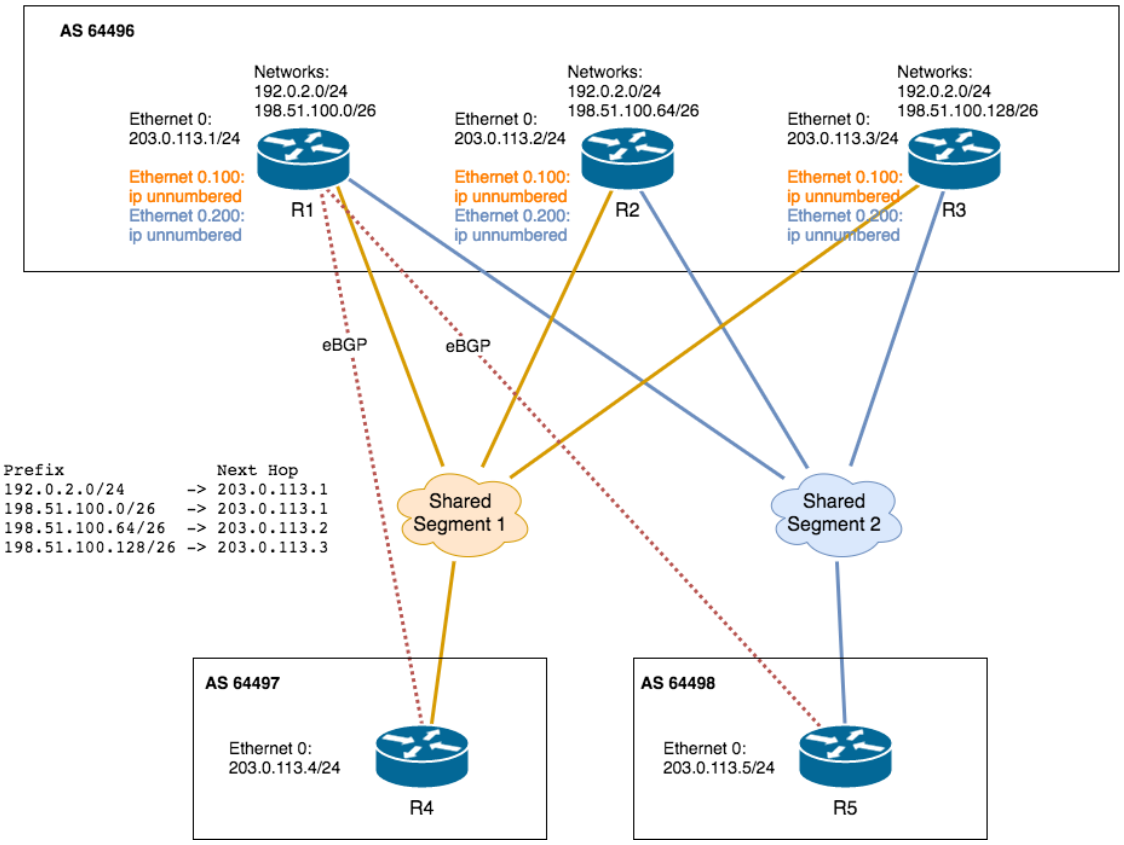
PROTOCOLO DE ENCAMINAMIENTO EXTERIOR BGP



ÍNDICE

1. INTRODUCCIÓN

El presente documento pretende servir como introducción al Protocolo de Encaminamiento Exterior BGP (Border Gateway Protocol), un componente fundamental en la infraestructura de Internet. A través de esta sección, se establecerá el contexto y la relevancia de BGP, además de definir los objetivos que se persiguen con este estudio.

1.1. CONTEXTO Y RELEVANCIA DEL PROTOCOLO BGP

El Protocolo de Encaminamiento Exterior BGP (BGP) desempeña un papel crucial en el funcionamiento de Internet. Se trata de un protocolo de enrutamiento dinámico que permite el intercambio de información de enrutamiento entre diferentes Sistemas Autónomos (AS), facilitando así la conectividad entre redes dispersas a nivel global ([1]). BGP funciona mediante el establecimiento de sesiones de comunicación entre pares de enrutadores fronterizos, los cuales intercambian información sobre las redes que conocen ([2]). A partir de esta información, cada enrutador construye su propia tabla de enrutamiento, la cual utiliza para determinar la mejor ruta para enviar los paquetes de datos hacia su destino final ([3]).

La relevancia de BGP radica en su capacidad para gestionar la complejidad de Internet, una red compuesta por miles de AS interconectados ([4]). Gracias a BGP, los enrutadores pueden intercambiar información de forma dinámica y eficiente, adaptándose a los cambios en la topología de la red y asegurando la entrega óptima de los datos ([5]).

1.2. OBJETIVOS DEL TRABAJO

El objetivo de este estudio es explorar en detalle el funcionamiento y la importancia de BGP en el panorama de las redes de computadoras. Se abordarán los siguientes aspectos:

- **Características fundamentales de BGP:** Se analizarán los mecanismos internos de BGP, incluyendo la forma en que se establecen las sesiones de comunicación, el intercambio de información de enrutamiento y la construcción de las tablas de enrutamiento ([6]).
- **Evolución histórica de BGP:** Se estudiará el desarrollo de BGP desde sus inicios hasta su estado actual, incluyendo los cambios en sus especificaciones y su adopción en la industria ([7]).
- **Papel de BGP en la interconexión de redes a gran escala:** Se examinará cómo BGP contribuye a la interconexión de redes a nivel global, permitiendo la comunicación entre usuarios ubicados en diferentes partes del mundo ([8]).
- **Políticas de enrutamiento en BGP:** Se analizarán las diferentes políticas de enrutamiento que pueden implementarse en BGP, y cómo estas políticas influyen en la selección de rutas y el tráfico de datos ([9]).
- **Desafíos de seguridad asociados con BGP:** Se identificarán los principales desafíos de seguridad que plantea la implementación de BGP, y se discutirán las medidas que pueden tomarse para mitigar estos riesgos.

A través de este estudio, se espera obtener una comprensión más profunda de cómo funciona Internet a nivel global y de los aspectos clave del enrutamiento en redes de gran escala.

2. FUNDAMENTOS DE ENRUTAMIENTO EN INTERNET

En esta sección, nos adentraremos en los conceptos básicos del enrutamiento en Internet para establecer una base sólida antes de abordar el Protocolo de Encaminamiento Exterior BGP.

