Diseño e implementación de una solución de administración de tráfico de red basada en DNS y chequeos de disponibilidad

Nicolás del Río[1], Lía Molinari[1], Luis Marrone[2]

Calle 50 y 120, 2do piso, La Plata, Buenos Aires, Argentina
Cátedra de Sistemas Distribuidos. Maestría en Redes de Datos
Facultad de Informática, Universidad Nacional de La Plata
[1] {ndelrio, lmolinari}@info.unlp.edu.ar
[2] lmarrone@linto.unlp.edu.ar

Resumen. Los servicios de red como ser publicación de contenido WWW[1] y mail, entre otros, han crecido considerablemente en los últimos años, sin prever en la mayoría de los casos la utilización de mecanismos de alta disponibilidad en el acceso a través de la red. Grandes organizaciones e ISP[2] han utilizado el protocolo BGP[3], como única herramienta que permita conmutar el tráfico de red que está siendo dirigido a un CPD[4] hacia otra locación ante eventuales fallas de red. El presente artículo analiza una alternativa de solución basada en chequeos de disponibilidad y uso de DNS[5], evaluando ventajas y desventajas de su utilización respecto del protocolo BGP.

Palabras claves: administración de tráfico de red, chequeos de disponibilidad, DNS, BGP.

1 Introducción

El acceso a InterNet y la posibilidad de contar con vínculos de alta velocidad en entornos empresariales pequeños y hasta inclusive hogareños, ha causado un importante incremento en los servicios que se prestan en la red. Hoy la publicación de contenido en Internet ha tomado carácter masivo, donde quienes publican lo hacen mediante sus propios vínculos de acceso e infraestructura. Este crecimiento no esperado ha generado que los niveles de servicio de distintos portales y sistemas de correo, ente otros, se vean ampliamente degradados debido a la falta de infraestructura de comunicaciones y las fallas que pudieran ocurrir en la red.

[1] WWW: World Wide Web
[2] Internet Service Provider
[3] Border Gateway Protocol
[4] CPD: Centro de Procesamiento de Datos
[5] DNS: Domain Name System

Los servicios provistos por grandes organizaciones desde centros de cómputo preparados para tal fin, cuentan con esquemas de redundancia tanto en los servidores, como en el acceso. Generalmente las organizaciones publican sus servicios utilizando un bloque de direcciones IP propio gestionado ante algún organismo[6], y rutean dicho bloque utilizando un número de Sistema autónomo propio a través de BGP. Esta tecnología permite que ante la falla de un vínculo de red, el acceso a los servicios sea conmutado inmediatamente a otro vínculo de red, generalmente provisto por otro proveedor de servicios.

En el presente artículo se analizarán las particularidades del protocolo BGP, así como los requerimientos actuales para obtener un bloque propio de direcciones IP y número de Sistema autónomo para una organización. Asimismo se analizará el protocolo DNS y se propondrá un mecanismo de solución que permita, a través del mismo y de chequeos de disponibilidad, simular el comportamiento del protocolo BGP; brindando una alternativa de solución de menor costo y más accesible para las pequeñas organizaciones.

2 Acerca de BGP

Con el fin de que los datos puedan viajar a través de una red TCP/IP, los mismos son divididos en paquetes de información que viajan de forma independiente y se ensamblan al final del proceso. Este concepto se aplica a las redes conmutadas por paquetes, que es el tipo de red que utiliza hoy en día InterNet. El protocolo IP brinda direccionamiento a los nodos de la red de modo tal que se pueda seguir un camino para que los paquetes lleguen hacia su destino. Para ello utiliza un esquema de direccionamiento y un protocolo para la toma de decisiones conocido como "protocolo de ruteo". La versión actual del protocolo IP es la 6 (definida en la RFC 2460); aunque la más utilizada, y en la que este artículo se enfocará, es la versión 4 (definida en la RFC 791).

Para encaminar los paquetes, se define el concepto de conmutador o router, que opera en el nivel de red del modelo OSI[7] examinando las cabeceras de los paquetes IP. Los mismos poseen interfaces conectadas a más de una red, y su función principal es pasar los datos de una red a otra. Los routers permiten interconectar tanto redes de área local (LANs o Local Area Networks) como redes de área extensa (WANs o Wide Area Networks). Otra clave importante en este esquema, son los protocolos de ruteo. Los mismos nutren a los routers de información indispensable para encaminar los datos. En las redes LAN, se utilizan protocolos de ruteo interior (iGP o interior Gateway Protocol) como RIP[8] y OSPF[9] entre otros; o bien ruteo estático. En redes del tipo WAN se utilizan protocolos de ruteo exterior (eGP o exterior Gateway Protocol). En este artículo, se analizarán las características del protocolo BGP (Border Gateway Protocol).

