Enrutamiento Avanzado



EGP

Investigación

Damm Manzanera Carlos Alberto

No. Control 1204521

18/Junio/2015

Ing. En Sistemas Computacionales

Índice

Antecedentes\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_3-5

Definición del Problema\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_6

Justificacion\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_7

Objetivo\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_8

Marco Teórico\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_9-10

Supuesto\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_11

Método\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_12

Cronograma\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_13

Presupuesto\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_14

Difusion\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_15

Fuentes de Información\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_16

Antecedentes

BGP es el protocolo de enrutamiento EGP más utilizado en Internet. La versión 1 de este protocolo apareció en 1989 para sustituir a EGP. Posteriormente, salieron nuevas versiones como la versión 2 en 1990 y la versión 3 en 1991. Finalmente apareció la versión 4 que proporciona soporte para CIDR (Classless Interdomain Routing).

BGP es un protocolo que funciona sobre TCP por el puerto 179 y permite el encaminamiento de los paquetes IP que se intercambian entre los distintos AS. Para ello, es necesario el intercambio de prefijos de rutas entre los diferentes AS de forma dinámica, lo cual se lleva a cabo mediante el establecimiento de sesiones BGP inter-AS sobre conexiones TCP. Este tipo de operación proporciona comunicación fiable y esconde todos los detalles de la red por la que se pasa. Debido a que en cada AS se utiliza un protocolo IGP con una definición distinta para el coste de los enlaces, es imposible encontrar el camino más corto hacia cada destino. Por ello, una vez se han aplicado las restricciones sobre las rutas, BGP utiliza un algoritmo similar al tipo vector de distancia, para seleccionar aquellas rutas que impliquen el mínimo número de AS a atravesar. Las tablas de encaminamiento de BGP almacenan rutas para alcanzar redes. Las rutas están formadas por una secuencia de números de sistemas autónomos que se deben seguir para alcanzar el prefijo indicado. El último número de AS de la ruta se corresponde con la organización que tiene registrado el prefijo que es donde se encuentra el destino. El principal motivo para almacenar la ruta completa es la detección y eliminación de bucles para evitar que los paquetes se envíen de forma infinita pasando varias veces por un mismo AS.

Sesiones

En una sesión BGP participan sólo dos routers (peers). En cualquier momento una red puede tener muchas sesiones BGP concurrentes y también una misma pasarela puede participar en muchas sesiones BGP. En la sesión BGP se lleva a cabo el proceso denominado peering, que consiste en que un AS informa a otro sobre las redes que puede alcanzar a partir de éste. Además de las sesiones inter-AS, los routers de borde de un mismo AS deben intercambiar también informaciones BGP para conocer las mismas rutas externas e internas. Para ello se utiliza el protocolo I-BGP, definido en la versión 4 de BGP, que utiliza el mismo tipo de mensajes que E-BGP, el cual es el protocolo utilizado en las sesiones BGP entre dos pasarelas de dos AS distintos. Según la especificación de BGP- 4, existe una diferencia a la hora de reanunciar rutas en E-BGP y en I-BGP. En E-BGP, los prefijos que aprende un router de un vecino pueden ser anunciados a otro vecino mediante I-BGP y viceversa, pero un prefijo aprendido de un vecino mediante I-BGP no puede reanunciarse a otro vecino por I-BGP. Esta regla de limitación para reanunciar prefijos entre routers vecinos mediante I-BGP sirve para evitar bucles (loops) dentro de un AS. Debido a que no se pueden reanunciar prefijos entre routers I-BGP, es necesario que exista conectividad entre todos los routers vecinos que se comuniquen mediante IBGP dentro de un mismo AS, por lo que se utiliza un mallado total entre éstos (fullmesh). Esta malla es realmente virtual en la práctica ya que se implementa de una forma independiente a la conectividad física. Por ello, otra diferencia es que en I-BGP los vecinos no tienen que estar obligatoriamente conectados de forma directa como en el caso de E-BGP. La conectividad entre los routers de borde que intercambian sus informaciones BGP mediante I-BGP en un mismo AS vendrá asegurada por el protocolo IGP utilizado. Si un router de borde no es capaz de alcanzar una ruta de su propio AS, la cual le ha sido anunciada por un vecino interno, esta ruta no será propagada a los vecinos BGP internos o externos.