2.1. BREVE REPASO DE ENRUTAMIENTO EN INTERNET

En Internet, el enrutamiento se refiere al proceso de dirigir el tráfico de datos desde su origen hasta su destino a través de una red de computadoras interconectadas. Aquí hay un breve repaso de cómo funciona el enrutamiento en Internet:

Direcciones IP: Cada dispositivo conectado a Internet posee una dirección IP única, como un DNI digital que lo identifica en la red. Estas direcciones IP, expresadas en formato numérico (por ejemplo, 192.168.1.100), sirven como puntos de referencia para que los routers puedan dirigir los paquetes de datos hacia su destino [10].

Protocolos de enrutamiento: En Internet, se utilizan varios protocolos de enrutamiento para determinar las mejores rutas para enviar datos entre dispositivos. Algunos de estos protocolos incluyen:

- **Protocolo de Internet (IP):** El pilar fundamental del enrutamiento, IP define el formato de los paquetes de datos y establece las reglas básicas para su transporte [12].
- **OSPF (Open Shortest Path First):** Este protocolo dinámico busca la ruta más corta entre dos puntos, optimizando el flujo de datos [13].
- **BGP (Border Gateway Protocol):** Un protocolo crucial para la interconexión de redes a gran escala, BGP permite el intercambio de información de enrutamiento entre diferentes sistemas autónomos (AS) [14].

Tablas de enrutamiento: Cada router en Internet mantiene una tabla de enrutamiento que contiene información sobre las rutas disponibles y cómo llegar a ellas. Estas tablas se actualizan dinámicamente a medida que cambian las condiciones de la red y se reciben nuevas rutas [11].

Anuncio de rutas: Los routers intercambian información de enrutamiento a través de anuncios de rutas. Cuando un router descubre una nueva ruta o un cambio en una ruta existente, puede anunciar esta información a otros routers en la red para que puedan actualizar sus tablas de enrutamiento [11].

Toma de decisiones de enrutamiento: Los routers toman decisiones sobre cómo enrutar los paquetes de datos en función de la información de enrutamiento disponible en sus

tablas de enrutamiento. Utilizan algoritmos y métricas para determinar la ruta más eficiente para enviar los datos al destino deseado [11].

En resumen, el enrutamiento en Internet es el proceso mediante el cual los paquetes de datos son dirigidos a través de la red desde su origen hasta su destino. Esto se logra a través de protocolos de enrutamiento, tablas de enrutamiento y la toma de decisiones de enrutamiento por parte de los routers en la red [11, 12, 13, 14 y 15].

2.2. CONCEPTO DE SISTEMA AUTÓNOMO (AS)

En el contexto de las redes de computadoras, un Sistema Autónomo (AS) se refiere a una colección de redes y routers que están bajo un control administrativo único y aplican políticas de enrutamiento coherentes. Estos sistemas se identifican mediante un número único denominado Número de Sistema Autónomo (ASN) [15].

El concepto de AS es fundamental en el enrutamiento en Internet porque permite dividir la infraestructura de la red en dominios gestionables y bien definidos. Cada AS es responsable de decidir cómo enrutar el tráfico que entra y sale de su red. Además, los AS se utilizan para establecer fronteras entre diferentes entidades administrativas, como proveedores de servicios de Internet, empresas, universidades, entre otros.

Los AS pueden ser de dos tipos principales:

Sistema Autónomo Multihomed (Multihome AS): Este tipo de AS tiene múltiples conexiones de red con otros AS, lo que le brinda redundancia y opciones de ruta. Los Multihome AS suelen ser proveedores de servicios de Internet (ISPs) o grandes empresas que necesitan alta disponibilidad y conectividad a Internet.

Sistema Autónomo Stub (Stub AS): Estos AS tienen una única conexión de salida hacia otro AS. Suelen ser organizaciones más pequeñas, como empresas locales o universidades, que no necesitan múltiples conexiones de red para alcanzar el resto de Internet.

La identificación única de los AS mediante los ASN facilita el intercambio de información de enrutamiento entre ellos, lo que permite la construcción de una red global coherente y escalable. En la siguiente sección, exploraremos cómo los protocolos de enrutamiento exterior, como BGP, se utilizan para intercambiar información entre sistemas autónomos en Internet.

2.3. ROL DE LOS PROTOCOLOS DE ENRUTAMIENTO EXTERIOR

Los protocolos de enrutamiento exterior juegan un papel crucial en la arquitectura de Internet al facilitar el intercambio de información de enrutamiento entre sistemas autónomos (AS). Estos protocolos son responsables de determinar las rutas óptimas para el tráfico de red a través de múltiples AS, asegurando así la conectividad global.

Según Feinler y el Grupo de Trabajo en Redes [15], uno de los protocolos más importantes en este ámbito es el Protocolo de Puerta de Enlace Fronteriza (BGP, por sus siglas en inglés), que se destaca por su amplia utilización en la infraestructura de Internet. BGP facilita el intercambio de información de enrutamiento y políticas entre AS, permitiendo a los administradores de red tomar decisiones informadas sobre las rutas más eficientes para alcanzar destinos específicos. Este protocolo se basa en vectores de distancia y políticas configuradas manualmente, otorgando flexibilidad y control sobre el enrutamiento [16].

Otro protocolo relevante es el Protocolo de Puerta de Enlace Exterior (EGP), precursor de BGP y utilizado en las primeras etapas de Internet para intercambiar información de enrutamiento entre AS. Pero EGP la desplazó sobre todo BGP por sus limitaciones y falta de soporte para políticas avanzadas de enrutamiento [17].

Además, el Protocolo de Estado de Enlace Abierto más Corto (OSPF) Exterior Gateway Protocol (OSPF-EGP) se destaca como un protocolo de enrutamiento interior utilizado dentro de un AS para determinar las mejores rutas entre routers. OSPF-EGP, una extensión de OSPF, permite la redistribución de rutas externas aprendidas a través de BGP dentro del dominio OSPF, facilitando la integración de diferentes tipos de redes en un solo sistema autónomo.

Estos protocolos de enrutamiento exterior son fundamentales para la operatividad de Internet al posibilitar la conectividad entre redes dispersas a nivel global. En la próxima sección, profundizaremos en el Border Gateway Protocol (BGP) y examinaremos detalladamente su funcionamiento y características.

