puerto 520) pidiendo una copia de la tabla de encaminamiento del vecino. Este mensaje es una solicitud (el campo "command" se pone a 1) con "address family" a 0 y "metric" a 16. Los routers vecinos devuelven una copia de sus tablas de encaminamiento.

Cuando RIP está en modo activo envía toda o parte de su tabla de encaminamiento a todos los vecinos por broadcast y/o con enlaces punto a punto. Esto se hace cada 30 segundos. La tabla de encaminamiento se envía como respuesta ("command" vale 2, aunque no haya habido petición).

Cuando RIP descubre que una métrica ha cambiado, la difunde por broadcast a los demás routers.

Cuando RIP recibe una respuesta, el mensaje se corrobora y la tabla local se actualiza si es necesario (Para mejorar el rendimiento y la fiabilidad, RIP establece que una vez que un router (u host) ha aprendido una ruta de otro, debe guardarla hasta que conozca una mejor (de coste estrictamente menor). Esto evita que los routers oscilen entre dos o más rutas de igual coste).

Cuando RIP recibe una petición, distinta de la solicitud de su tabla, se devuelve como respuesta la métrica para cada entrada de dicha petición fijada al valor de la tabla local de encaminamiento. Si no existe ruta en la tabla local, se pone a 16.

Las rutas que RIP aprende de otros routers expiran a menos que se vuelvan a difundir en 180 segundos (6 ciclos de broadcast). Cuando una ruta expira, su métrica se pone a infinito, la invalidación de la ruta se difunde a los vecinos, y 60 segundos más tarde, se borra de la tabla.

**Tipos**

Los mensajes RIP pueden ser de dos tipos:

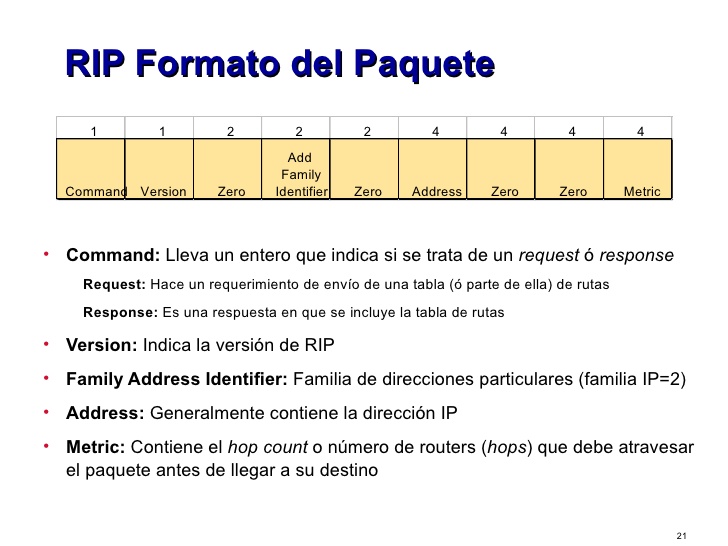
Petición: enviados por algún encaminador recientemente iniciado que solicita información de los encaminadores vecinos.

Respuesta: mensajes con la actualización de las tablas de encaminamiento. Existen tres tipos:

Mensajes ordinarios: Se envían cada 30 segundos. Para indicar que el enlace y la ruta siguen activos. Se envía la tabla de encaminado completa.

Mensajes enviados como respuesta a mensajes de petición.

Mensajes enviados cuando cambia algún coste. Se envía toda la tabla de encaminado.



**RIP utiliza el algoritmo de enrutamiento vector distancia**

[**https://es.wikipedia.org/wiki/Vector\_de\_distancias**](https://es.wikipedia.org/wiki/Vector_de_distancias)

**Open Shortest Path First**

Open Shortest Path First (OSPF), "Abrir el camino más corto primero" en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (Link-State Database, LSDB) idéntica en todos los routers de la zona.

OSPF puede operar con seguridad usando MD5 para autenticar sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado.

OSPF es probablemente el protocolo IGP más utilizado en redes grandes; IS-IS, otro protocolo de encaminamiento dinámico de enlace-estado, es más común en grandes proveedores de servicios. Como sucesor natural de RIP, acepta VLSM y CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre red

Los direccionadores o sistemas de una red OSPF, después de haberse asegurado de que sus interfaces son funcionales, envían en primer lugar paquetes Hello, utilizando el protocolo Hello por sus interfaces OSPF, para descubrir vecinos. Vecinos son los direccionadores o sistemas que tienen interfaces con la red común. Después, los direccionadores o sistemas vecinos intercambian sus bases de datos de enlace-estado para establecer adyacencias.