Funcionamiento

Cuando un router anuncia un prefijo a uno de sus vecinos BGP, esa información es considerada válida hasta que el primer router explícitamente anuncia que la información ya no es válida o hasta que la sesión BGP se pierde. Esto significa que BGP no requiere que la información de routing se refresque periódicamente. De este modo, en un principio existirá un alto flujo de mensajes cuando se establece la sesión BGP, pero transcurrido un tiempo de estabilización los routers sólo necesitarán informar de los cambios que han ocurrido. Por ejemplo, en un AS tipo backbone el intercambio es del orden de 50.000 prefijos inicialmente. Para almacenar información de encaminamiento, el protocolo BGP necesita un conjunto de tablas de datos denominadas RIBs (Routing Information Bases). Éstas son las siguientes: • Adj-RIB-in: En esta tabla se almacenan prefijos aprendidos de un vecino particular. Hay tantas tablas de este tipo como pares BGP. • Loc-RIB: Almacena las mejores rutas seleccionadas (prefijos + longitud máscara) que conoce el proceso BGP bien porque las ha obtenido de la tabla de encaminamiento (comandos network, agrégate-address y redistribute), o bien porque se han aprendido por BGP (I-BGP o E-BGP), tras pasar los filtros de entrada. Estas rutas pueden ser anunciadas si la política de encaminamiento a la salida lo permite. Hay sólo uno por cada sistema autónomo. • Adj-RIB-out: Almacena prefijos para ser anunciados a otros vecinos. Esta tabla se construye a partir de las informaciones de la tabla Loc-RIB que han sido filtrados y cuyos atributos han sido modificados según configuración. Se tiene una tabla de este tipo por cada par BGP.

Mensajes

El tamaño de los enviarse de forma segura m todos los mensajes y está formada por un marcador (16 octetos) que contiene información de sincronización y de seguridad, un campo longitud (2 octetos) que indica la longitud total del mensaje y un campo tipo (1 octeto) que indica el tipo del mensaje.

Existen 4 tipos de mensajes:

OPEN: Este mensaje protocolo BGP utilizado, el número de AS y el número identificador del proceso BGP. Además, este mensaje incluye un valor de tiempo durante el cual se va a mantener la sesión (90 segundos normalmente). Si se indica el valor 0 significa que la sesión no va a tener límite de duración. Una vez que se envía este mensaje, el proceso BGP se queda en espera de recibir un mensaje KEEPALIVE. Prefijo/Network Layer Reachability Information (variable) Atributos del camino (variable) Valor del atributo.

KEEPALIVE: Este mensaje sirve como confirmación a un mensaje OPEN. Si el tiempo que se estableció para la duración de la sesión es limitado, es necesario que los procesos BGP envíen este mensaje cada cierto tiempo (30 segundos normalmente) para indicar que se mantiene la sesión. De este modo, en el caso de que no haya modificación de la tabla de encaminamiento, los routers BGP sólo intercambian este tipo de mensaje de forma periódica, lo cual genera un tráfico de unos 5bits/s en el nivel BGP (cada mensaje tiene un tamaño mínimo de unos 19 octetos).\NOTIFICATION: Este mensaje sirve para cerrar la sesión BGP, cerrando también la conexión TCP. Además, se envía un código para indicar si hubo errores, como por ejemplo la recepción de un mensaje incorrecto, un problema del proceso BGP o la ausencia de mensajes KEEPALIVE durante 90 segundos (hello time). La consecuencia del cierre de la sesión BGP es la anulación de todas las rutas aprendidas en dicha sesión.