3. PROTOCOLO DE ENCAMINAMIENTO EXTERIOR BGP

3.1. HISTORIA Y EVOLUCIÓN DE BGP

El Border Gateway Protocol (BGP) ha experimentado una evolución significativa desde su concepción hasta su estado actual como el principal protocolo de enrutamiento exterior en Internet. En esta sección, exploraremos la historia y las etapas clave de desarrollo de BGP:

Orígenes de BGP: BGP se originó a principios de la década de 1980 como una respuesta a la necesidad de intercambiar información de enrutamiento entre sistemas autónomos (AS). Surgió como una evolución del Exterior Gateway Protocol (EGP), el primer protocolo de enrutamiento exterior utilizado en Internet [18].

BGP-1 y BGP-2: Las primeras versiones de BGP, conocidas como BGP-1 y BGP-2, se desarrollaron en la década de 1980. Estas versiones iniciales establecieron los fundamentos del protocolo y se centraron en el intercambio de información de enrutamiento básica entre sistemas autónomos [19].

BGP-3 y BGP-4: A medida que Internet continuaba creciendo, surgieron nuevas necesidades y desafíos en el enrutamiento. BGP-3 introdujo mejoras en la capacidad de intercambio de información de enrutamiento y en la eficiencia del protocolo. Fue BGP-4 la versión que se convirtió en el estándar predominante y sigue siendo muy utilizado hoy. BGP-4 introdujo características importantes como la capacidad de soportar direcciones IPv6, la agregación de rutas y la capacidad de anunciar atributos de ruta extendidos [20].

BGP es el protocolo de enrutamiento exterior dominante en Internet y juega un papel fundamental en la interconexión de redes a nivel global. Ha evolucionado para adaptarse a los cambios en la infraestructura de Internet y sigue siendo objeto de desarrollo y mejora continua para abordar nuevos desafíos, como la escalabilidad, la seguridad y el soporte para nuevas tecnologías [21].

Esta breve historia de BGP nos da una visión de cómo ha evolucionado el protocolo en el tiempo y cómo ha desempeñado un papel central en la arquitectura de Internet. En las secciones siguientes, nos adentraremos más en detalle en las características y el funcionamiento de BGP hoy.

3.2. CARACTERÍSTICAS PRINCIPALES DE BGP

El Border Gateway Protocol (BGP) es un protocolo de enrutamiento exterior que se utiliza para intercambiar información de enrutamiento entre sistemas autónomos (AS) en Internet. A continuación, destacaremos algunas de las características principales de BGP:

Protocolo de vector de distancia basado en la política: A diferencia de los protocolos de enrutamiento interior, como RIP o OSPF, que se basan en métricas de distancia para determinar las rutas, BGP utiliza políticas configuradas manualmente por los administradores de red para tomar decisiones de enrutamiento. Esto permite un control granular sobre la selección de rutas y la influencia en el tráfico de red [22].

Soporte para múltiples tipos de atributos de ruta: BGP puede anunciar una amplia gama de atributos de ruta, como la longitud del prefijo, la métrica, el próximo salto, el AS de origen, entre otros. Estos atributos proporcionan información detallada sobre las rutas disponibles y permiten la selección de la ruta óptima según los criterios específicos de la red [23].

Escalabilidad: BGP está diseñado para operar eficientemente en entornos de red a gran escala. Su arquitectura distribuida y su capacidad para anunciar resúmenes de rutas (agregación de rutas) ayudan a reducir la cantidad de información de enrutamiento que los routers deben procesar, lo que contribuye a la escalabilidad de Internet [24].

Soporte para IPv4 e IPv6: BGP es compatible tanto con direcciones IPv4 como IPv6, lo que lo convierte en una herramienta versátil para la interconexión de redes que utilizan ambas versiones del protocolo IP. Esto es crucial cuando la transición hacia IPv6 es cada vez más importante por la escasez de direcciones IPv4 [25].

Establecimiento de sesiones TCP para el intercambio de información: BGP utiliza conexiones TCP (Transmission Control Protocol) para establecer sesiones entre routers vecinos e intercambiar información de enrutamiento. Esto proporciona fiabilidad y garantiza que las actualizaciones de enrutamiento se entreguen de manera segura y sin pérdida de datos [26].

Estas características hacen que BGP sea una herramienta poderosa y fundamental en la infraestructura de Internet. Su flexibilidad, escalabilidad y capacidad para adaptarse a diversos entornos de red lo convierten en el protocolo de elección para la interconexión de sistemas autónomos en todo el mundo.

3.3. FUNCIONAMIENTO BÁSICO DE BGP

El funcionamiento básico del Border Gateway Protocol (BGP) implica el intercambio de información de enrutamiento entre routers que pertenecen a diferentes sistemas autónomos (AS) en Internet. Aquí se describe un resumen de cómo funciona este proceso:

Establecimiento de sesiones BGP: Los routers BGP establecen sesiones TCP (Transmission Control Protocol) entre sí para intercambiar información de enrutamiento. Estas sesiones se establecen entre pares BGP, que pueden ser routers dentro del mismo AS (iBGP) o routers en diferentes AS (eBGP) [27].

Intercambio de rutas: Una vez que se establece una sesión BGP entre dos routers, comienza el intercambio de información de enrutamiento. Cada router envía actualizaciones BGP que contienen información sobre las rutas que conoce y está dispuesto a anunciar. Estas actualizaciones contienen atributos de ruta que describen características como la longitud del prefijo, el próximo salto, la métrica y otros detalles relevantes [28].

Procesamiento de rutas: Cuando un router recibe una actualización BGP de su vecino, procesa la información y toma decisiones sobre las mejores rutas disponibles hacia los destinos anunciados. Estas decisiones se basan en las políticas de enrutamiento configuradas por el administrador de red y en los atributos de ruta recibidos [29].

Selección de la mejor ruta: Después de procesar las actualizaciones de enrutamiento, cada router BGP selecciona la mejor ruta hacia cada destino anunciado. La mejor ruta se hace según criterios, que pueden incluir la longitud del prefijo, la preferencia de la ruta, la medición de la ruta, entre otros [30].

Anuncio de rutas seleccionadas: Una vez que se selecciona la mejor ruta hacia un destino, el router BGP anuncia esta ruta a sus vecinos BGP a través de actualizaciones de enrutamiento salientes. Estas actualizaciones contienen información sobre la ruta seleccionada y los atributos asociados [31].

Mantenimiento de la tabla de enrutamiento BGP: Los routers BGP mantienen una tabla de enrutamiento BGP que contiene información sobre las mejores rutas hacia todos los destinos anunciados por sus vecinos BGP. Esta tabla de enrutamiento se actualiza dinámicamente a medida que se reciben nuevas actualizaciones de enrutamiento y se toman decisiones sobre las rutas óptimas [32].

