Red Grupo de Trabajo d. Meyer
Petición de Comentarios: 4274 K. Patel
Categoría: informativos Cisco Systems

Enero 2006

BGP-4 Protocolo de Análisis

Condición de este memo

Este memorándum proporciona información para la comunidad de Internet. No
No especifica un estándar de Internet de ningún tipo. Distribución de este
Memo es ilimitada.

Aviso de Copyright

Resumen

El propósito de este informe es la forma en que el documento de requisitos para la
Publicación de un protocolo de enrutamiento de Internet como un Proyecto de Norma han
Sido satisfechos por Border Gateway Protocolo de la versión 4 (BGP-4).

En este informe se cumple el requisito de que "el segundo informe", como
Describe en la Sección 6,0 de RFC 1264. Con el fin de cumplir la
Requisito, en este informe se aumenta el RFC 1774 y se resumen los principales
Características de BGP-4, así como analiza el protocolo con respecto a
La ampliación y el rendimiento.

Tabla de contenidos

1. Introducción

BGP-4 es un sistema autónomo entre los protocolos de enrutamiento diseñado para TCP / IP internets. Versión 1 de BGP-4 fue publicado en [RFC1105]. Desde entonces, BGP versiones 2, 3, y 4 se han desarrollado. Versión 2 Se documenta en [RFC1163]. Versión 3 está documentado en [RFC1267]. La versión 4 está documentado en [BGP4] (versión 4 de BGP en adelante se Denominado BGP). Los cambios entre las versiones se explican en Apéndice A de [BGP4]. Posibles aplicaciones de BGP en Internet Están documentadas en [RFC1772].

BGP introducido apoyo a Classless Inter-Domain Routing (CIDR) [RFC1519]. Dado que las versiones anteriores de BGP carecían de apoyo a la CIDR, que se consideran obsoletos e inservibles en la actual Internet.

El propósito de este informe es la forma en que el documento de requisitos para la Publicación de un protocolo de enrutamiento de Internet como un Proyecto de Norma han Sido satisfechos por Border Gateway Protocolo de la versión 4 (BGP-4).

En este informe se cumple el requisito de que "el segundo informe", como Describe en la Sección de 6,0 [RFC1264]. Con el fin de cumplir la Requisito, en este informe se aumenta [RFC1774], y un resumen de las principales Características de BGP-4, así como analiza el protocolo con respecto a La ampliación y el rendimiento.

2. Características clave y Algoritmos de BGP

En esta sección se resumen las principales características y los algoritmos de BGP. BGP Es un sistema autónomo entre los protocolos de enrutamiento, que está diseñado ser Utilizado entre múltiples sistemas autónomos. BGP asume que el enrutamiento Dentro de un sistema autónomo es realizado por una intra-sistema autónomo Protocolos de enrutamiento. BGP también asume que se encaminan paquetes de datos de Fuente hacia el destino independiente de la fuente. BGP no Hacer ninguna hipótesis sobre intra-sistema autónomo protocolos de enrutamiento Desplegados dentro de los distintos sistemas autónomos. En concreto, BGP No requiere de todos los sistemas autónomos para administrar el mismo dentro de la Sistema autónomo de enrutamiento de protocolo (es decir, protocolo de pasarela interior O IGP).

Por último, señalar que BGP es un verdadero inter-sistema autónomo de enrutamiento Protocolo, y, como tal, no impone limitaciones a la subyacente Topología de interconexión de los sistemas autónomos. La información Intercambiados a través de BGP es suficiente para construir un gráfico de autónomos Los sistemas de conectividad de los bucles de enrutamiento que pueden ser podadas, y muchos

Enrutamiento de las decisiones políticas en el nivel de sistema autónomo puede ser
Forzadas.

2,1. Características clave

Las características fundamentales del mismo son la noción de atributos camino
Y la agregación de la Red de Información Layer Reachability (NLRI).

Ruta de proporcionar atributos BGP con flexibilidad y extensibilidad. Sendero
Atributos son bien conocidos o facultativo. El crédito para
Atributos opcionales permite la experimentación que puede implicar un grupo
De los routers BGP sin afectar el resto de la Internet. Nueva
Atributos opcionales se pueden añadir al protocolo de la misma manera
Que se añaden nuevas opciones para, por ejemplo, el protocolo Telnet
[RFC854].