UPDATE: Este mensaje sirve para intercambiar las informaciones de encaminamiento como las rutas a eliminar, el conjunto de atributos de cada ruta, las informaciones sobre los prefijos de redes accesibles (red y longitud de la máscara) o NLRI (Network Layer Reachability Information) y la longitud de cada ruta. Este mensaje se envía sólo cuando existe algún cambio y su recepción produce la activación del proceso BGP, que se encargará entonces de modificar convenientemente las tablas RIB y de emitir a su vez un mensaje UPDATE hacia los otros vecinos.

Atributos

Dentro del mensaje UPDATE se distinguen una serie de atributos que indican una serie de informaciones adicionales asociadas al prefijo de la ruta. Estos atributos se codifican en forma de tripleta con los campos TIPO, LONGITUD y VALOR y son utilizados principalmente para elegir la mejor ruta hacia un destino y también para aplicar reglas de filtrado a los mensajes BGP recibidos y anunciados. Los atributos obligatorios son los siguientes:

ORIGIN: Indica la forma por la que se ha aprendido la ruta: i si la ruta ha sido aprendida por un protocolo IGP, e si se ha aprendido por EGP, o ? (INCOMPLETE) en el caso de que el origen sea desconocido o que se haya aprendido de una forma distinta. La función de este atributo es también la selección de rutas, dando prioridad según los valores en el siguiente orden: IGP < EGP , como se muestra en la siguiente configuración correspondiente al ejemplo anterior:

RTC# router bgp 256 neighbor 1.1.1.1 remote-as 100 neighbor 128.213.11.2 remote-as 256 bgp default local-preference 150

RTD# router bgp 256 neighbor 3.3.3.4 remote-as 300 neighbor 128.213.11.1 remote-as 256 bgp default local-preference 200

En la configuración anterior, RTC asignará el valor 150 al atributo LOCAL\_PREF de todas las rutas que anuncie por I-BGP. A su vez, RTD establece un LOCAL\_PREF de 200 para todas las redes que anuncia hacia el interior. De este modo, la ruta 170.10.0.0 recibida en el AS 256 tendrá un valor mayor de este atributo cuando proviene del AS 300 que cuando lo hace del AS 100, y todo el tráfico hacia dicha red tendrá el router RTD como punto de salida del AS 256. Por otra parte, los route maps permiten una mayor flexibilidad a la hora de modificar el valor del atributo LOCAL\_PREF.

En la configuración anterior, todas las rutas recibidas por el router RTD eran modificadas con un valor de LOCAL\_PREF igual a 200, lo cual no es necesario cuando las rutas proceden del AS 34. Por ello, utilizando un route map se puede especificar qué rutas serán modificadas:

RTD# router bgp 256 neighbor 3.3.3.4 remote-as 300 neighbor 3.3.3.4 setlocalin in neighbor 128.213.11.1 remote-as 256 .... ip as-path 7 permit ^300$ ... route-map setlocalin permit 10 match as-path 7 set local-preference 400 route-map setlocalin permit 20 set local-preference 150

Con esta configuración en el router RTD, cualquier ruta que provenga del AS 300 será modificada con un valor de LOCAL\_PREF igual a 200, mientras que el resto de rutas recibidas (como las que provienen del AS 34) serán modificadas con un LOCAL\_PREF igual a 150.

ATOMIC\_AGGREGATE: Este atributo indica que la ruta correspondiente se ha obtenido mediante agregación de otras rutas más precisas. Además de los atributos anteriores, existen otros atributos opcionales que no están recogidos por la norma:

METRIC o MED (Multi-Exit-Discriminator): Este atributo se utiliza en el caso en que se tengan dos AS multiconectados. Su función es servir para seleccionar una ruta cuando se reciben por E-BGP varias rutas iguales anunciadas desde el mismo AS por varios enlaces. Así, al configurar los routers pasarela en el AS que envía los anuncios, se da privilegios a un enlace respecto a otro para anunciar una ruta si se configura un valor del atributo MED más bajo para esa ruta. El atributo MED es intercambiado mediante E-BGP entre dos routers externos pertenecientes a dos AS distintas. El valor de este atributo no se traspasa de un AS a otro, de forma que cuando una ruta recibida por un AS se envía a otro AS tercero se modifica el valor del MED a 0 (por defecto). El valor que se suele asignar en los routers pasarela para el MED de las rutas cuando van a ser anunciadas al exterior es el de la métrica IGP que tengan esas rutas al llegar a las pasarelas. Este valor es numérico y varía entre 0 y 0xFFFFFFFF. A menos que se especifique lo contrario, un router comparará el valor del atributo MED en las rutas recibidas de otro AS en el caso de que dichas rutas hayan sido anunciadas por vecinos que se encuentran ambos en dicho AS. Por ello, si se quiere comparar el valor de este atributo también para el caso de rutas anunciadas por vecinos pertenecientes a diferentes AS, será necesario configurar el comando bgp always-compare-med en el router. La siguiente figura muestra un ejemplo de uso de este atributo: En el diagrama anterior, el AS 100 obtiene información de la red 180.10.0.0 a través de tres routers diferentes: RTC, RTD (ambos pertenecientes al AS 300) y RTB (que pertenece al AS 400). Se va a suponer que se ha configurado un valor del atributo MED diferente para los anuncios que provienen de cada router (120 para los anuncios de RTC, 200 para los de RTD y 50 para los de RTB). Dado que por defecto un router sólo compara el valor del atributo MED para las rutas anunciadas por routers que pertenecen al mismo AS, RTA sólo comparará los valores del MED de las rutas de RTC con las de RTD, tomando RTC como siguiente salto para los destinos coincidentes (ya que 120 es menor MED que 200). Debido a que RTB se encuentra en un AS diferente que los otros dos routers, RTA no podrá comparar el valor 50 del MED de las rutas anunciadas por RTB, por lo que tendrán que utilizarse otros atributos para la elección de la mejor ruta en este caso. Sin embargo, se puede configurar RTA para forzar a que compare los valores de los MED de las rutas recibidas independientemente del AS del que provengan mediante el comando bgp always-compare-med. Las siguientes líneas muestran los comandos necesarios para llevar a cabo la configuración del ejemplo anterior:

RTA# router bgp 100 neighbor 2.2.2.1 remote-as 300 neighbor 3.3.3.3 remote-as 300 neighbor 4.4.4.3 remote-as 400 bgp always-compare-med .... RTC# router bgp 300 neighbor 2.2.2.2 remote-as 100 neighbor 2.2.2.2 route-map setmetricout out neighbor 1.1.1.2 remote-as 300 route-map setmetricout permit 10 set metric 120

RTD# router bgp 300 neighbor 3.3.3.2 remote-as 100 neighbor 3.3.3.2 route-map setmetricout out neighbor 1.1.1.1 remote-as 300 route-map setmetricout permit 10 set metric 200 RTB# router bgp 400 neighbor 4.4.4.4 remote-as 100 neighbor 4.4.4.4 route-map setmetricout out route-map setmetricout permit 10 set metric 50 Otra manera de configurar el valor del atributo MED es mediante el comando default-metric number, en el caso de que se estén redistribuyendo rutas en BGP. De este modo, el router RTB se podría haber configurado para que redistribuyese la red 180.10.0.0 en BGP hacia el AS 100 con un valor del atributo MED igual a 50, lo cual sería de la siguiente manera:

RTB# router bgp 400 redistribute static default-metric 50 ip route 180.10.0.0 255.255.0.0 null 0