3.4. TIPOS DE MENSAJES BGP

El Border Gateway Protocol (BGP) utiliza varios tipos de mensajes para intercambiar información de enrutamiento y mantener la conectividad entre los routers que participan en sesiones BGP. Aquí se describen los tipos de mensajes BGP más comunes:

Open (Apertura): Este mensaje se utiliza para iniciar una sesión BGP entre dos routers. Contiene parámetros de configuración, como el número de versión de BGP, el ASN del router remoto y las capacidades admitidas por el router que envía el mensaje. Una vez que ambos routers han intercambiado mensajes Open y han acordado los parámetros de la sesión, se establece la conexión BGP [33].

Update (Actualización): El mensaje Update es el tipo más importante de mensaje BGP, ya que se utiliza para anunciar cambios en la información de enrutamiento. Este mensaje puede contener anuncios de nuevas rutas, retiros de rutas previamente anunciadas y actualizaciones de atributos de ruta. Los routers BGP envían mensajes Update a sus vecinos para informarles sobre las mejores rutas disponibles hacia los destinos anunciados [34].

Keepalive (Mantener vivo): Los mensajes Keepalive se utilizan para mantener la conexión BGP activa entre dos routers. Estos mensajes se envían periódicamente entre los routers para confirmar que la conexión está operativa y para evitar que se cierre debido a inactividad. Si un router no recibe un mensaje Keepalive dentro de un período de tiempo especificado, puede considerar que la conexión BGP ha fallado y tomar medidas para restablecerla [35].

Notification (Notificación): El mensaje Notification se utiliza para informar a un router BGP sobre eventos o condiciones anormales que requieren la terminación de una sesión BGP. Estos eventos pueden incluir errores de configuración, problemas de autenticación, cambios en los parámetros de la sesión o cambios en las capacidades admitidas.
Cuando se recibe un mensaje Notification, el router receptor debe tomar medidas para finalizar la sesión BGP y manejar el evento de acuerdo con las políticas de configuración [36].

4. TOPOLOGÍA Y CONFIGURACIÓN DE BGP

4.1. TOPOLOGÍA TÍPICA DE UN SISTEMA AUTÓNOMO

La topología de un Sistema Autónomo (AS) puede variar considerablemente dependiendo de su tamaño, propósito y configuración específica. Sin embargo, aquí describiremos una topología típica de un AS que se encuentra en la infraestructura de Internet:

Enrutadores de borde (Edge Routers): Estos son los enrutadores que se encuentran en los límites del AS y son responsables de intercambiar información de enrutamiento con otros AS. Los enrutadores de borde suelen tener múltiples conexiones de red, ya sea a otros AS (enrutamiento eBGP) o a otros routers dentro del mismo AS (enrutamiento iBGP). También pueden implementar políticas de filtrado y manipulación de rutas para controlar el tráfico que entra y sale del AS [37].

Enrutadores internos (Internal Routers): Estos enrutadores se encuentran dentro del AS y son responsables de enrutar el tráfico dentro de la red interna del AS. Los enrutadores internos pueden estar conectados a múltiples enrutadores de borde y a otros enrutadores internos, formando una red interna compleja. Utilizan protocolos de enrutamiento interno, como OSPF o IS-IS, para intercambiar información de enrutamiento y calcular las mejores rutas dentro del AS [38].

Servidores y dispositivos de red: Además de los enrutadores, un AS típico puede incluir servidores y dispositivos de red que proporcionan servicios y funcionalidades adicionales. Esto puede incluir servidores de nombres de dominio (DNS), servidores de correo electrónico, servidores web, firewalls, balanceadores de carga, y otros dispositivos especializados para gestionar y proteger el tráfico de red [39].

Puntos de interconexión (Peering Points): Estos son los puntos físicos donde se conectan los enrutadores de borde de un AS con los enrutadores de otros AS para intercambiar tráfico de red. Los puntos de interconexión pueden ser instalaciones de terceros, como puntos de intercambio de Internet (IXP), o conexiones directas entre los centros de datos de los proveedores de servicios de Internet [40].

Políticas de enrutamiento y seguridad: En todo el AS, se implementan políticas de enrutamiento y seguridad para controlar el flujo de tráfico y garantizar la estabilidad y la seguridad de la red. Esto puede incluir políticas de filtrado de rutas, preferencias de enrutamiento, configuración de listas de acceso, autenticación de vecinos BGP, y otras medidas para proteger la red contra ataques y mal uso [41].

4.2. CONFIGURACIÓN BÁSICA DE BGP

La configuración básica de BGP implica varios pasos para establecer y mantener sesiones BGP entre routers y para anunciar y recibir información de enrutamiento. Aquí están los pasos típicos involucrados en la configuración básica de BGP:

Asignación de números de sistema autónomo (ASN): Cada sistema autónomo (AS) debe tener un número de sistema autónomo único (ASN) que lo identifique en Internet. Antes de configurar BGP, se debe asignar un ASN al AS, asegurándose de que sea único y que no entre en conflicto con otros ASN en Internet [42].

Configuración de vecinos BGP: Se configuran las sesiones BGP entre routers vecinos estableciendo conexiones TCP entre ellos. Esto implica especificar la dirección IP del vecino, su ASN y otras configuraciones relacionadas con la autenticación y el establecimiento de la sesión [43].

Intercambio de información de enrutamiento: Una vez que se establecen las sesiones BGP, los routers comienzan a intercambiar información de enrutamiento a través de mensajes BGP. Se pueden configurar políticas de filtrado y redistribución para controlar qué rutas se anuncian y se reciben a través de las sesiones BGP [44].

Configuración de atributos de ruta: Se pueden configurar atributos de ruta para influir en el proceso de selección de ruta y controlar el flujo de tráfico a través de la red. Estos atributos pueden incluir preferencias de ruta, atributos de comunidad, métricas y otras características que afectan cómo se eligen y propagan las rutas [45].

Monitoreo y mantenimiento: Una vez configurado BGP, se debe monitorear y mantener regularmente para garantizar su correcto funcionamiento y resolver cualquier problema que pueda surgir. Esto puede incluir la supervisión del estado de las sesiones BGP, el análisis de los registros de enrutamiento y la implementación de ajustes según sea necesario para optimizar el rendimiento y la estabilidad de la red [46].

Estos son los pasos básicos involucrados en la configuración de BGP en un sistema autónomo. La configuración exacta puede variar según los requisitos específicos de la red y las políticas de enrutamiento del administrador. Es importante tener en cuenta las consideraciones de seguridad y las mejores prácticas al configurar BGP para garantizar la integridad y la seguridad de la red.