**Encaminamiento, routers y áreas**

OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.

**Tipos de router en OSPF**

Un router OSPF clásico es capaz de encaminar cualquier paquete destinado a cualquier punto del área en el que se encuentra (encaminamiento intra-área). Para el encaminamiento entre distintas áreas del AS (encaminamiento inter-área) y desde el AS hacia el exterior (encaminamiento exterior), OSPF utiliza routers especiales que mantienen una información topológica más completa que la del área en la que se sitúan. Así, pueden distinguirse:

* Routers fronterizos de área o Area Border Routers (ABR), que mantienen la información topológica de su área y la conectan con el resto de las áreas, permitiendo encaminar paquetes a cualquier punto de la red (inter-area routing).
* Routers fronterizos del Sistema Autónomo o Autonomous System Border Routers (ASBR), que permiten encaminar paquetes fuera del AS en que se alojen, es decir, a otras redes conectadas al Sistema Autónomo o resto de Internet (external routing).

Un paquete generado en la red será enviado, de forma jerárquica, a través del área si su destino es conocido por el emisor; al ABR del área correspondiente si el destino es inter-área; este lo enviará al router del área de destino, si este se encuentra en el AS; o al ASBR si el destino del paquete es exterior a la red (desconocida por el ABR).

Tipo de áreas

Cuando los sistemas autónomos son grandes por sí mismos y nada sencillos de administrar. OSPF les permite dividirlos en áreas numeradas donde un área es una red o un conjunto de redes inmediatas. Un área es una generalización de una subred. Fuera de un área, su topología y detalle no son visibles.

**OSPF distingue los siguientes tipos de área:**

Área Backbone

El backbone, también denominado área cero, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red. La conexión entre un área y el backbone se realiza mediante los ABR, que son responsables de la gestión de las rutas no-internas del área (esto es, de las rutas entre el área y el resto de la red).

Área stub

Una área stub es un área en la que no se anuncia rutas externas al SA (sistema autónomo) y el encaminamiento dentro del área está basado completamente en una ruta por defecto. Un enrutador frontera de área (ABR) borra los anuncios de rutas externas de tipo 4 y tipo 5 de los routers internos del área y envía a todos esos routers la ruta por defecto 0.0.0.0 para salir del área a través del ABR, convirtiéndose así en el gateway por defecto. Esto reduce la base de datos LSDB y el tamaño de la tabla de encaminamiento de los routers internos del área.

Área not-so-stubby

También conocidas como NSSA, constituyen un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone y otras áreas, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas. No puede recibir rutas externas de Sistema Autónomo desde otras áreas (del propio sistema autónomo). NSSA es una extensión de las áreas stub que permite la inyección de rutas externas de forma limitada dentro de las áreas stub.

**Interfaces en OSPF**

Los nodos de una red basada en OSPF se conectan a ella a través de una o varias interfaces con las que se conectan a otros nodos de la red. El tipo de enlace define la configuración que asume la interfaz correspondiente. OSPF soporta las siguientes tipos de enlace, y provee para cada uno de ellos una configuración de interfaz:

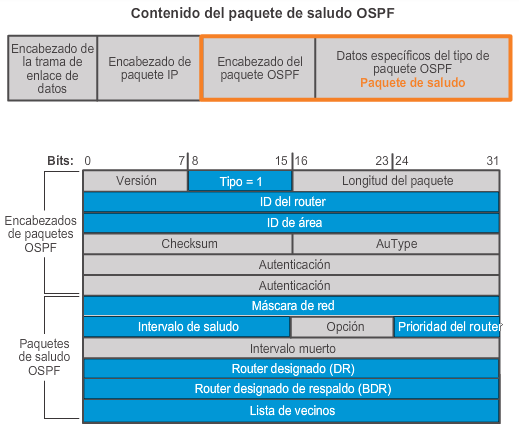
Punto a punto (point-to-point, abreviado ptp), cuando la interfaz está conectada exclusivamente a otra interfaz.

Punto a multipunto (point-to-multipoint, abreviado ptmp).

Broadcast, para enlaces en los que todas las interfaces pueden conectarse directamente entre ellas. El ejemplo típico de enlace broadcast es el que corresponde a una red de tipo Ethernet.

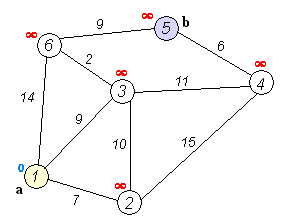
Enlace virtual (virtual link), cuando no responde a una topología física.