---

[6] LACNIC es el organismo que asigna IP para América Latina

[7] Modelo conceptual en el marco de la estandarización de funciones de los sistemas de comunicación.

[8] RIP: Routing Information Protocol

[9] OSPF: Open Shortest Path First

Los protocolos de ruteo exterior como BGP (Border Gateway Protocol), tienen como propósito intercambiar información de ruteo entre organizaciones, conocidas también como sistemas autónomos. La versión actual de BGP es la 4 (BGP4) y se encuentra documentada en la RFC 1774 y RFC 4271 desde el año 1995 y 2006 respectivamente. BGP 4 es el protocolo de ruteo exterior que utiliza InterNet desde el año 1995.

BGP es un protocolo de ruteo del tipo path-vector o vector de caminos, lo que significa que cuando un router recibe información acerca de un destino, recibe la lista completa de nodos que se debe atravesar para alcanzarlo. A través de esta información se calcula el camino óptimo hacia cada punto de la red basando principalmente su decisión en la longitud del vector. Con el fin de ocultar los pormenores cada red, BGP define el concepto de *sistema autónomo*. Un *sistema autónomo* es un conjunto de routers que operan bajo una única política de ruteo y definen una o más organizaciones. La métrica de BGP se basa en la cantidad de saltos, es decir, la cantidad de sistemas autónomos que debe atravesar el paquete para llegar a la red destino. De este modo, la ruta que tenga la menor cantidad de saltos, será la elegida como mejor ruta. Una característica importante de BGP, y lo que lo hace muy potente frente a otros protocolos, es la posibilidad de definir políticas de ruteo. Las políticas son implementadas en cada router, y permiten tomar decisiones diferentes a las que podría indicar la tabla de ruteo. A través de las políticas, se puede manipular el ruteo y se pueden tomar decisiones acerca de dónde o hacia dónde transmitir el tráfico. Las políticas son implementadas a través de filtros, aceptando, rechazando o modificando rutas informadas por los vecinos de modo de manipular el flujo de los datos.

BGP utiliza el puerto 179 de TCP para la comunicación con sus vecinos. Esto representa una gran diferencia respecto de otros protocolos, lo cuales corren sobre IP o UDP. Para que un router pueda intercambiar información con otros, primero debe establecer una sesión con uno o más vecinos, a través de la cual intercambiarán mensajes. Dicha sesión debe ser configurada manualmente en ambos extremos y permite mantener un link virtual entre 2 dispositivos, el cual permitirá no solo el intercambio de información, sino el monitoreo del estado de la red. En caso de detectarse una caída sobre la sesión configurada, se podrá inferir que el par está presentando inconvenientes, lo que generará que deban actualizarse las tablas de ruteo para dejar de enviar información a través de él. Cuando un router BGP se enciende, el mismo establece una sesión contra cada uno de sus vecinos configurados, lo que se conoce como “establecer una vecindad”, y envía los correspondientes saludos definidos en la RFC. Si la vecindad es aceptada, entonces se establece el emparejamiento o “peering”. Una vez establecida la vecindad/peering, ambos routers intercambian información, enviando una copia de sus propias tablas y recibiendo la correspondiente información de su par a través de mensajes del tipo “update”. En este punto es donde las políticas de ruteo cobran un rol importante, ya que en cualquier protocolo de ruteo estándar se enviaría toda la tabla de ruteo, mientras que en BGP se enviará la información que se encuentre definida en la política, ocurriendo lo mismo al incorporar las rutas recibidas a la tabla de ruteo. Una vez que este proceso se haya completado, los routers solo intercambiarán mensajes del tipo “keepalive” para indicar que la sesión se encuentra activa y mensajes con la porción de la tabla de ruteo que haya sufrido cambio si es que lo hubiera. Con el fin de evitar procesamiento

innecesario, las actualizaciones de las tablas de ruteo solo se enviarán al iniciarse un router o bien cuando se produzca algún cambio en la red.