4.3. RELACIÓN ENTRE PARES BGP (EBGP Y IBGP)

En la configuración de BGP, se establecen relaciones entre pares BGP para intercambiar información de enrutamiento entre sistemas autónomos (AS). Estas relaciones pueden ser de dos tipos principales: eBGP (External BGP) e iBGP (Internal BGP). Aquí se describe la relación entre pares BGP:

eBGP se refiere a las sesiones BGP establecidas entre routers en sistemas autónomos diferentes.

Los routers que participan en sesiones eBGP intercambian información de enrutamiento entre AS vecinos.

eBGP se utiliza para anunciar rutas hacia destinos fuera del AS local y para recibir rutas anunciadas por otros AS.

Las sesiones eBGP suelen requerir que los routers estén directamente conectados entre sí o a través de una red confiable.

iBGP se refiere a las sesiones BGP establecidas entre routers dentro del mismo sistema autónomo.

Los routers que participan en sesiones iBGP intercambian información de enrutamiento sobre rutas internas dentro del AS.

iBGP se utiliza para propagar rutas aprendidas a través de eBGP a través de toda la red interna del AS.

Las sesiones iBGP suelen requerir una red interna completa y pueden atravesar múltiples enrutadores.

Relación entre eBGP y iBGP:

Es común que un router actúe como un punto de entrada o salida de enrutamiento BGP para un AS.

Cuando se reciben rutas a través de eBGP, se propagan a través de iBGP a otros routers dentro del AS para alcanzar todos los destinos anunciados.

Se deben tomar medidas para evitar problemas de bucles de enrutamiento y para garantizar que todas las rutas aprendidas a través de eBGP se propaguen correctamente a través de iBGP.

En resumen, eBGP se utiliza para intercambiar rutas entre AS vecinos, mientras que iBGP se utiliza para propagar estas rutas dentro del mismo AS. Ambos tipos de relaciones son esenciales para garantizar una conectividad eficiente y coherente en la infraestructura de Internet.

5. POLITICAS DE ENRUTAMIENTO EN BGP

5.1. Concepto de políticas de enrutamiento

Las políticas de enrutamiento en BGP son un conjunto de reglas y criterios que se utilizan para controlar el intercambio de información de enrutamiento entre routers. Estas políticas permiten a los administradores de redes definir cómo se anuncian y se reciben las rutas, lo que les da un control preciso sobre el flujo de tráfico en sus redes.

Las políticas de enrutamiento se basan en varios criterios, como:

- Origen de la ruta: Se puede especificar si se aceptan o rechazan rutas según su origen, como si provienen de un proveedor de Internet específico o de un router interno [47].
- Destino de la ruta: Se puede definir si se anuncia o no una ruta a un destino específico, o si se prefiere una ruta sobre otra para llegar a ese destino [47].
- Atributos de la ruta: Se pueden utilizar los atributos de la ruta, como la preferencia, la métrica o la comunidad, para influir en la selección de la ruta y el flujo de tráfico [47].
- Seguridad: Se pueden implementar políticas de seguridad para proteger la red contra ataques de enrutamiento, como la falsificación de direcciones IP o el secuestro de BGP [47].

5.2. Principios de las políticas de enrutamiento en BGP

Especificidad [48]:

Las políticas de enrutamiento deben ser lo más específicas posible para evitar ambigüedades y conflictos. Se recomienda definir las políticas en base a criterios específicos como:

- **Prefijo de red:** Especificar las redes exactas a las que se aplica la política.
- **Origen de la ruta:** Identificar el origen de la ruta, como un proveedor de Internet específico o un router interno.
- **Destino de la ruta:** Indicar el destino al que se aplica la política, como un rango de direcciones IP o un nombre de host.
- **Atributos de la ruta:** Utilizar atributos como la preferencia, la métrica o la comunidad para diferenciar entre rutas.

Al definir políticas específicas, se reduce la posibilidad de errores y se facilita la gestión de las políticas.

Flexibilidad:

Las políticas de enrutamiento deben ser lo suficientemente flexibles para adaptarse a los cambios en la topología de la red y las necesidades de enrutamiento. Esto se puede lograr mediante:

- **Uso de variables:** Incorporar variables en las políticas para permitir ajustes dinámicos sin necesidad de reconfigurar manualmente las políticas.
- **Definición de políticas condicionales:** Implementar políticas que se activan o desactivan en función de condiciones específicas, como la hora del día o el estado de la red.
- **Uso de herramientas de automatización:** Implementar herramientas que automaticen la creación y gestión de políticas, facilitando la adaptación a cambios en la red.

La flexibilidad en las políticas de enrutamiento permite una mejor adaptación a las necesidades cambiantes de la red.

Seguridad:

Las políticas de enrutamiento deben tener en cuenta la seguridad y proteger la red contra ataques. Algunas medidas de seguridad que se pueden implementar en las políticas de BGP son:

- **Filtrado de rutas:** Denegar el anuncio o la recepción de rutas que provienen de fuentes no confiables o que no son necesarias.
- **Validación de rutas:** Verificar la integridad de las rutas antes de aceptarlas para evitar la falsificación de información de enrutamiento.
- **Autenticación BGP:** Requerir autenticación entre routers BGP para evitar conexiones no autorizadas.
- **Comunidades BGP:** Utilizar comunidades BGP para identificar y controlar el flujo de tráfico sensible.

La implementación de medidas de seguridad en las políticas de BGP ayuda a proteger la red contra ataques e intrusiones.

Simplicidad:

Las políticas de enrutamiento deben ser lo más simples posible para facilitar su comprensión y mantenimiento. Se recomienda:

- **Utilizar un lenguaje claro y conciso:** Evitar el uso de términos técnicos complejos que puedan dificultar la comprensión de las políticas.
- **Organizar las políticas de forma lógica:** Agrupar las políticas por función o por tipo de ruta para facilitar su gestión.
- **Documentar las políticas:** Registrar la información sobre las políticas, como su propósito, los criterios que utilizan y su impacto en la red.

La simplicidad en las políticas de enrutamiento facilita su gestión y reduce la posibilidad de errores.