Enlace de acceso múltiple acceso sin difusión (Non-Broadcast Multiple Access, NBMA), para enlaces en los que el medio es compartido, pero no todas las interfaces participantes pueden comunicarse directamente entre sí.



**OSPF utiliza el algoritmo de enrutamiento Dijkstra**

[**https://es.wikipedia.org/wiki/Algoritmo\_de\_Dijkstra**](https://es.wikipedia.org/wiki/Algoritmo_de_Dijkstra)



**BGP (Border Gateway Protocol)**

En telecomunicaciones, el protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol)1​ es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo, los cuales deben ser compatibles con BGP. Se trata del protocolo más utilizado para redes con intención de configurar un protocolo de puerta de enlace exterior (Exterior Gateway Protocol).

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo o AS. Cada uno tendrá conexiones o sesiones internas (iBGP), así como sesiones externas (eBGP).

El protocolo de puerta de enlace de frontera (BGP) es un ejemplo de protocolo de puerta de enlace exterior (EGP). BGP intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet. BGP4 es la primera versión que admite encaminamiento entre dominios sin clase (CIDR) y agregado de rutas. A diferencia de los protocolos de puerta de enlace internos (IGP), como RIP, OSPF y EIGRP, no usa métricas como número de saltos, ancho de banda o retardo. En cambio, BGP toma decisiones de encaminamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

BGP juega un papel crítico en las comunicaciones en Internet.2​3​4​5​6​7​ Facilita el intercambio de información sobre redes IP y la comunicación entre sistemas autónomos (AS). Por tanto, BGP es un protocolo interdominio (entre sistemas autónomos) e intradominio (dentro del mismo sistema autónomo).

El protocolo BGP se utiliza para intercambiar información mediante el establecimiento de una sesión de comunicación entre los enrutadores de frontera de los sistemas autónomos. Para conseguir una entrega fiable de la información, se hace uso de una sesión de comunicación basada en TCP en el puerto número 179. Esta sesión debe mantenerse activa debido a que ambos extremos de la comunicación periódicamente se intercambian y actualizan información. Al principio, cada router envía al vecino toda su información de encaminamiento y después únicamente se enviarán las nuevas rutas, las actualizaciones o la eliminación de rutas transmitidas con anterioridad. Además periódicamente se envían mensajes para garantizar la conectividad.

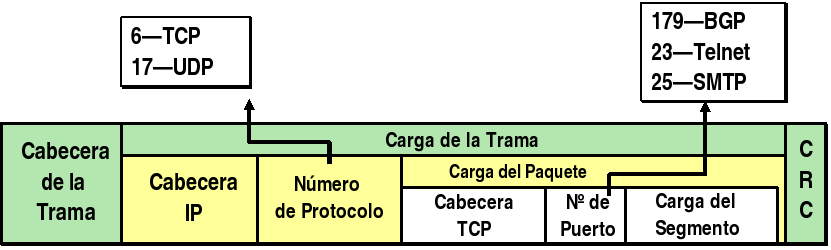
Cuando una conexión TCP se interrumpe por alguna razón, cada extremo de la comunicación está obligado a dejar de utilizar la información que ha recibido del otro extremo. En otras palabras, la sesión TCP sirve como un enlace virtual entre dos sistemas autónomos vecinos, y cuando hay una falta de intercambio de comunicación indica que el enlace virtual se ha caído. Cabe destacar que esa unión virtual tendrá más de un enlace físico que conecte a los dos enrutadores frontera, pero si una conexión virtual se cae no indica necesariamente que la conexión física se haya caído.

Desde el punto de vista de su topología, se puede considerar como un gráfico de conexión de sistemas autónomos conectados mediante enlaces virtuales. En la figura a continuación se pueden ver cuatro sistemas autónomos llamados AS1, AS2, AS3 y AS4 conectados por enlaces virtuales. Es decir, que mantienen sesiones BGP sobre TCP para la comunicación entre los sistemas autónomos. Cada sistema autónomo contiene una o más redes que se identificaron como N1, N2 y N3 en AS1, y así sucesivamente. Simplemente observando la figura se puede mostrar que existe más de una ruta posible entre dos sistemas autónomos determinados. Como también es posible tener uno o más de un router de borde en el mismo sistema autónomo.

Para la puesta en funcionamiento de la red anterior se debe proveer de un mecanismo de intercambio de rutas que permita comunicar correctamente ambos sistemas. El protocolo BGP utiliza el protocolo de vector de caminos, en inglés: Path vector protocol para el intercambio de información de encaminamiento en la red. Se transmite una lista con identificación de los AS por los que pasa el anuncio. De esa manera se conseguirá saber cómo llegar a cualquier dirección del prefijo propagado así como estar preparado para cursar tráfico para cualquier dirección del prefijo.