Uno de los atributos más importantes es el camino Autónoma Sistema
Camino, o AS_PATH. A medida que la información atraviesa la accesibilidad
Internet, esta información (AS_PATH) se ve aumentada por la lista de
Sistemas autónomos que se han recorrido hasta el momento, la formación de la
AS_PATH. El AS_PATH permite sencillo de la represión
Bucle de información de enrutamiento. Además, el AS_PATH sirve de
Versátil y potente mecanismo para la elaboración de políticas basadas en el enrutamiento.

BGP mejora el atributo AS_PATH incluir conjuntos de autónomo
Sistemas así como a través de las listas AS_SET atributo. Este ampliado
Formato permite agregado generado rutas para transportar la información sobre la ruta

De las rutas más específica utilizada para generar la suma. Es
Hay que señalar, sin embargo, que a partir de este escrito, rara vez son AS_SETs
Utilizados en la Internet [ROUTEVIEWS].

2,2. Algoritmos BGP

BGP utiliza un algoritmo que no es ni una pura distancia de vectores
Algoritmo o un vínculo estado puro algoritmo. En lugar de ello, utiliza un
Vector modificado distancia algoritmo, denominado "Ruta de Vector"
Algoritmo. Este algoritmo utiliza información de la ruta para evitar la tradicional
Vector distancia problemas. Cada ruta BGP pares dentro de la información
Acerca de la información de la ruta con destino a ese destino.
Ruta de la información (también conocido como AS_PATH información) se almacena dentro de
El atributo AS_PATH en BGP. La información de la ruta en la ayuda a BGP
AS detección de bucles, lo que permite seleccionar a los oradores BGP loop-libre
Rutas.

BGP utiliza una estrategia de actualización incremental para ahorrar ancho de banda y
Potencia de procesamiento. Esto es, después del intercambio inicial completa
Información de enrutamiento, un par de routers BGP intercambios sólo los cambios
De la información. Este tipo de diseño requiere de la actualización incremental

Transporte fiable entre un par de routers BGP para funcionar
Correctamente. BGP resuelve este problema mediante el uso de TCP para fiables
Transporte.

Además de actualizaciones incrementales, BGP ha añadido el concepto de
Ruta de agregación de modo que la información sobre los grupos de destinos
Que utilizan la dirección jerárquica cesión (por ejemplo, CIDR) puede ser
Agregadas y enviadas por una sola Network Layer Reachability (NLRI).

Por último, señalar que BGP es un protocolo autónomo. Es decir, BGP
Especifica cómo se intercambia información de enrutamiento, tanto entre BGP
Oradores de diferentes sistemas autónomos, y entre los oradores BGP
Dentro de un mismo sistema autónomo.

2,3. BGP máquina de estados finitos (FSM)

BGP El FSM es un conjunto de reglas que se aplica a un conjunto de oradores BGP
De los compañeros configurado para la operación de BGP. Una aplicación BGP
BGP requiere que un orador debe conectarse y escuchar en el puerto TCP
179 para la aceptación de las nuevas conexiones BGP de sus pares. El BGP
Finitos Estado Machine, o FSM, debe ser iniciado y mantenido por
Cada uno de los nuevos entrantes y salientes de la conexión entre pares. Sin embargo, en cons
tante
Operación estatal, sólo habrá un BGP FSM por conexión por
Pares.

Puede haber un breve período de tiempo durante el cual un BGP puede tener separados los par
es
Conexiones de entrada y salida resulta en la creación de dos
Diferentes BGP FSMs relativas a un compañero (en vez de uno). Esto puede ser
Resueltas por la siguiente conexión BGP colisión normas definidas en
La especificación [BGP4].

El FSM ha BGP los siguientes estados asociados a cada uno de sus
Compañeros:

IDLE: Estado cuando BGP pares niega cualquier conexiones entrantes.

CONNECT: Estado en el que los pares BGP está a la espera de su TCP
Se completará la conexión.

ACTIVO: Estado en el que los pares BGP está tratando de adquirir un compañero
Escuchando y aceptando conexión TCP.

OPENSENT: BGP está a la espera de los pares OPEN mensaje de su pares.

OPENCONFIRM: BGP pares está a la espera de la notificación o KEEPALIVE
Mensaje de sus pares.

ESTABLECIDO: BGP relación se establece entre pares y de los intercambios

UPDATE, la notificación, y con sus mensajes KEEPALIVE
Pares.