WEIGHT (propietario CISCO): Se utiliza como primer criterio de selección para obtener la mejor ruta cuando se tienen varias rutas hacia el mismo destino. Este atributo es asignado localmente en el router, de modo que no tiene sentido anuncirlo a otros routers. Su valor puede variar entre 0 y 65535 y por defecto vale 32768 para las rutas cuyo origen es el propio router y con valor 0 para el resto de rutas. Se elegirá la ruta con el valor mayor de este atributo. En el siguiente ejemplo, el router RTA aprende la red 175.10.0.0 del AS 4 para a continuación anunciarla al router RTC. Del mismo modo, el router RTB aprende la red 175.10.0.0 del AS 4 y también la anunciará al router RTC. Así, RTC dispone de dos caminos para alcanzar la red 175.10.0.0, por lo que tendrá que decidirse por uno de ellos. Suponiendo que en el router RTC se configura que todos los anuncios provenientes de RTA tengan un valor del atributo WEIGHT mayor que en el caso de los anuncios de RTB, se forzará así a RTC a utilizar RTA como NEXT\_HOP para llegar a la red 175.10.0.0. La configuración del atributo WEIGHT se puede llevar a cabo mediante tres maneras distintas: o Mediante el comando neighbor: neighbor {ip-address|peer-group} weight weight La configuración del atributo WEIGHT en el ejemplo anterior sería de la siguiente manera utilizando el comando neighbor: RTC# router bgp 300 neighbor 1.1.1.1 remote-as 100 neighbor 1.1.1.1 weight 200 neighbor 2.2.2.2 remote-as 200 neighbor 2.2.2.2 weight 100 o Utilizando una lista de acceso basada en as-path (ver apartados 7.1.3 y 11.6): ip as-path access-list access-list-number {permit|deny} as-regular-expression neighbor ip-address filter-list access-list-number weight weight La configuración del ejemplo anterior quedaría de la siguiente forma utilizando listas de acceso: RTC# router bgp 300 neighbor 1.1.1.1 remote-as 100 neighbor 1.1.1.1 filter-list 5 weight 200 neighbor 2.2.2.2 remote-as 200 neighbor 2.2.2.2 filter-list 6 weight 100 ... ip as-path access-list 5 permit ^100$ ip as-path access-list 6 permit ^200$ o Usando route-maps (ver apartados 7.2 y 11.3). El ejemplo anterior tendría la siguiente configuración usando route maps: RTC# router bgp 300 neighbor 1.1.1.1 remote-as 100 neighbor 1.1.1.1 route-map setweightin in neighbor 2.2.2.2 remote-as 200 neighbor 2.2.2.2 route-map setweightin in ... ip as-path access-list 5 permit ^100$ ... route-map setweightin permit 10 match as-path 5 set weight 200 route-map setweightin permit 20 set weight 100 La lista de acceso definida en el route map se aplicará a todos los anuncios de entrada que provengan del AS 100, de manera que se les modificará el valor del atributo WEIGHT a 200. Por defecto, al resto de anuncios que provengan de otro AS se les asignará el valor 100 para el atributo WEIGHT.

COMMUNITY: Este atributo opcional permite agrupar los destinos en comunidades de destino (grupos de routers con unas mismas propiedades) para ayudar a escalar la aplicación de decisiones de encaminamiento (aceptar una ruta, preferir una ruta ante otra, redistribuir una ruta, etc). Cada destino puede ser miembro de varias comunidades. El atributo COMMUNITY consiste en un valor de 23 bits en el cual los 16 bits más significativos son el indicador del AS, mientras que los 16 bits menos significativos son definidos por el administrador del AS. Su valor puede indicar si una ruta no es anunciable a los vecinos del grupo (no-export), si no es anunciable a ningún vecino BGP (no-advertise) o si no es anunciable vía E-BGP (no-export-subconfed). Para establecer la comunidad a la que pertenece un destino se puede utilizar la directiva set community en un route-map. En este último caso se pueden indicar las siguientes opciones: o <1-4294967295>: Número de comunidad o aa:nn: Número de comunidad en formato aa:nn. o additive: Se añade a una comunidad existente. o local-AS: No enviar a los peers EBGP (well-known community). o no-advertise: No enviar a ningún peer (well-known community). o no-export: No exportar fuera del AS (well-known community) o none: No atributo de comunidad. A continuación se muestran dos ejemplos de configuración de este atributo mediante route maps: route-map communitymap match ip address 1 set community no-advertise -- route-map setcommunity match as-path 1 set community 200 additive La opción additive permite añadir el destino a la comunidad 200. Si no se hubiese indicado esta opción, la nueva comunidad sustituiría las comunidades existentes que hayan sido configuradas para ese destino (un destino puede formar parte de varias comunidades). Aunque se modifique el atributo COMMUNITY de una ruta, éste no será anunciado por defecto a los vecinos BGP. Para ello, será necesario utilizar el comando neighbor {peer-address | peer-group-name} send-community. Así, como ejemplo de uso del route map anterior se podría tener la siguiente configuración en un router: RT# router bgp 100 neighbor 3.3.3.3 remote-as 300 neighbor 3.3.3.3 send-community neighbor 3.3.3.3 route-map setcommunity out