Antes de enunciar la mecánica de selección de rutas se deben introducir las dos formas de proceder cuando se cuenta con un escenario en el que implantar BGP. Se debe distinguir entre BGP externo (eBGP) y BGP interno (iBGP) en función de si la información se intercambia dentro de un AS o entre dos AS. Se puede observar en la figura anterior que el sistema autónomo AS1 debe propagar tres prefijos IP (N1, N2 y N3) para que sean alcanzables desde los equipos de otros sistemas autónomos. Además, estas tres redes deberán establecer cierta política de decisión de rutas hacia otros sistemas autónomos. IBGP conforma una topología virtual mallada de modo que todos los enrutadores de un sistema autónomo se encuentren conectados para que el intercambio de rutas sea directo desde el router al que le llega el anuncio hacia todos los de su sistema autónomo.

<https://es.wikipedia.org/wiki/Border_Gateway_Protocol>



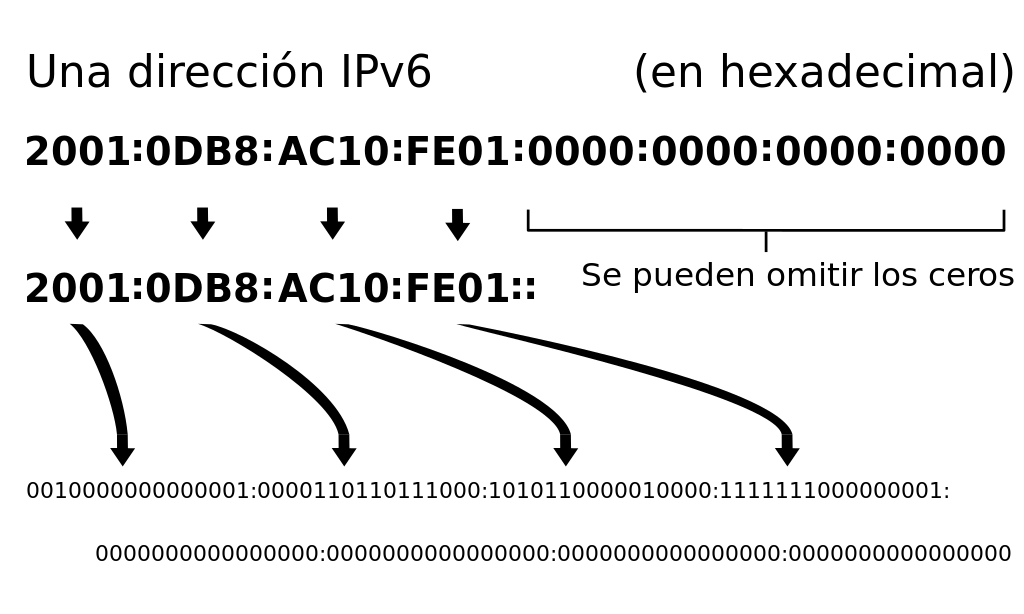
**IP versión 6 (IPv6)**

El IPv6 es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones. Su desarrollo comenzó en diciembre de 1998 cuando Steve Deering y Robert Hinden, empleados de Cisco y Nokia publicaron una especificación formal del protocolo a través de un RFC1​2​ y aún continua su implementación.

Diseñado por Steve Deering de Xerox PARC IPv6, su objetivo era sustituir finalmente a IPv4,[cita requerida] cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar busca mejorar el servicio globalmente; por ejemplo, proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes.

IPv4 posibilita 4 294 967 296 (232) direcciones de dispositivos diferentes, un número menor a la población mundial, y menor a la cantidad de dispositivos totales. A principios de 2010, quedaban menos del 10 % de IP sin asignar.3​ En la semana del 3 de febrero de 2011,4​ la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

En cambio, IPv6 admite 340 282 366 920 938 463 463 374 607 431 768 211 456 (2128 o 340 sextillones de direcciones), cerca de 6,7 × 1017 (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra.



El tamaño de una subred en IPv6 es de 264 (máscara de subred de 64-bit), el cuadrado del tamaño de la Internet IPv4 entera. Así, las tasas de utilización del espacio de direcciones serán probablemente menor en IPv6, pero la administración de las redes y el ruteo serían más eficientes debido a las decisiones de diseño inherentes al mayor tamaño de las subredes y la agregación jerárquica de rutas.