2.1 Requerimientos para obtener un bloque de direcciones IPv4

Con el fin de poder publicar un servicio en InterNet y que el mismo sea consumido por los usuarios, las organizaciones deben contar con un bloque de direcciones IP asignadas para tal fin. Generalmente las organizaciones solicitan a su proveedor de servicios de InterNet (ISP), un subconjunto de direcciones asignadas al mismo, durante el período de contrato que establezcan. Mediante dichas direcciones se publica el contenido en la red. El principal problema de este tipo de asignación, es que no permite el manejo de un esquema multiproveedor, ya que el rango de direcciones IP asignado temporalmente a la organización, solo será ruteado globalmente a través de la infraestructura de comunicaciones de su ISP. Si la organización quisiera contratar el servicio de conectividad a un segundo proveedor, no podrá rutear el rango de direcciones que le hubiera asignado el primero, a través del nuevo ISP. Con el fin de subsanar este inconveniente, y en el caso de que la organización quisiera contar con un esquema multiproveedor, deberá solicitar un bloque de direcciones IPv4 propio, a través de la entidad de registro que lo alcance localmente de acuerdo a la distribución internacional establecida por IANA[10]

El registro de direcciones IPv4 para la región de América Latina y Caribe está a cargo de LACNIC[11]. Cuando una organización desea obtener un bloque de direcciones IPv4, debe solicitarlo a dicha organización, cumpliendo como mínimo con los siguientes requisitos:

- Proveer información detallada mostrando como el bloque solicitado será utilizado dentro de tres, seis y doce meses
- Entregar planes de subneteo por al menos un año, incluyendo máscaras de subred y números de hosts sobre cada subred. El uso de VLSM[12] es requerido
- Entregar una descripción detallada de la topología de la red
- Realizar una descripción detallada de los planes de ruteo de la red, incluyendo los protocolos de ruteo a ser usado también como cualquier limitación existente
- En caso de que el solicitante aun no cuente con un bloque IPv6 asignado por Lacnic, solicitar al mismo tiempo un bloque IPv6 cumpliendo con la política aplicable

Adicionalmente, la organización deberá demostrar que tiene planes de proveer servicios bajo un esquema multiproveedor, que utilizará y ocupará al menos el 50% de las direcciones IP asignadas en el plazo máximo de 1 año, y pagar el costo de registración inicial y renovación anual, que a Julio/2014 asciende a U$D2500 (dos mil quinientos dólares) y U$D600 (seiscientos dólares) respectivamente.

---

[10] IANA: La Internet Assigned Numbers Authority tiene autoridad sobre todo el espacio de direcciones IP utilizado en InterNet

[11] http://www.lacnic.net

[12] Variable Length Subnet Masking

2.2 Requerimientos para obtener un número de Sistema autónomo

Un sistema autónomo está representado por un conjunto de routers que se muestran hacia InterNet bajo una política única de administración. De este concepto, se desprende que lo primero que debe cumplimentar una organización para obtener un número de sistema autónomo (ASN) que permita rutear bajo un esquema multiproveedor su bloque propio de direcciones IP, es una política de ruteo clara y coherente. La política de ruteo definida por la organización debe ser independiente a la de sus proveedores y debe ser aprobada por la autoridad de registro para la obtención del ASN. Adicionalmente, se debe demostrar que la organización operará bajo una política multiproveedor, y pagar el costo de registración inicial, que a Julio/2014 asciende a U$D1000 (mil dólares).

.2.3 Convergencia de BGP: Tipos y Tiempos

Un factor importante en cualquier protocolo de ruteo, es el tiempo de convergencia. El mismo define el tiempo que transcurre desde que se produce un cambio en la red hasta que todos los routers son notificados y cambian sus tablas de ruteo para mantener la consistencia. En BGP, los cambios pueden producirse porque un router informa una nueva ruta, o bien pueden ser advertidos por los vecinos. Cuando se establece una vecindad entre dos routers, los mismos envían mensajes de keepalive para indicar que la sesión se encuentra establecida y el vínculo está activo. Si un router no recibe dichos mensajes de su vecino por un período determinado de tiempo, entonces considerará que el mismo está presentando problemas y disparará la convergencia para actualizar las tablas de ruteo del resto de sus vecinos, dejando de anunciar las rutas aprendidas a través del primero. Los mensajes keepalive son enviados en la configuración por defecto cada 60 segundos, y si en un lapso de 180 segundos no se recibe ningún mensaje, el router considerará a su vecino caído. Es en ese momento, donde iniciará el proceso de convergencia enviando mensajes del tipo "update" a sus vecinos actualizando la información de ruteo. La convergencia en la red puede tardar tanto tiempo como nodos haya que notificar. A mayor cantidad de routers en la red, mayor será el tiempo que tarde en lograrse la convergencia total. De acuerdo al paper "Delayed Internet Routing Convergence"[13], la misma puede tardar hasta 50 minutos en completarse en redes de gran tamaño y con un gran número de cambios.