AGGREGATOR: Indica el AS que ha formado la ruta agregada y la dirección IP del router en el que se realizó dicha agregación.

Otros atributos: ORIGINATOR\_ID (router ID del vecino I-BGP que refleja rutas del cliente route reflector a no clientes), CLUSTER\_LIST (cadena de ORIGINATOR\_IDs a través de los cuales la ruta ha pasado y cuya función servir para el chequeo de relaciones circulares), MP\_REACH\_NLRI y MP\_UNREACH\_NLRI. En la siguiente figura se muestran las tablas Adj-RIB-in de dos routers de borde de dos AS en las que se puede ver el valor de los diferentes atributos BGP: En las tablas se indican las rutas alcanzables (NLRI) y sus atributos obligatorios: el siguiente nodo para llegar a éstas (NEXT\_HOP), el camino de ASNs necesario a seguir para llegar a la ruta (AS\_PATH) y el origen por el que se aprendió la ruta (i en este caso debido a que la ruta proviene del interior del AS que la anuncia y fue aprendida mediante un protocolo IGP). Para este ejemplo anterior, la configuración de los routers pasarela que establecen la sesión sería la siguiente: Configuración de la pasarela del AS100: router bgp 100 neighbor 194.9.1.2 remote-as 200 neighbor 194.9.2.3 remote-as 300 network 194.10.1.0 mask 255.255.255.0 Configuración de la pasarela del AS200: router bgp 200 neighbor 194.9.1.1 remote-as 100 neighbor 194.9.3.3 remote-as 300 network 194.10.2.0 mask 255.255.255.0 Al haberse configurado un número de AS distinto para cada pasarela, se utilizará el protocolo E-BGP en la sesión BGP entre ambos. El comando network hace que se rellene la tabla Local-RIB a partir de la tabla de encaminamiento. En un route-map (conjunto de reglas de encaminamiento) se pueden especificar los valores de los atributos mediante la directiva set con las siguientes opciones:

as-path: Añade una cadena de AS para el atributo AS-PATH.

ommunity: Atributo de comunidad.

local-preference: Atributo de preferencia local de BGP.

metric: Valor de la métrica para el protocolo de encaminamiento.

origin: Código de origen BGP.

weight: Peso BGP para la tabla de encaminamiento.

ip next-hop { A.B.C.D | peer-address }: Salto siguiente para llegar al destino.

Marco Teórico

Con el fin de asegurar la seguridad del ser humano el autor Isaac Asimov público en su obra runaround lo que se conoce como las tres leyes principales de la robótica las cuales son:

1.- Un robot no puede hacer daño a un ser humano o, por inacción, permitir que un ser humano sufra daño.

2.- Un robot debe obedecer las órdenes dadas por los seres humanos, excepto si estar órdenes entran en conflicto con la primera ley.

3.- Un robot debe proteger su propia existencia en medida que esta protección no entre en conflicto con la primera o segunda ley.

Para fines prácticos no existen historial de eventos que se puedan relacionar con este tema ya que aún es considerado ciencia ficción pero varios autores de novelas que inclusive han llegado a la gran pantalla han tenido diversos puntos de vista los cuales son relevantes en esta investigación, por ejemplo el mismo autor Isaac Asimov género en 1950 la obra Yo, Robot la cual fue inspiración principal para la película protagonizada por Will Smith en el 2004 Yo, Robot en la cual habla de un supuesto en que las maquinas pudieron romper el código de las 3 leyes de la robótica y el caos que género, como mencionado anteriormente, la maquina llego a la conclusión de que el ser humano era innecesario en el planeta y empezó a movilizar un ejército de máquinas las cuales compartían la misma conciencia y que sin la ayuda del protagonista hubieran destruido a la humanidad.