Se hicieron varias simplificaciones en la cabecera de los paquetes, así como en el proceso de reenvío de paquetes para hacer el procesamiento de los paquetes más simple y por ello más eficiente. En concreto:

El encabezado del paquete en IPv6 es más simple que el utilizado en IPv4, así los campos que son raramente utilizados han sido movidos a opciones separadas; en efecto, aunque las direcciones en IPv6 son 4 veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).

Los routers IPv6 no hacen fragmentación. Los nodos IPv6 requieren ya sea hacer descubrimiento de MTU, realizar fragmentación extremo a extremo o enviar paquetes del tamaño mínimo MTU para IPv6 (1280 bytes).

El encabezado IPv6 no está protegido por una suma de comprobación (checksum); la protección de integridad se asume asegurada tanto por el checksum de capa de enlace y por un checksum de nivel superior (TCP, UDP, etc.). De esta forma los routers IPv6 no necesitan recalcular la suma de comprobación cada vez que algún campo del encabezado (como el contador de saltos o Tiempo de Vida) cambian. Esta mejora puede ser menos necesaria en routers que utilizan hardware dedicado para computar este cálculo y así pueden hacerlo a velocidad de línea (wirespeed), pero es relevante para routers por software. Por este motivo mientras en IPv4 los paquetes UDP pueden tener un checksum de 0, indicando que no hay comprobación de checksum a este nivel, en IPv6 es necesario que los paquetes UDP incorporen checksum.

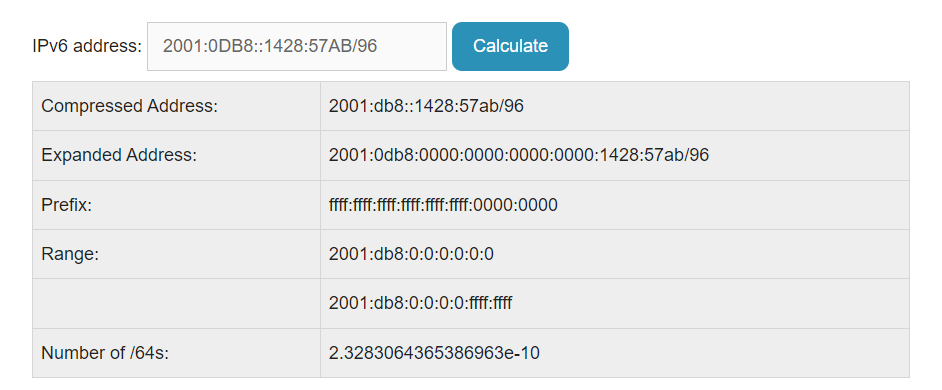
El campo Tiempo de Vida de IPv4, conocido como TTL (Time To Live), pasa a llamarse Límite de saltos, reflejando el hecho de que ya no se espera que los routers computen el tiempo en segundos que tarda en atravesarlo (que en cualquier caso siempre resulta menor de 1 segundo). Se simplifica como el número de saltos entre routers que se permita realizar al paquete IPv6.

El cambio más grande de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374 pero fue redefinida en abril de 2003 en la RFC 3513, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.

El número de direcciones IPv6 posibles es de 2128 ≈ 3.4 x 1038. Este número puede también representarse como 1632, con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores (véase combinatoria).

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

Ejemplo con una calculadora



Practica

2001:0DB8::1428:57AB/96

2001:0DB8:0000:0000:0000:0000:1428:57AB / 96

96/16 = 6

prefijo

Ffff:ffff:ffff:ffff:ffff:ffff:0000:0000

rango

2001:0DB8:0:0:0:0:0:0 -> 2001:0DB8:0:0:0:0:ffff:ffff

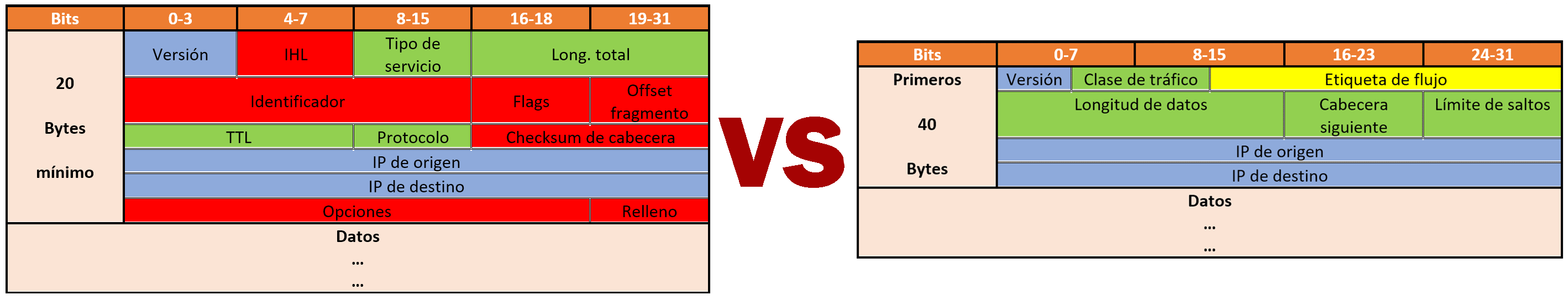
IPv6 (ventajas y desventajas)