5.3. Implementación de políticas en BGP

Las políticas de enrutamiento en BGP se pueden implementar de diversas maneras, como:

- Listas de control de acceso (ACL): Se pueden usar ACL para permitir o denegar el tráfico en función de la dirección IP de origen o destino [49].
- Mapas de ruta: Se pueden usar mapas de ruta para modificar los atributos de una ruta antes de anunciarla o recibirla [50].
- Filtros de BGP: Se pueden usar filtros de BGP para controlar qué rutas se anuncian o se reciben [51].
- Comunidades BGP: Se pueden usar comunidades BGP para agrupar rutas y aplicar políticas a grupos específicos de rutas [52].

La elección del método de implementación depende de la complejidad de las políticas y de las características específicas del router BGP.

6. SEGURIDAD EN BGP

6.1 Desafíos de seguridad en el enrutamiento

Los desafíos principales en la seguridad del enrutamiento de las rutas del Border Gateway Protocol, se basan en garantizar la autenticidad de las rutas existentes anunciadas y en la prevención de la manipulación del tráfico maligno en internet.

- Falsificación en el origen: Los atacantes pueden enviar anuncios BGP falsos, que aparentan venir de un sistema autónomo legitimo. Esto puede llevar a una redirección del tráfico por rutas diferentes a las correctas, con los riesgos a la exposición de los datos que esto conlleva.[53]

- Inyección de rutas: Se pueden inyectar rutas falsas en la tabla de enrutamiento BGP de un router para desviar los flujos de paquetes hacia destinos malignos controlados por los atacantes. [53]

- Ataques de inundación: Este tipo de ataques sobrecargan los routers con una elevada cantidad de anuncios BGP inútiles, lo que lleva a una carga en los routers que afecta a su capacidad para enrutar tráfico legitimo.[54]

- Secuestro de rutas: Un atacante puede anunciar de manera fraudulenta una ruta que pertenece a otro sistema autónomo, desviando el tráfico hacia su red. Esto puede acabar en la interceptación de datos o interrupción del servicio.[55]

6.2 Mecanismos de seguridad en BGP

BGP cuenta con varios mecanismos de seguridad para protegerse contra ataques maliciosos y errores inadvertidos. Los principales mecanismos de seguridad del protocolo BGP son los siguientes:

- **Autenticación**: BGP tiene la capacidad de autenticar las actualizaciones de enrutamiento utilizando autenticación basada en contraseñas o utilizando TCP MD5. Esto permite que solo los routers que estén autorizados puedan enviar actualizaciones de enrutamiento. Sin embargo, TCP MD5 ha demostrado ser en ocasiones insegura respecto a ciertos tipos de ataques, y se están desarrollando métodos de autenticación más seguros. [56]

- **Filtrado de rutas**: Los operadores de red pueden configurar filtros para configurar el acceso de determinadas rutas. Esto ayuda a la prevencion de la propagación de rutas falsas, así como controlar todo tráfico entrante y saliente de la red. [57].

- **Route Origin Validation (ROV)**: Verifica la autenticidad de la ruta para prevenir ataques de enrutamiento maliciosos. Esto se logra a traves de la creación y distribución de certificados digitales que se vinculan a las direcciones IP con los sistemas autónomos. [58]

- **Resource Public Key Infrastructure (RPKI)**: Utiliza criptografía de clave pública para asociar direcciones IP con recursos veridicos. Utiliza certificados digitales para validar la autenticidad de las rutas BGP, proporcionando una capa adicional de seguridad contra ataques de enrutamiento. [59].

- **BGPsec (BGP Security Extensions)**: Extensión de BGP que proporciona seguridad a nivel de protocolo a través de firmas digitales en las actualizaciones de enrutamiento. Esto permite verificar la autenticidad de las rutas BGP, proporcionando una protección robusta contra ataques de enrutamiento maliciosos. [60]

6.3 Casos reales de problemas BGP

En este apartado se examinarán casos reales de incidentes en BGP que han tenido un impacto significativo en las operaciones de red a nivel global. Al indagar sobre estos incidentes, se busca comprender las causas, las repercusiones y las posibles soluciones que puedan aplicarse para fortalecer la seguridad y la fiabilidad de BGP en el futuro.

- En 2008, el gobierno de Pakistán ordeno a la compañía Pakistán Telecom bloquear el acceso a YouTube dentro de su territorio, lo que resultó en la introducción de anuncios erróneos en la tabla de enrutamiento global. Estos anuncios incorrectos produjeron que los proveedores de servicios de Internet de todo el mundo redirigieran el tráfico destinado a YouTube a través de Pakistán, lo que provocó una interrupción durante horas al acceso a YouTube globalmente Las consecuencias de este incidente subrayaron la fragilidad de la infraestructura de Internet y resaltaron la necesidad de medidas más rigurosas para garantizar la precisión y la seguridad en la gestión de BGP, así como la importancia de la coordinación y la colaboración internacional en la resolución de incidentes de este tipo.[61]

- En 2017 se produjo una fuga de rutas debido a un error en la configuración de BGP por parte de un proveedor de servicios de Internet en China, que anunció incorrectamente rutas de IP a través de su red. Esto resultó en que una parte significativa de todo el tráfico de Internet estadounidense incluidas algunas agencias gubernamentales, fuera desviado hacia China, produciendo una latencia adicional el rendimiento y afectando a la seguridad de las comunicaciones. Las consecuencias de este incidente destacaron la necesidad de una mayor vigilancia y medidas de seguridad en la gestión de BGP, tanto como resaltar la importancia de implementar protocolos de autenticación y verificación para disminuir la posibilidad de que ocurran incidentes similares de desvíos maliciosos o accidentales en la infraestructura crítica de Internet.[62]

7. CASOS DE ESTUDIO Y EJEMPLOS PRÁCTICOS DE BGP

7.1 Comandos para un Router BGP

La configuración y administración adecuada de BGP requiere el dominio de una variedad de comandos para diagnosticar y solucionar problemas, verificar el estado de la red y realizar ajustes en la configuración.

Los siguientes comandos son indispensables para trabajar con Routers BGP. Estos comandos proporcionan información sobre el estado de la vecindad BGP, las rutas aprendidas y permiten realizar cambios en la configuración según sea necesario.