Hay una serie de eventos BGP que operan en el mencionado
Estados de la FSM para BGP BGP compañeros. Apoyo de estos eventos es BGP
Ya sea obligatorio o facultativo. Estos acontecimientos se desencadenan por la
Protocolo de la lógica como parte de la BGP o usando un operador
Intervención a través de una interfaz de configuración para el protocolo BGP.

Estos eventos son de BGP siguientes tipos: Opcional acontecimientos vinculados a
Opcional reunión atributos, Acto Administrativo, Temporizador Eventos, TCP
Conexión basada en eventos, y BGP Mensaje basada en eventos. Tanto el FSM
Y la BGP acontecimientos se explican en detalle en [BGP4].

3. Capacidades BGP

La capacidad mecanismo BGP [RFC3392] proporciona una fácil y flexible
Manera de introducir nuevas características en el protocolo. En particular,
La capacidad BGP BGP mecanismo permite que un altavoz para anunciar a sus
Compañeros durante el arranque diversas opciones de funcionamiento apoyados por el
Orador (y recibir información análoga de la pares). Este
Permite a la base de BGP para contener sólo la funcionalidad esencial, en tanto que
Proporcionar un mecanismo flexible de extensiones de protocolo de señalización.

4. Peer oscilaciones persistentes BGP

Cada vez que un orador BGP detecta un error en una relación entre iguales,
Se apaga la computadora cambia su estado al FSM IDLE. BGP orador
Requiere un evento de inicio de volver a iniciar una relación entre iguales inactivo. Si
El error sigue siendo persistente y BGP orador genera un evento de inicio
Automáticamente, entonces puede dar lugar a la persistencia de los pares el batido.
Aunque pares oscilación se considera de gran propagación en BGP
Implementaciones, los métodos para la prevención de las oscilaciones persistentes entre homól
ogos
Están fuera del ámbito de la especificación base de BGP.

5. Directrices para la aplicación de

Un robusto BGP aplicación es "la conservación de los trabajos". Esto significa que si
El número de prefijo es limitada, arbitrariamente altos niveles de ruta
Cambio puede ser tolerada. Los altos niveles pueden ser toleradas con limitada
Impacto en la ruta de la convergencia de cambios ocasionales en general
Estable rutas.

Un robusto aplicación de BGP debe tener las siguientes
Características:

1. Es capaz de funcionar en casi arbitrariamente altos niveles de
   Colgajo ruta sin perder peerings (no se envía

Keepalives) o perder otro protocolo adjacencies como resultado
BGP de carga.

2. La inestabilidad de un subconjunto de las rutas no deben afectar a la ruta
   Transmisión de anuncios o asociados con el conjunto de estable
   Rutas.

3. La inestabilidad no debe ser causada por otros jóvenes con altos niveles de
   La inestabilidad o con diferente velocidad de la CPU o de carga que en el resultado
   Más rápido o más lento el procesamiento de rutas. Estos compañeros inestable
   Debería tener un impacto limitado en el tiempo para la convergencia
   Rutas en general, estable.

Numerosos robusto existen implementaciones de BGP. La creación de un sólido
Aplicación no es una cuestión trivial, pero es claramente alcanzable.

6. BGP características de rendimiento y escalabilidad

En esta sección, proporcionamos "orden de magnitud" respuestas a la
Cuestiones de vínculo cuánto ancho de banda, router memoria y la CPU del router
Ciclos BGP se consumen en condiciones normales. En particular,
Se dirigirá a la escalabilidad de BGP y sus limitaciones.

6,1. Link utilización de la CPU y el ancho de banda

Inmediatamente después de la configuración inicial de conexión BGP, BGP compañeros
Juegos completos intercambio de información de enrutamiento. Si denotamos la
Número total de vías en la Internet como N, la trayectoria total
Atributos (para todas las rutas N) recibidas de un compañero como A, y asumir
Que las redes están distribuidas de manera uniforme entre los autónomos
Sistemas, el peor de los casos, cantidad de ancho de banda consumido durante el
Intercambio inicial entre un par de oradores BGP (P) es

BW = O ((N + A) * P)

BGP-4 se creó específicamente para reducir el tamaño del conjunto de NLRI
Entradas, que ha de ser ejecutado e intercambiada por los routers frontera.
El esquema de agregación, se definen en el [RFC1519], se describen los
Proveedor basado en la agregación sistema en uso hoy en el Internet.