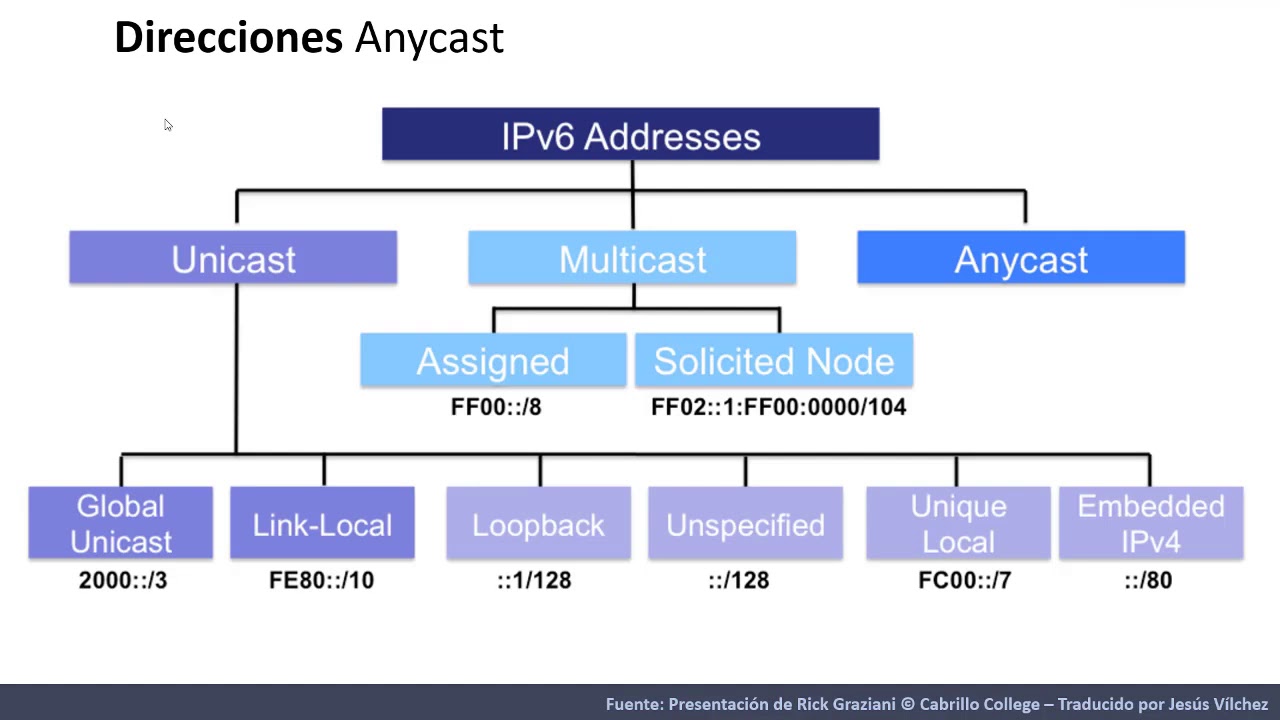
Ventajas:

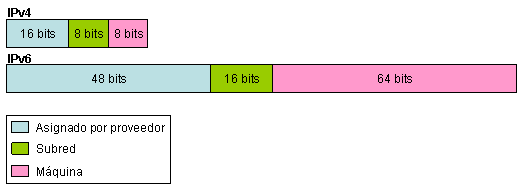
Para dimensionar la cantidad de direcciones IP que puede suministrar IPV6, basta con afirmar que este protocolo puede asignar una cantidad cercana a los 670 mil millones de direcciones por cada milímetro cuadrado de la superficie de la tierra, con lo cual lograría que cada persona pueda asignarle una IP única a cada uno de sus dispositivos. Otra ventaja de utilizar IPV6 son sus niveles de seguridad, ya que incluye dentro de sus especificaciones procesos de Cifrado de información y la verificación de autenticidad del origen de la misma; IPV6 permite utilizar Jumbogramas (Paquetes de datos de mayor tamaño, hasta de 64 bits). Dentro de las bondades que nos ofrece IPV6 también se incluye el mecanismo Plug and play, facilitando así la pronta conexión de dispositivos a la red, gracias a que la configuración se realiza de forma automática, Plug and play permite que al conectar un dispositivo a una red con IPV6 se le asigne una o más direcciones, lo cual facilita la administración de la red; IPV6 fue pensado y desarrollado para ser escalable permitiendo introducir mejoras a futuro. Al incorporar IPv6 una gran cantidad de direcciones, no será necesario utilizar NAT Traducción de direcciones de red, y sus nuevas capacidades de Plug and Play, seguridad, y QoS implicarán mejores conexiones de voz.