Otro factor importante es que sucesivos cambios en las tablas de ruteo, pueden sufrir penalizaciones por parte de los ISP. La convergencia en BGP implica utilizar ciclos de CPU de los routers para procesar los cambios y notificarlos. Un router que publique muchos cambios en las tablas de ruteo, puede sufrir penalizaciones por parte de los ISP, que hagan que sus rutas no sean publicadas por un período de tiempo estipulado. Este tiempo puede generar que una red determinada, no sea globalmente accesible y por ende tampoco los servicios que se publican a través de dicho bloque de direcciones IP.

[13] http://www.cs.ucsb.edu/~ravenben/classes/papers/laa01.pdf

3 Acerca de DNS

El sistema de nombres de dominio (DNS o Domain Name System), es un sistema de nomenclatura jerárquica estandarizado en la RFC 1034 y 1035 que permite asociar información con nombres de dominio. Su uso principal permite asociar nombres a direcciones IP con el fin de que los mismos puedan ser localizados más fácilmente usando un lenguaje más elegible para los humanos. Para dar soporte al servicio, se utiliza una base de datos jerárquica y distribuida que permite almacenar la información de resolución. Asimismo, el servicio permite por su naturaleza descentralizada que cada porción de la base de datos sea administrada por la entidad u organización a la que fue delegada, permitiendo de esta manera que cada administrador solo pueda manipular los datos de su propia base de datos.

Cuando una aplicación cliente necesita resolver un nombre, enviará el requerimiento de resolución a algún servidor de nombres, del cual esperará recibir como resultado, la dirección IP asociada a dicho nombre. Con el fin de agilizar el proceso y proveer mayores tiempos de respuesta, las resoluciones realizadas, son almacenadas en cachés temporales que residen en distintos puntos del proceso.

Cuando una aplicación necesita resolver un nombre, primero verificará su propia cache con el fin de determinar si la resolución se ha realizado con anterioridad y el resultado se encuentra almacenado. Si el resultado se encuentra localmente y es válido, entonces será consumido desde la base de datos local; caso contrario se procederá a enviar el requerimiento de resolución al sistema operativo, quien de modo similar verificará su propia cache de resolución con el fin de verificar si posee el dato solicitado. Si el sistema operativo no posee dicho dato, entonces enviará la consulta al servidor DNS que tena configurado. El servidor DNS realizará la consulta en nombre del cliente, hasta obtener el dato solicitado o bien un mensaje de error indicando que el nombre no puede ser resuelto. Para ello, realizará tantas consultas como sean necesarias a la base de datos jerárquica, con el fin de alcanzar la porción de la base de datos que pueda devolver la solicitud completa. Suponiendo el nombre www.ejemplo.com.ar, la primera acción que se realizará será consultar al servidor raíz. (punto), la dirección del servidor responsable de responder por el subdominio ar. Una vez obtenida dicha dirección, se consultará la dirección del servidor responsable por responder el subdominio .com.ar. Por último se consultará la dirección del servidor responsable del subdominio .ejemplo.com.ar, al cual se le realizará una última consulta por el registro www. Este último servidor, conocido como autoritativo para el dominio, responderá al primer servidor DNS, quién se encargará de entregar la respuesta final al cliente. La respuesta obtenida, estará compuesta por el nombre resuelto, la dirección IP asociada a dicho nombre y el tiempo por el cual dicho nombre será válido previo a que deba realizarse una nueva consulta para validarlo. Este último valor es de suma importancia para las caches de resolución, ya que permiten que las respuestas sean temporalmente almacenadas por los participantes intermedios, de modo tal que ante futuros requerimientos del mismo dato, los intermediarios puedan responder directamente sin la necesidad de tener que realizar el proceso completo de resolución hasta el servidor DNS autoritativo. Esta metodología permite optimizar los tiempos de respuesta ante cada requerimiento, al no tener que realizar resoluciones de nombres para cada conexión que se desee realizar desde el cliente.

3.1 Requerimientos para registrar un dominio de DNS

El registro de un dominio en el sistema de nombres de InterNet se basa en la delegación. La entidad autorizada para delegar subdominios.ar es NIC Argentina[14]. Cada país posee su entidad registrante y existen entidades registrantes a nivel global.