Debido a las ventajas de la publicidad global de unos pocos grandes bloques
(En lugar de muchas pequeñas clases individuales basados en las redes), es
Difícil estimar la reducción en el ancho de banda real y
Procesamiento que BGP-4 ha proporcionado más de BGP-3. Si nos limitamos
Enumerar todos los agregados en sus bloques individuales, la clase de base
Redes, que no tendrían en cuenta "muerto" el espacio que se ha
Reservado para una futura ampliación. El mejor indicador para determinar la
BGP éxito de la agrupación se muestra el número de entradas en NLRI
El mundo conectados a Internet hoy en día, y compararlo con las tasas de crecimiento

Que se proyectaron antes de BGP se desplegó.

En el momento de escribir esto, el conjunto de rutas a cargo exterior
Por BGP es de aproximadamente 134000 entradas de la red [ROUTEVIEWS].

6.1.1. Utilización de CPU

Una importante y fundamental característica de BGP BGP es que la CPU
Utilización sólo depende de la estabilidad de su red que
Se refiere a BGP en términos de mensaje BGP UPDATE anuncios. Si el
BGP red es estable, todos los routers BGP dentro de su red están en
El estado de equilibrio. Así, el único enlace del router de ancho de banda y CPU
Ciclos consumidos por BGP se deben al intercambio de la BGP KEEPALIVE
Mensajes. El KEEPALIVE sólo se intercambian mensajes entre pares.
El sugirió frecuencia de los intercambios es de 30 segundos. El KEEPALIVE
Son mensajes muy breves (19 octetos) y prácticamente no requieren
Procesamiento. Como resultado, el ancho de banda consumido por el KEEPALIVE
Mensajes es de unos 5 bits / seg. Confirma que la experiencia operacional
Los gastos generales (en términos de ancho de banda y CPU) asociados a la
KEEPALIVE mensajes deben ser vistos como insignificantes.

Durante los períodos de inestabilidad de red, routers BGP dentro de la red
Están generando actualizaciones de enrutamiento que son intercambiados usando el BGP
UPDATE mensajes. Los mayores gastos generales por cada mensaje aparece UPDATE
UPDATE cuando cada mensaje contiene una única red. Debería
Que señalar que, en la práctica, los cambios de itinerario tienen una fuerte
Localidad con respecto a los atributos de la ruta. Esto es, las rutas que
Cambio es probable que tengan atributos comunes de ruta. En este caso,
Múltiples redes pueden agruparse en un único mensaje UPDATE, por lo tanto,
Reducir significativamente la cantidad de ancho de banda necesario (véase también
Apéndice de F.1 [BGP4]).

6.1.2. Requisitos de memoria

Para cuantificar el peor de los casos, los requisitos de memoria para BGP, la denotamos
Número total de las redes en Internet como N, la media distancia AS
De la Internet como M (distancia en el nivel de un sistema autónomo,
Expresada en términos del número de sistemas autónomos), el total
Número de rutas como única AS A. Entonces, la peor de los casos la memoria
Necesarios (MR) puede expresarse como

MR = O (N + (M * A))

Debido a una media distancia AS M es un movimiento lento de la función
Interconectividad ("meshiness") de Internet, en la práctica
Efectos de la peor de los casos, los requisitos de memoria del router están en el orden
Del número total de las redes en la Internet multiplicado por el
Número de pares que el sistema local es intercambio con. Esperamos
Que el número total de las redes en Internet crecerá más

Más rápido que el promedio de sus pares por router. Como resultado de ello,
BGP-ampliar la memoria de las propiedades son linealmente relacionado con el total
Número de redes en Internet.

La siguiente tabla ilustra los requisitos de memoria típica de un
Router corriendo BGP. Nos indican el número medio de las rutas
Anunciados por cada uno de los pares como N, el número total de caminos como único AS
A, la media distancia como de la Internet como M (distancia en el nivel
De un sistema autónomo, expresada en términos del número de
Sistemas autónomos), el número de bytes requerido para almacenar una red
Como R, y el número de bytes requerido para almacenar un AS en un camino AS
Como P. Se supone que cada red está codificado como cuatro bytes, cada uno de ellos
AS está codificado como dos bytes, y cada uno es, a través de las redes de algunos
Fracción de todos los compañeros (# BGP peers / por netas). A los efectos de la
Estimaciones de aquí, vamos a calcular MR = (((N * R) + (M * A) * P) * S).