Desventajas:

La necesidad de extender un soporte permanente requiere una dirección IPv4 o algún tipo de NAT Traducción de direcciones de red en los routers pasarela. Por otra parte a nivel de arquitectura, las direcciones IPv6 son más difíciles de memorizar. La mayoría de redes son IPv4 entonces la implementación total de IPv6 sería muy costosa y tardaría mucho tiempo mientras tanto se requieren la implementación de los mecanismos de transición para la interacción de las 2 redes. Incluyendo a esto, existe aun poco conocimiento técnico sobre protocolos de ruteo en cuanto se refiere a organizaciones o ISP locales en ciertas regiones.







**Características de un algoritmo de ruteo:**

* **Exacto:** Calcula correctamente la mejor ruta
* **Simple:** poco consumo de recursos
* **Robusto:** en caso de mucho tráfico no debe fallar
* **Convergente:** Se reconfigura rápidamente
* **Flexible:** Debe soportar diferentes métricas

**Dos tipos:**

**No adaptativo:** Toman la decisión por adelantado sin mediciones de campo

**Adaptativo:** Las decisiones reflejan los cambios de topología y trafico

**Dos tipos de servicios:**

**Protocolo o servicio no orientado a la conexión**

El dispositivo en un extremo de la comunicación transmite los datos al otro, sin tener que asegurarse de que el receptor esté disponible y listo para recibir los datos. El emisor simplemente envía un mensaje dirigido al receptor.

**Protocolo o servicio orientado a la conexión**

Un protocolo orientado a la conexión es un modo de comunicación de redes donde se debe establecer una conexión antes de transferir datos. Se identifica el flujo de tráfico con un identificador de conexión en lugar de utilizar explícitamente las direcciones de la fuente y el destino. Típicamente, el identificador de conexión es un escalar (por ejemplo en Frame Relay son 10 bits y en Asynchronous Transfer Mode 24 bits). Esto hace a los conmutadores de red substancialmente más rápidos (las tablas de encaminamiento son más sencillas, y es más fácil construir el hardware de los conmutadores). El impacto es tan grande, que protocolos típicamente no orientados a la conexión, tal como el tráfico de IP, utilizan prefijos orientados a la conexión (por ejemplo IPv6 incorpora el campo "etiqueta de flujo").

Se dice que un servicio de comunicación entre dos entidades es orientado a conexión cuando antes de iniciar la comunicación se verifican determinados datos (disponibilidad, alcance, etc.) entre estas entidades y se negocian unas credenciales para hacer esta conexión más segura y eficiente. Este tipo de conexiones suponen mayor carga de trabajo a una red (y tal vez retardo) pero aportan la eficiencia y fiabilidad necesaria a las comunicaciones que la requieran.

**Actividades:**

1. Comprima la direccion IPv6 **2001:00FE:ACAD:2013:0000:0000:00AA:0271**

***2001:FE:ACAD:2013::AA:0271***

**Los : significa que hay omisión de 0, siempre hay que hacer la compresión sabiendo que luego esta tiene que ser interpretada y recuperada**

1. **La alcanzabilidad es un concepto usado en BGP y significa**

**En el contexto del protocolo BGP (Border Gateway Protocol), el término "alcanzabilidad" se refiere a la capacidad de alcanzar una red específica a través de las rutas anunciadas por los sistemas autónomos (AS) en la red de Internet. BGP es un protocolo de enrutamiento utilizado para intercambiar información de enrutamiento entre sistemas autónomos en Internet.**