El procedimiento de registro es sencillo, debiendo seleccionar el nombre del dominio que se desea registrar y delegando el mismo a uno o más servidores DNS. Para realizar esta gestión es necesario crear una cuenta de usuario válida y abonar el costo de registración del dominio que a Julio/2014 asciende a $160 (ciento sesenta pesos argentinos).

3.2 Tiempos de expiración de registros y zonas de DNS

Todo recurso en un sistema de nombres está compuesto por una serie de atributos dentro de los cuales se destaca su nombre, su dirección IP y su tiempo de vida o TTL (Time to Live). Este último define cuánto tiempo debe almacenarse en caché luego de haber sido resuelto. Por cada zona definida en un servidor DNS, existe un valor global que determina el tiempo de expiración para la zona completa, y además existe un valor opcional por cada registro definido. Cuando un cliente resuelve un nombre, el mismo almacena dicho resultado por el tiempo indicado en el campo TTL en su cache. Este valor es también utilizado por servidores DNS intermedios con el fin de almacenar en cache las resoluciones hechas de modo tal de poder resolver futuras consultas de forma local.

Si bien el valor TTL forma parte de estándar definido en la RFC, algunos ISP, sistemas operativos y aplicaciones no lo tienen en cuenta y almacenan en caché los resultados por tiempos arbitrarios. Por ejemplo, versiones de Internet Explorer posteriores a 4.0, almacenan los registros de DNS por 30 minutos independientemente del valor definido en el TTL. La tendencia actual tiende a reducir estos tiempos y respetar los definidos en el campo TTL. Por ejemplo Google Chrome respeta el TTL definido en la respuesta obtenida del servidor DNS del mismo modo que lo hacen los sistemas operativos Microsoft Windows y GNU/Linux.

Es importante destacar que si bien el campo TTL permite definir la expiración para un registro dentro de una cache local, el cierre de la aplicación como por ejemplo el navegador; o el reinicio del sistema operativo, causarán el vaciamiento automático de las caches, debiéndose realizar nuevamente las consultas correspondientes en caso de querer acceder a un recurso determinado.

4 Propuesta de administración de tráfico basada en DNS

El protocolo DNS, ha sido y sigue siéndolo, un gran pilar de la red de comunicaciones de Internet. Es a través del cual se permite localizar a los recursos en esta inmensa nube de contenidos, dirigiendo el tráfico que los usuarios demandan hacia un servidor u otro. Es por esta razón, que podemos comparar a este protocolo

[14] http://www.nic.ar

con un protocolo estricto de ruteo como BGP (salvando las diferencias que existen entre ellos), reconociendo que como resultado final, y actuando en distintos escenarios, ambos permiten que los requerimientos de los usuarios lleguen al destino solicitado. El protocolo BGP, por su naturaleza, permite identificar las fallas de red y converger por sus propios medios garantizando un nuevo camino para el ruteo de los datos solicitados. El protocolo DNS, provee únicamente localización de recursos mediante la resolución de nombres. Basándose en la técnica de localización se pueden encaminar los requerimientos de los usuarios hacia el punto de la red que se desee, modificando las respuestas del servicio de DNS y basando las mismas en la disponibilidad que presente un servicio determinado. De este modo, si un servicio es publicado a través de más de un ISP y cada ISP provee un direccionamiento distinto, el mismo será accesible a través de más de una dirección IP. Adicionalmente, si dependiendo del estado de la red, el servicio de resolución de nombres pudiera responder con una IP u otra, se lograría cambiar la ruta de los requerimientos hacia otra red, permitiendo la convergencia hacia un nuevo punto de acceso a los recursos. Por lo tanto podemos concluir que lo que le falta al protocolo DNS para aproximarse al funcionamiento de BGP, es una componente que se encargue de determinar los estados de la red, disparar la convergencia; y garantizar la consistencia y estabilidad.

A continuación se analizarán los aspectos necesarios para proveer una herramienta que permita conmutar el tráfico de una red a otra, y comparar los tiempos de convergencia del protocolo BGP contra los provistos por la solución planteada. Se pretende demostrar que es posible contar con redundancia en el acceso utilizando servicios básicos como DNS y chequeos de disponibilidad con el fin de alcanzar a la gama de usuarios que no puede acceder al protocolo BGP; brindando una alternativa de solución al problema de la disponibilidad.