- **show ip bgp**: Muestra la tabla BGP, pudiendo visualizar las rutas aprendidas y el estado de la vecindad BGP.[63]

- **show ip bgp neighbors**: Muestra informacion sobre los vecinos BGP, incluyendo el estado de la vecindad, los tiempos de retardo y la dirección IP del vecino. [63]

- **neighbor [IP_address] remote-as [AS_number]**: Establece la asociación BGP con un vecino especificado utilizando el número de sistema autónomo remoto. [63]

- **neighbor [IP_address] next-hop-self**: Fuerza al router a anunciar su propia dirección IP como el siguiente salto para las rutas enviadas al vecino BGP. [63]

- **neighbor [IP_address] route-map [route-map_name] in/out**: Aplica un route-map para filtrar o modificar las rutas BGP entrantes (in) o salientes (out) de un vecino BGP específico. [63]

- **neighbor [IP_address] ebgp-multihop [ttl]**: Permite la configuración de una sesión BGP eBGP (BGP entre sistemas autónomos diferentes) con un vecino que no está fisicamente conectado a través de un salto, especificando el número de saltos TTL (Time-To-Live). [63]

8. CONCLUSIONES

El estudio del Protocolo de Encaminamiento Exterior BGP ha proporcionado una comprensión más profunda de cómo se intercambia la información de enrutamiento entre sistemas autónomos en Internet. A través de este trabajo, hemos identificado varias conclusiones importantes:

- **Importancia de BGP**: BGP desempeña un papel fundamental en la infraestructura de Internet al permitir la interconexión de redes a nivel global. Su capacidad para tomar decisiones de enrutamiento basadas en políticas lo convierte en un componente esencial para dirigir el tráfico de manera eficiente y segura.

- **Flexibilidad y escalabilidad**: BGP ofrece una gran flexibilidad y escalabilidad, lo que lo hace adecuado para entornos de red a gran escala como Internet. Su capacidad para adaptarse a diversos requisitos de enrutamiento y políticas lo convierte en una herramienta versátil para la interconexión de sistemas autónomos.

- **Desafíos de configuración y mantenimiento**: Aunque BGP ofrece muchas ventajas, también presenta desafíos significativos en términos de configuración y mantenimiento. La correcta configuración de políticas de enrutamiento y la gestión de la seguridad son aspectos críticos que los administradores de red deben tener en cuenta al implementar BGP en sus redes.

- **Seguridad y confiabilidad**: La seguridad es un aspecto crucial en el diseño y la implementación de BGP. Los protocolos de seguridad, como la autenticación y la firma de rutas, son necesarios para proteger las sesiones BGP y garantizar la integridad de la información de enrutamiento.

En resumen, el Protocolo de Encaminamiento Exterior BGP es un componente vital de Internet que permite la conectividad global y el intercambio eficiente de información de enrutamiento entre sistemas autónomos. Sin embargo, su implementación exitosa requiere un enfoque cuidadoso y una comprensión profunda de sus características y desafíos asociados.

9. BIBLIOGRAFÍA

[1] Wikipedia - Border Gateway Protocol: https://en.wikipedia.org/wiki/Border_Gateway_Protocol - Accedido el 25/04/2024

[2] Wikipedia - Border Gateway Protocol: https://en.wikipedia.org/wiki/Border_Gateway_Protocol - Accedido el 26/04/2024

[3] AWS - ¿Qué es el Border Gateway Protocol (BGP)?: https://aws.amazon.com/what-is/border-gateway-protocol/ - Accedido el 26/04/2024

[4] Juniper Networks - Introducción a BGP: https://www.juniper.net/documentation/us/en/software/junos/bgp/topics/topic-map/bgp-overview.html - Accedido el 26/04/2024

[5] Wikipedia – Sistema autónomo: https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo - Accedido el 26/04/2024

[6] Cisco - Configuración de una red BGP básica: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/configuring-a-basic-bgp-network.html - Accedido el 26/04/2024

[7] Cloudflare Blog - Etiqueta BGP: https://blog.cloudflare.com/tag/bgp - Accedido el 26/04/2024

[8] Wikipedia – Enrutamiento: https://es.wikipedia.org/wiki/Encaminamiento - Accedido el 26/04/2024

[9] Wikipedia – Sistema autónomo: https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo - Accedido el 26/04/2024

[10] Wikipedia - Enrutamiento en Internet: https://en.wikipedia.org/wiki/Routing - Accedido el 26/04/2024

[11] Cisco - Conceptos básicos de enrutamiento: https://www.cisco.com/c/en/us/products/routers/what-is-routing.html - Accedido el 26/04/2024

[12] Microsoft - ¿Qué es el enrutamiento?: https://learn.microsoft.com/en-us/azure/route-server/ - Accedido el 26/04/2024

[13] Juniper Networks - Introducción a BGP: https://datatracker.ietf.org/doc/html/rfc827 - Accedido el 26/04/2024

[14] Cloudflare Blog - Etiqueta BGP: https://blog.cloudflare.com/tag/bgp - Accedido el 26/04/2024

[15] Cloudflare Blog – Sistema autónomo: https://www.cloudflare.com/es-es/learning/network-layer/what-is-an-autonomous-system/ - Accedido el 26/04/2024

[16] Feinler, J., & Network Working Group. (1982). "Exterior Gateway Protocol (EGP)." IETF RFC 827.: https://www.cloudflare.com/es-es/learning/network-layer/what-is-an-autonomous-system/ - Accedido el 26/04/2024

[17] Mills, D. (1985). "Exterior Gateway Protocol Formal Specification." IETF RFC 904. - https://datatracker.ietf.org/doc/rfc904/ - Accedido el 26/04/2024

[18] Rekhter, Y., & Li, T. (2006). A border gateway protocol 4 (BGP-4). RFC 4271. - https://datatracker.ietf.org/doc/html/rfc4271 - Accedido el 26/04/2024

[19] Rekhter, Y., & Li, T. (1989). A Border Gateway Protocol (BGP). RFC 1105 - https://tools.ietf.org/html/rfc1105 - Accedido el 26/04/2024

[20] Fuller, V., Li, T., Yu, J., & Varadhan, K. (1997). Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. RFC 1519 - https://datatracker.ietf.org/doc/html/rfc1519 - Accedido el 26/04/2024

[21] Huston, G. (2003). BGP scaling considerations. RFC 3221 - https://datatracker.ietf.org/doc/html/rfc3221 - Accedido el 26/04/2024

[22] Wikipedia – Sistema autónomo: https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo - Accedido el 26/04/2024

[23] Rekhter, Y., & Li, T. (2006). A border gateway protocol 4 (BGP-4). RFC 4271. https://tools.ietf.org/html/rfc4271 - Accedido el 26/04/2024

[24] Bates, T., Chandra, R., Katz, D., & Rekhter, Y. (1996). Multiprotocol extensions for BGP-4. RFC 2283. https://tools.ietf.org/html/rfc2283 - Accedido el 26/04/2024

[25] Huston, G. (2003). BGP scaling considerations. RFC 3221. https://tools.ietf.org/html/rfc3221 - Accedido el 26/04/2024