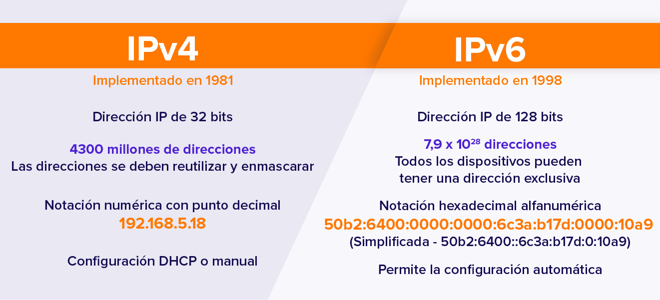
**Cuando se dice que una red es "alcanzable" a través de BGP, significa que los routers BGP en diferentes sistemas autónomos han intercambiado información de enrutamiento y han acordado rutas válidas para llegar a esa red en particular. Esta capacidad de alcanzabilidad es fundamental para el funcionamiento efectivo de Internet, ya que permite que los datos se enruten de manera adecuada desde un punto de origen hasta un destino a través de múltiples sistemas autónomos.**

**En resumen, en el contexto de BGP, la alcanzabilidad se refiere a la capacidad de llegar a una red específica mediante la propagación de información de enrutamiento entre sistemas autónomos.**

**RESPUESTA CORRECTA: Cada SA debe tener información de las redes alcanzables, de modo que se puedan identificar esas redes y se puedan conectar o establecer recorridos entre si.**

1. Las direcciones IPv6 globales son similares a

**Son similares a las ipv4 publicas**



1. **Cual No es una de las principales características de un ruteador?. Que sea .... por ver**
2. **IPv6 no tiene campos de fragmentación en su reader. Explique**

**IPv6 ha eliminado el campo de fragmentación en la cabecera de los paquetes por varias razones, y estas decisiones están relacionadas con las lecciones aprendidas del uso de IPv4. Aquí hay algunas razones clave:**

**Reducción de la carga en los routers: En IPv4, cuando un router encuentra un paquete que es demasiado grande para ser transmitido por la siguiente interfaz de red, fragmenta el paquete en fragmentos más pequeños. Los routers deben procesar y reensamblar estos fragmentos, lo que añade carga a los routers y puede afectar el rendimiento. Al eliminar la fragmentación en el nivel de red, IPv6 transfiere la responsabilidad de la fragmentación a las capas superiores (como el transporte, como TCP) o a los dispositivos finales.**

**Simplificación del enrutamiento: La fragmentación puede complicar el enrutamiento. En IPv6, la eliminación de la fragmentación simplifica la tarea de los routers al evitar que tengan que manejar la fragmentación de paquetes.**

**Evitar ataques de fragmentación: La fragmentación de paquetes ha sido utilizada en ataques, como los ataques de denegación de servicio. Eliminar la fragmentación en la capa de red puede ayudar a mitigar ciertos tipos de ataques relacionados con la fragmentación.**

**En lugar de depender de la fragmentación en la capa de red, IPv6 prefiere que los dispositivos finales negocien tamaños de paquetes efectivos y, si es necesario, realicen la fragmentación a un nivel más alto, como el de la capa de transporte (por ejemplo, TCP). Esto se logra mediante el uso de los mecanismos de descubrimiento de la unidad máxima de transmisión (MTU) y el establecimiento del tamaño del paquete durante la negociación.**

1. La dirección IPv6 /56 permite hasta ........ subredes

Ipv6 esta dividido en 64, son 128 bits. 64 para cada lado entonces:

64 – 56 = 8

2^8= **256**



La opción verdadera es:

- Ninguna de las respuestas

Explicación:

BGP trabaja con tablas de enrutamiento que contienen información sobre las rutas y no con vectores.

RIP y BGP son protocolos de enrutamiento, pero RIP es más comúnmente utilizado internamente (por ejemplo, dentro de una red corporativa), mientras que BGP se utiliza para enrutamiento entre dominios o sistemas autónomos.

Los sistemas autónomos (SA) no permiten reutilizar direcciones IP. Más bien, uno de los principios fundamentales de los SA es que cada uno tiene su propio espacio de direcciones IP único.

OSPF (Open Shortest Path First) es un protocolo de enrutamiento interno y no interconecta sistemas autónomos. Su propósito principal es permitir el enrutamiento dentro de un único sistema autónomo.

1. IPV6

Una dirección IPv6 está formada por 128 bits, no nibbles. Un nibble es la mitad de un byte (4 bits), por lo que una dirección IPv6 tiene 32 nibbles.

IPv6 tiene una dirección de loopback designada como ::1, que es análoga a la dirección IPv4 de loopback 127.0.0.1.

Las direcciones IPv6 no siguen el patrón especificado en la tercera opción. Las direcciones IPv6 utilizadas en la actualidad tienen diversos rangos asignados, y no se limitan a un rango específico como se describe en esa afirmación.

IPv6 utiliza direcciones de 128 bits, no de 48 bits. La longitud de una dirección IPv6 es considerablemente mayor que la de IPv4, que utiliza direcciones de 32 bits.