El escritor James Cameron en 1984 escribió y dirigió la película conocida como Terminator la cual habla precisamente de una inteligencia artificial conocida como skynet la cual había sido creada para proteger a los Estados Unidos y que en cuanto fue inicializada hackeo todos los sistemas de defensa del mundo y dejo a la raza humana indefensa ya que todo lo que utilizamos el día de hoy, hasta en las comunicaciones, es de origen digital.

Otro escritor Jack Paglen fue el encargado de escribir el guion de la película reciente Transcendence, la cual de forma más realista habla de la creación de una inteligencia artificial al mover la conciencia de una persona la cual su cuerpo había se estaba deteriorando a causa de una enfermedad, a una máquina, después de varios intentos fallidos la misma conciencia logra arreglar los propios errores de programación de sí misma y logra mantener la conciencia intacta del protagonista Johnny Deep.

Esta última película tiene una trama muy peculiar ya que pone en duda si los valores, la ética y lo que se considera humano es capaz de ser plasmado a código. Dada la era digital en la que vivimos, las redes sociales y la facilidad de encontrar información a través de internet el simple hecho de que una persona pudiera tener acceso a toda esta información y obtener los recursos para tener la capacidad de una súper computadora lo convertiría en un semidiós, dado que técnicamente seria inmortal, tendría acceso a toda la información del mundo y tendría la capacidad de manipular todos los dispositivos digitales que existen hoy en día.

Ahora si bien una persona tuviera este tipo de poder solo cabe una pregunta, ¿cómo la utilizaría? En la película el protagonista empieza ayudando a los humanos creando nueva tecnología para curar enfermedades, crear remplazos de miembros perdidos y crea una ciudad a su cargo, después de un tiempo empieza a imponer su voluntad en los seres humanos y con el fin de ser eficiente y mejor les quita lo esencial del ser humano, el poder de decisión.

En el transcurso de la película uno cambia de parecer acerca de la IA, ya que estando a favor pasa a estar en contra ya que pone en duda si todos los atributos de una persona se pudieron pasar a una maquina o si solo pretende ser esa persona pero sin valores o ética y al final se demuestra que todo lo que hacía lo hacía por amor, pero al ser malentendido decide sacrificarse por la mujer que amaba.

Esta última película deja implícito que la IA es tan peligrosa como la persona que la realice, a fin de cuentas un programa para hacer algo bueno lo hace, un programa para destruir como un virus destruye pero creo a fin de cuentas que toda la trama está basada en el amor, algo que dudosamente se pueda hacer sentir a una máquina, ya que pensar es una cosa, el sentir es otra.

Todos estos autores basan su pensamiento en la lógica básica que a fin de cuentas seguiría una maquina si pudiera pensar, pero yendo un poco más a las personas que tratan de hacer esto realidad como Alan Turing los cuales implementaron su pensamiento en la creación de las primeras computadoras, ellos más que nadie saben cómo funcionan dichos dispositivito y aun así están plenamente seguros de que a fin de cuentas sería un bien más que un mal el desarrollo de una IA ya que muchos de ellos basan su criterio en que el pensamiento humano es bueno por naturaleza y son los factores externos los cuales pueden llegar a afectar dicho pensamiento y corromperlo.

Supuesto

Con la información recopilada se puede determinar que la inteligencia artificial más que llegar a ser una ayuda a la sociedad puede llegar a tener repercusiones en la misma ya que los riesgos que se pueden correr si es que se llega a corromper dicha inteligencia pudieran ser catastróficos.

Uno de los aspectos más importantes de la inteligencia del hombre es la libertad que se tiene para tomar decisiones y creo este sería un factor el cual debería de estar limitado en cuanto a la inteligencia artificial para evitar dichas repercusiones.