# Redes de media distancia (N)	AS # (M)	# ASes BGP peers (A)	/ Memory neto por Req (P) (MR)
100000	20	3000	20 10400000
100000	20	15000	20 20000000
120000	10	15000	100 78000000
140000	15	20000	100 116000000

BGP en el análisis de la memoria de necesidades, nos centramos en el tamaño de la
BGP RIB mesa (haciendo caso omiso de los detalles de la ejecución). En particular,
Obtener límites superior para el tamaño de la tabla BGP RIB. Por ejemplo,
En el momento de escribir esto, el BGP RIB tablas de una típica columna vertebral
Router llevar del orden de 120.000 entradas. Dado este número, una
Cabe preguntarse si sería posible tener un sistema funcional router
Con una tabla que contiene 1.000.000 entradas. Evidentemente, la respuesta a
Esta cuestión está más relacionada con la forma en BGP es aplicado. Un robusto
BGP con una aplicación razonable de la CPU y la memoria no deben tener
Cuestiones de la ampliación a los límites.

7. Política Expressiveness BGP y sus Consecuencias

BGP es el único entre los protocolos de enrutamiento IP desplegadas en que se enrutamiento
Determina utilizando semánticamente rica políticas de enrutamiento. Aunque
Enrutamiento de las políticas son generalmente el primer BGP cuestión que llega a una
Operador de red la mente, es importante señalar que los idiomas
Y técnicas de enrutamiento BGP para especificar las políticas no son parte de
La especificación de protocolo (ver [RFC2622] para un ejemplo de tal
Política de la lengua). Además, la especificación contiene pocas BGP
Restricciones, explícitas o implícitas, sobre la política de enrutamiento idiomas.
Estos idiomas han sido desarrollados por los proveedores y se han
Evolucionado a través de la interacción con los ingenieros de red en un entorno
Falta de proveedores independientes de las normas.

La complejidad de las configuraciones típicas BGP, por lo menos en proveedor

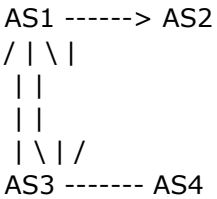
Redes, ha aumentado de manera constante. Router vendedores normalmente
Proporcionar cientos de comandos especiales para su uso en la configuración de
BGP, y este comando conjunto está en continua expansión. Por ejemplo, BGP
Comunidades [RFC1997] permiten a los escritores de política selectiva adjuntar etiquetas
A las rutas y que las use para señal de la política de información a otros
Habla routers BGP. Muchos proveedores permiten que los clientes, y, a veces,
Pares, el envío de las comunidades que determinan el alcance y la preferencia de
Sus rutas. Debido a estos acontecimientos, la tarea de escribir BGP
Configuraciones tiene cada vez más aspectos relacionados con open -
Terminó la programación. Esto ha permitido que los operadores de red para codificar
Complejo de las políticas para hacer frente a muchas situaciones imprevistas, y
Ha abierto la puerta a una gran cantidad de creatividad y

En la experimentación de políticas de enrutamiento. Esta política de flexibilidad es una
De las principales razones por BGP es tan bien al comercial
Entorno de la actual Internet.

Sin embargo, esta rica expresividad política ha llegado a un costo que es
A menudo no se reconoce. En particular, es posible construir
Enrutamiento definen las políticas a nivel local que puede llevar a la divergencia de protocolo
Inesperado y global de enrutamiento como anomalías (no deseados) no
Determinismo. Si el que interactúan las políticas que causan este tipo de anomalías son
Definirse de diferentes sistemas autónomos, estos problemas pueden ser
Muy difícil de depurar y corregir. En las siguientes secciones,
Describir dos de esos casos relativos a la existencia (o falta de ella)
De rutas estables.

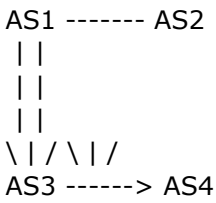
7,1. La existencia de la única estable rutas

Uno puede fácilmente construir conjuntos de las políticas para los que no pueden BGP
Garantía de que son únicas rutas estables. Esto queda ilustrado por
El siguiente ejemplo sencillo. Examinar cuatro Autónoma Systems, AS1,
AS2, AS3, y AS4. AS1 y AS2 son iguales, y que proporcionan el tránsito
Para AS3 y AS4, respectivamente. Supongamos AS3 proporciona tránsito para AS4
(En este caso, AS3 es un cliente de AS1, AS4 y es un multihomed
Cliente de ambos AS2 y AS3). AS4 lo desea, puede utilizar el enlace a AS3
Como una "copia de seguridad", y envía AS3 valor de una comunidad que ha AS3
Configurado para bajar la preferencia de AS4 las rutas a un nivel inferior
Que aguas arriba de su proveedor, AS1. La intención de "copia de seguridad de ruta" para
AS4 se ilustra aquí:



Es decir, el AS3-AS4 vínculo está destinado a ser utilizado solamente cuando el AS2 -

AS4 enlace es hacia abajo (para el tráfico saliente, AS4 simplemente da las rutas de
AS2 una mayor preferencia local). Se trata de un escenario en el día de hoy
Internet. Pero tenga en cuenta que esta configuración tiene otro estable
Solución:



Meyer & Patel Informativo [Página 10]

RFC 4274 BGP-4 Protocolo Analysis enero 2006
En este caso, no se traduce AS3 la "depref mi ruta" comunidad
Recibida de AS4 en una "depref mi ruta" para la comunidad AS1.
Por lo tanto, si conoce de la ruta AS1 a AS4 que AS3 tránsitos, se
Prefiero que la ruta (porque AS3 es un cliente). Este estado podría ser
A que se había llegado, por ejemplo, a partir de la "correcta" de copia de seguridad de enrutami
ento
Muestra en primer lugar, con lo que el AS2-
AS4 BGP período de sesiones y, a continuación, con lo que
Proceso de regeneración. En general, BGP no tiene manera de preferir la "intención"
La solución más anómala. La solución dependerá de recogida
El imprevisible fin de los mensajes BGP.

Si bien este ejemplo es relativamente simple, muchos operadores pueden no
Reconocemos que la verdadera fuente del problema es que la BGP
Políticas de ASes pueden interactuar de maneras inesperadas, y que estos
Interacciones puede resultar en múltiples rutas estables. Uno puede imaginar
Que las interacciones pueden ser mucho más complejos en la vida real
Internet. Sospechamos que tales anomalías sólo será más
Comunes como BGP sigue evolucionando con la política más rica expresividad.
Por ejemplo, cursó comunidades ofrecen una mayor flexibilidad significa
Señalización de la información dentro y entre los sistemas autónomos de
Es posible con las comunidades [RFC1997]. Al mismo tiempo,
Solicitudes de las comunidades por los operadores de red están evolucionando para
Resolver cuestiones complejas y entre dominio ingeniería de tráfico.

7,2. Existencia de rutas estables

Uno también puede construir un conjunto de políticas para los que no pueden BGP
Garantía de que existe un establo de enrutamiento (o, lo que es peor, que es estable
Enrutamiento será nunca encontradas). Por ejemplo, los documentos [RFC3345]
Varios escenarios que conducen a la ruta oscilaciones asociados a la
Uso de la Multi-Exit Discriminator (MED) atributo. Ruta
Oscilación que va a suceder en BGP cuando un conjunto de políticas no tiene
Solución. Es decir, cuando no hay enrutamiento estable que satisfaga
Las limitaciones impuestas por la política, BGP no tiene otra opción que mantener
Tratando. Además, incluso si las configuraciones BGP puede tener un estable
Enrutamiento, el protocolo puede no ser capaz de encontrarla; BGP puede "llegar
Atrapados "en un callejón sin salida que no tiene solución.

Protocolo de divergencia no es, sin embargo, un problema asociado únicamente con
Uso de la MED atributo. Este potencial existe en BGP incluso sin
El uso del atributo MED. Por lo tanto, al igual que los no deseados
Nondeterminism descritos en la sección anterior, este tipo de
Protocolo divergencia es una consecuencia no deseada de los sin
BGP naturaleza de la política de idiomas.