[26] Heitz, J., & Harrison, R. (2005). BGP Route Reflection - An alternative to full mesh IBGP. RFC 4456. https://tools.ietf.org/html/rfc4456 - Accedido el 26/04/2024

[27] Wikipedia – Sistema autónomo: https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo - Accedido el 26/04/2024

[28] Rekhter, Y., & Li, T. (2006). A border gateway protocol 4 (BGP-4). RFC 4271. https://tools.ietf.org/html/rfc4271 - Accedido el 26/04/2024

[29] Bates, T., & Rekhter, Y. (1995). Border Gateway Protocol (BGP) route reflection. RFC 4456. https://tools.ietf.org/html/rfc4456 - Accedido el 26/04/2024

[30] Chen, E., & Rekhter, Y. (1990). Application of the border gateway protocol in the internet. RFC 1164. https://tools.ietf.org/html/rfc1164 - Accedido el 26/04/2024

[31] Villamizar, C. (1994). BGP4 case studies, historical perspectives, and future directions. RFC 1774. https://tools.ietf.org/html/rfc1774 - Accedido el 26/04/2024

[32] Lougheed, K., & Rekhter, Y. (1993). A border gateway protocol 3 (BGP-3). RFC 1267. https://tools.ietf.org/html/rfc1267 - Accedido el 26/04/2024

[33] Wikipedia – Sistema autónomo: https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo - Accedido el 26/04/2024

[34] Rekhter, Y., & Li, T. (2006). A border gateway protocol 4 (BGP-4). RFC 4271. https://tools.ietf.org/html/rfc4271 - Accedido el 26/04/2024

[35] Chen, E., & Rekhter, Y. (1990). Application of the border gateway protocol in the internet. RFC 1164. https://tools.ietf.org/html/rfc1164 - Accedido el 26/04/2024

[36] Villamizar, C. (1994). BGP4 case studies, historical perspectives, and future directions. RFC 1774. https://tools.ietf.org/html/rfc1774 - Accedido el 26/04/2024

[37] Wikipedia – Sistema autónomo: https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo - Accedido el 26/04/2024

[38] Rekhter, Y., & Li, T. (2006). A border gateway protocol 4 (BGP-4). RFC 4271. https://tools.ietf.org/html/rfc4271 - Accedido el 26/04/2024

[39] Bates, T., & Rekhter, Y. (1995). Border Gateway Protocol (BGP) route reflection. RFC 4456. https://tools.ietf.org/html/rfc4456 - Accedido el 26/04/2024

[40] Chen, E., & Rekhter, Y. (1990). Application of the border gateway protocol in the internet. RFC 1164. https://tools.ietf.org/html/rfc1164 - Accedido el 26/04/2024

[41] Villamizar, C. (1994). BGP4 case studies, historical perspectives, and future directions. RFC 1774. https://tools.ietf.org/html/rfc1774 - Accedido el 26/04/2024

[42] Wikipedia – Sistema autónomo: https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo - Accedido el 26/04/2024

[43] Rekhter, Y., & Li, T. (2006). A border gateway protocol 4 (BGP-4). RFC 4271. https://tools.ietf.org/html/rfc4271 - Accedido el 26/04/2024

[44] Bates, T., & Rekhter, Y. (1995). Border Gateway Protocol (BGP) route reflection. RFC 4456. https://tools.ietf.org/html/rfc4456 - Accedido el 26/04/2024

[45] Chen, E., & Rekhter, Y. (1990). Application of the border gateway protocol in the internet. RFC 1164. https://tools.ietf.org/html/rfc1164 - Accedido el 26/04/2024

[46] Villamizar, C. (1994). BGP4 case studies, historical perspectives, and future directions. RFC 1774. https://tools.ietf.org/html/rfc1774 - Accedido el 26/04/2024

[47] Descripción general de BGP: https://www.juniper.net/documentation/mx/es/software/junos/bgp/topics/topic-map/bgp-overview.html - Accedido el 26/04/2024

[48] Internet Engineering Task Force (IETF): - https://datatracker.ietf.org/doc/html/rfc1105 - Accedido el 26/04/2024

[49] Listas de Control de Acceso (ACL): Funcionamiento y Creación - https://ccnadesdecero.es/listas-control-acceso-acl-router-cisco/ - Accedido el 26/04/2024

[50] Route-Maps para la Configuración de Redistribución de IP Routing Protocol - https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/49111-route-map-bestp.html - Accedido el 26/04/2024

[51] Tránsitos y filtros en BGP - https://www.eduardocollado.com/2022/10/03/transitos-y-filtros-en-bgp/ - Accedido el 26/04/2024

[52] BGP Communities - https://www.alferez.es/redes/conectividad/bgp-communities/ - Accedido el 26/04/2024

[53] Cloudflare Blog - ¿Que es el secuestro de BGP? : https://www.cloudflare.com/es-es/learning/security/glossary/bgp-hijacking/ - Accedido el 23/04/2024

[54] BGP with BGPsec : https://ieeexplore.ieee.org/abstract/document/8594708 - Accedido el 23/04/2024

[55] ¿Cloudflare Blog - ¿Que es el secuestro de BGP? : https://www.cloudflare.com/es-es/learning/security/glossary/bgp-hijacking/ - Accedido el 24/04/2024

[56] Descripcion de la autenticación de enrutador para BGP : https://www.juniper.net/documentation/mx/es/software/junos/bgp/topics/topic-map/bgp_security.html#id-understanding-router-authentication-for-bgp - Accedido el 24/04/2024

[57] Descripcion general del filtrado de rutas : https://docs.megaport.com/es/mcr/route-filtering/ - Accedido el 25/04/2024

[58] BGP origin validation : https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/bgp-origin-validation/ - Accedido el 26/04/2024

[59] RPKI - The required cryptographic upgrade to BGP routing : https://blog.cloudflare.com/rpki - Accedido el 26/04/2024

[60] BGP security: the BGPsec protocol : https://www.noction.com/blog/bgpsec-protocol - Accedido el 27/04/2024

[61] How Pakistan knocked YouTube offline (and how to make sure it never happens again) : https://www.cnet.com/culture/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/

[62] Oracle confirms China Telecom internet traffic 'misdirections' : https://www.zdnet.com/article/oracle-confirms-china-telecom-internet-traffic-misdirections/

[63] BGP commands : https://docs.nvidia.com/networking/display/onyxv3104302/bgp+commands#src-132451846_BGPCommands-neighborexport-localpref