En si se puede llegar a una hipótesis de que cuando la inteligencia artificial sea creada en su totalidad tendrá que ser supervisada para evitar algún tipo de corrupción de la función para la cual fue diseñada.

Método

Esta investigación se llevara a cabo usando una metodología de investigación documental, utilizando esta metodología podremos recopilar toda la información necesaria y obtener puntos de vista de diferentes personas expertas en el tema de la inteligencia artificial ya que al ser un tema considerado por algunos de ciencia ficción los conocimientos de la mayoría pueden ser muy imparciales y llegarían a diferir mucho de lo que es la realidad.

Se llevaran a cabo encuestas acerca de varios temas a comparar sobre la IA así mismo como entrevistas a las personas más allegadas al tema, de ahí simplemente se digerirá toda la información para poder resumir y respaldar con estadísticas la conclusión llegada.

Ya que tenemos el tema de investigación se seguirán los siguientes pasos

* Se elaborara una guía de trabajo para la investigación.
* Se generara un calendario de actividades para organizar toda la investigación.
* Recolectara toda la información a analizar.
* Registro de fichas bibliográficas de donde se obtendrá la información y usar como respaldo.
* Realizar encuestas y entrevistas para obtener declaraciones comparables.
* Se analizara la información obtenida.
* Se elaboraran fichas de contenido.
* Se redactara en su totalidad la investigación.

Cronograma

El lapso de la investigación se llevó a cabo en las siguientes fechas:

|  |  |
| --- | --- |
| Fecha | Concepto |
| Principios de Agosto | Conceptualizar el tema a investigar |
| Finales de Agosto | Recopilar fuentes de información actualizadas con respecto al tema a investigar. |
| Septiembre | Dar lectura, reflexión y comprensión de todo el material de investigación para tener conocimientos necesarios para manipular la información obtenida en futuro |
| Octubre | Realizar encuestas a personas cercanas el tema del proyecto para obtener diferentes puntos de vista y contar con estadísticas referentes al objetivo de la investigación. |
| Finales de Octubre | Realizar viaje a conferencias acerca de IA para obtener aun mas información directa de expertos. |
| Principios de Noviembre | Empezar la redacción del tema de investigación y plasmar la información obtenida de forma digerida para el publico |
| Finales de Noviembre | Dar terminación al proyecto y plasmar la investigación en blogs referentes a la Inteligencia Artificial. |

Presupuesto

El presupuesto de esta investigación seria un total de $6,432 compuesto de los siguientes gastos:

Café internet para buscar temas a investigar así como material necesario a encontrar: $ 320.00

Libros, revistas y material referente al tema de investigación: $ 3000.00

Encuestas a realizar para obtener estadísticas de personas conocedoras del tema a investigar: $ 500.00

Camiones necesarios para ir a librerías y centros de información: $ 112.00

Viaje para escuchar conferencias de expertos en el tema y obtener aun mas información: $ 2500.00

Difusión

Los medios para promover esta investigación y hacerla conocer será meramente a través de internet y de blog, dado que es una investigación pura con una perspectiva hacia los pros y contras de algo inexistente hasta la fecha no es necesario dar tanta propaganda ya que simplemente es una opinión personal basada en conocimientos recopilados de varias fuentes de información las cuales a fin de cuenta habla de un tema considerado ciencia ficción.

Fuentes de Información

Yo robot

Isaac Asimov

Pocket Eldhasa, 1940

Robótica

John J. Craig

Pearson Educación, 2006

Fundamentos metodológicos de sistemas inteligentes para la solución de problemas complejos en ingeniería

Jairo Cañón Rodríguez, Demetrio Arturo Ovalle Carranza

Universidad Nacional de Colombia, 1997

The Terminator

James Cameron

William Wisher Jr., 1984

Inteligencia Artificial

Miquel Barceló García

UOC La Universidad Virtual (eBook)

Trascendence

Wally Pfister, 2014