8. Aplicabilidad

En esta sección, para determinar los entornos que así es BGP
Adecuados, y los entornos para los que no es adecuado. Este
La pregunta es, en parte, respondió en la Sección 2 de BGP [BGP4], que
Estados:

> "Para caracterizar el conjunto de las decisiones de política que se puede ejecutar
> Utilizando BGP, uno debe centrarse en la regla de que un AS anuncia a su
> ASes vecino sólo las rutas que él mismo utiliza. Esta norma
> Refleja el "hop-by-hop" paradigma de enrutamiento generalmente utilizados
> En toda la actual Internet. Tenga en cuenta que algunas políticas no pueden
> El apoyo de la "hop-by-hop" paradigma de enrutamiento y por lo tanto exigen
> Técnicas como el enrutamiento de origen para hacer cumplir. Por ejemplo, BGP
> No permite a un AS para enviar tráfico a un vecino intención AS
> Que el tráfico de tomar una ruta diferente de la adoptada por el tráfico
> Originadas en el vecino AS. Por otra parte, puede BGP
> Cualquier política de apoyo se ajusten a los "hop-by-hop" encaminamiento
> Paradigma. Dado que la actual Internet utiliza sólo el "hop-by-hop"
> Y desde el paradigma de enrutamiento BGP puede apoyar cualquier política que
> Que se ajusta al paradigma, BGP es altamente aplicable como una inter-AS
> Protocolo de enrutamiento para el actual Internet ".

Uno de los puntos importantes en este caso es que sólo contiene esencial BGP
Funcionalidad, y al mismo tiempo proporcionar un mecanismo flexible
En el protocolo que nos permite extender su funcionalidad. Para
Ejemplo, BGP capacidades proporcionan una manera fácil y flexible a
Introducir nuevas características en el protocolo. Por último, porque se BGP
Diseñado para ser flexible y extensible, nuevas y / o en evolución
Las necesidades se pueden abordar a través de los mecanismos existentes.

En resumen, BGP es muy adecuado como un sistema autónomo inter -
Para cualquier protocolo de enrutamiento de Internet que se basa en IP [RFC791] como la
De protocolo de Internet y el "hop-by-hop" paradigma de enrutamiento.

9. Agradecimientos

Queremos dar las gracias a Paul Traina autoría de las versiones anteriores de
Este documento. Elwyn Davies, Tim Griffin, Randy Presuhn, Curtis
Villamizar y Atanu Ghosh también muchas observaciones perspicaces sobre
Versiones anteriores de este documento.

10. Consideraciones de Seguridad

BGP proporciona mecanismos flexibles con diferentes niveles de complejidad
Con fines de seguridad. BGP sesiones son autenticados mediante BGP
Período de sesiones de la dirección y la AS número asignado. Porque sesiones BGP
Uso de TCP (IP) para el transporte fiable, BGP sesiones son más

Meyer & Patel Informativo [Página 12]

RFC 4274 BGP-4 Protocolo Analysis enero 2006
Autenticadas y garantizado por toda la autenticación y la seguridad
Mecanismos utilizados por TCP e IP.

BGP utiliza TCP MD5 opción de validación de datos y la protección contra
Spoofing de los segmentos TCP intercambiados entre sus períodos de sesiones. El uso
MD5 opción de TCP para BGP es descrito en detalle en [RFC2385]. El
TCP MD5 clave de gestión se discute en [RFC3562]. BGP datos
Se proporciona encriptación IPsec utilizando el mecanismo, que cifra la
Datos de la carga útil IP (incluyendo TCP y datos BGP). El mecanismo de IPsec
Se puede utilizar tanto en el modo de transporte y el modo túnel. El
IPsec mecanismo se describe en [RFC2406]. Tanto la opción TCP MD5
IPsec y el mecanismo no son ampliamente implementado mecanismos de seguridad
Para BGP en la actual Internet. Por lo tanto, es difícil evaluar su
Impacto real de rendimiento cuando se utilizan con BGP. Sin embargo, debido a que ambos
Son los mecanismos y TCP-IP basados en los mecanismos de seguridad, el Link
Ancho de banda, la utilización de la CPU y la memoria consumida por router BGP se
El mismo que cualquier otro y TCP-IP basada en protocolos.

BGP utiliza el valor TTL IP para proteger su exterior BGP (EBGP) sesiones
De cualquier TCP-IP o basados en la CPU intensivos ataques. Se trata de un simple
Mecanismo que sugiere la utilización de filtrado BGP (PCT) de los segmentos,
IP utilizando el valor TTL a cargo dentro de la cabecera IP de BGP (TCP)
Segmentos que se intercambian entre los períodos de sesiones EBGP. El BGP TTL
Mecanismo se describe en [RFC3682]. El uso de los efectos [RFC3682]
El rendimiento de una manera similar como usar cualquier lista de control de acceso (ACL)
Políticas para BGP.

Tal flexible y TCP-IP basados en los mecanismos de seguridad, permitir a BGP
Prevenir la inserción / borrado / modificación de datos BGP, de cualquier snooping
Los datos, el período de sesiones el robo, etc Sin embargo, BGP es vulnerable a la
Misma seguridad que los ataques están presentes en TCP. El [BGP-VULN]
Explica en profundidad acerca de la vulnerabilidad de la seguridad BGP. En el momento
De escribir esto, varios se están realizando esfuerzos para crear y
La definición de una adecuada infraestructura de seguridad dentro de la BGP
Protocolo para proporcionar autenticación y seguridad para su enrutamiento
Información; estos esfuerzos incluyen [SBGP] y [SOBGP].

11. Referencias

11,1. Referencias Normativas

[BGP4] Rekhter, Y., Li., T., y S. Hares, Eds. "Una Frontera

Gateway Protocolo 4 (BGP-4) ", RFC 4271, de enero de 2006.

[RFC1519] Fuller, V., Li, T., Yu, J., y K. Varadhan, "Classless Inter-Domain Routing (CIDR): Asignación de una dirección y Estrategia de agregación ", RFC 1519, septiembre de 1993.

Meyer & Patel Informativo [Página 13]

RFC 4274 BGP-4 Protocolo Analysis enero 2006

[RFC791] Postel, J., "Protocolo de Internet", STD 5, RFC 791, De septiembre de 1981.

[RFC1997] Chandra, R., Traina, P., y T. Li, "Comunidades BGP Atributo ", RFC 1997, agosto de 1996.

[RFC2385] Heffernan, A., "La protección de BGP a través de la sesión TCP Firma MD5 Option ", RFC 2385, agosto de 1998.

[RFC3345] McPherson, D., Gill, V., Walton, D., y A. Retana, "Border Gateway Protocol (BGP) persistentes de carreteras Oscilación del Estado ", RFC 3345, agosto de 2002.

[RFC3562] sangre, M., "Consideraciones clave para la gestión de TCP Firma MD5 Option ", RFC 3562, julio de 2003.

[RFC3682] Gill, V., Heasley, J. y D. Meyer, "El Generalizado TTL Mecanismo de Seguridad (GTSM) ", RFC 3682, febrero 2004.

[RFC3392] Chandra, R. y J. Scudder, "Capacidades Publicidad Con BGP-4 ", RFC 3392, noviembre de 2002.

[BGP-VULN] Murphy, S., "BGP Análisis de Vulnerabilidades de Seguridad", RFC 4272, de enero de 2006.

[SBGP] Seo, K., S. y C. Lynn Kent, "Secure Border Gateway Protocolo (Secure-BGP) ", IEEE Journal on Selección de Áreas in Communications Vol. 18, No. 4, April 2000, pp. 582-592.

11.2. Informative References

[RFC854] Postel, J. and J. Reynolds, "Telnet Protocol Specification", STD 8, RFC 854, May 1983.

[RFC1105] Lougheed, K. and Y. Rekhter, "Border Gateway Protocol (BGP)", RFC 1105, June 1989.

[RFC1163] Lougheed, K. and Y. Rekhter, "Border Gateway Protocol (BGP)", RFC 1163, June 1990.

[RFC1264] Hinden, R., "Internet Routing Protocol Standardization Criteria", RFC 1264, October 1991.

Meyer & Patel Informational [Page 14]

[RFC1267] Lougheed, K. and Y. Rekhter, "Border Gateway Protocol 3 (BGP-3)", RFC 1267, October 1991.

[RFC1772] Rekhter, Y., and P. Gross, Editors, "Application of the Border Gateway Protocol in the Internet", RFC 1772, March 1995.

[RFC1774] Traina, P., "BGP-4 Protocol Analysis", RFC 1774, March 1995.

[RFC2622] Alaettinoglu, C., Villamizar, C., Gerich, E., Kessens, D., Meyer, D., Bates, T., Karrenberg, D., and M. Terpstra, "Routing Policy Specification Language (RPSL)", RFC 2622, June 1999.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[ROUTEVIEWS] Meyer, D., "The Route Views Project", http://www.routeviews.org.

[SOBGP] White, R., "Architecture and Deployment Considerations for Secure Origin BGP (soBGP)", Work in Progress, May 2005.

Authors' Addresses

David Meyer

EMail: dmm@1-4-5.net
Keyur Patel
Cisco Systems

EMail: keyupate@cisco.com

Full Copyright Statement

INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).