4.1 Arquitectura de la solución planteada

La figura 1 muestra un diagrama de red con un ejemplo de la arquitectura planteada. Para tal fin se creó una subred interna la cual utilizará direccionamiento privado, y se han seleccionado 2 (dos) direcciones IP públicas aleatorias simulando las provistas por cualquier proveedor de servicios de InterNet. Con el fin de ejemplificar la arquitectura y la convergencia, se publicarán 2 servicios sobre el dominio .ejemplo.com.ar que estarán representados por www (servidor de páginas web) y mail (servidor de correo). Se asumirá que el dominio .ejemplo.com.ar ha sido debidamente registrado ante la autoridad de registro correspondiente y debidamente delegado a los DNS cuyas IP son las provistas por cada ISP (190.40.66.10 y 200.22.130.20 para los fines del ejemplo).

Los routers de cada ISP tienen configurada la redirección de puertos sobre sus direcciones IP públicas de la siguiente manera:

- Puerto TCP/53 y UDP/53 de ISP 1 redireccionado a la IP 10.1.1.1 (DNS 1)
- Puerto TCP/80 de ISP 1 redireccionado a la IP 10.1.1.2 (www)
- Puerto TCP/25 de ISP 1 redireccionado a la IP 10.1.1.3 (mail)
- Puerto TCP/53 y UDP/53 de ISP 2 redireccionado a la IP 10.1.1.4 (DNS 2)
- Puerto TCP/80 de ISP 2 redireccionado a la IP 10.1.1.2 (www)
- Puerto TCP/25 de ISP 2 redireccionado a la IP 10.1.1.3 (mail)

El servidor DNS 1 tiene configurada su puerta de enlace con la IP 10.1.1.253 (ISP 1) y el servidor DNS 2 tiene configurada su puerta de enlace con la IP 10.1.1.254 (ISP 2). Por último, todo requerimiento hacia los servidores www y mail serán nateados con la IP privada correspondiente a cada ISP dependiendo del vínculo de InterNet por el que llegue el requerimiento de modo que la respuesta sea devuelta a través del mismo.

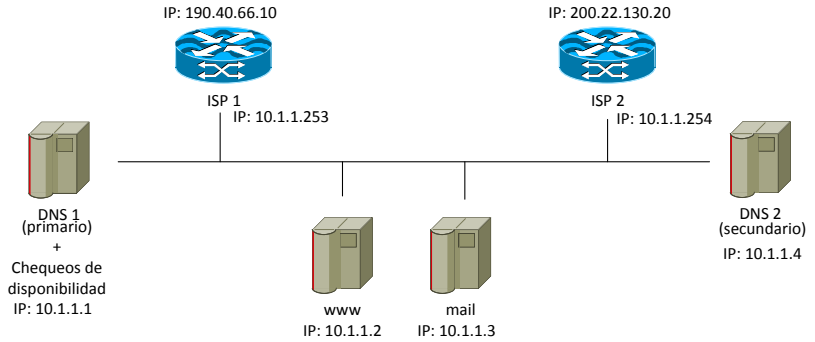

Figura 1: Arquitectura de Ejemplo de la solución Planteada

DNS 1, es el servidor primario para la zona .ejemplo.com.ar. Todo cambio en la configuración de su zona, será reflejado en el servidor DNS 2, a través de transferencias de zonas de acuerdo a lo descripto en la RFC 1035. El mismo posee un servidor BIND[15] instalado sobre un sistema operativo GNU/Linux, el cual permite que a través de actualizaciones dinámicas de DNS descriptas en la RFC 2136 y utilizando el comando *nsupdate*, se pueda hacer interfaz con el servicio para modificar el contenido de una zona determinada. Adicionalmente el servidor cuenta con un servicio de monitoreo que chequea a intervalos regulares que el servicio www y mail sea accesible a través de la dirección IP pública asignada por el ISP 2. Para tal fin se instaló el software de monitoreo libre y de código abierto ICINGA[16], que permite configurar chequeos y periodicidad de los mismos. Ante la caída de alguno de los servicios monitoreados (www o mail), ICINGA ejecutará el comando de actualización de DNS, que permitirá cambiar el registro de resolución apuntando a la dirección IP del segundo proveedor hasta que el problema haya sido solucionado. ICINGA permite que se definan diversos chequeos sobre los servicios publicados o saltos intermedios de la red con el fin de lograr un alto nivel de granularidad.

Se define como enlace principal sobre el cuál van a estar publicados los servicios, al provisto por el ISP 2, es decir que los registros www y mail en el dominio ejemplo.com.ar, serán localizables en InterNet a través de la IP 200.22.130.20 de acuerdo al ejemplo planteado. Es importante que esta premisa sea definida, debido a que es el vínculo sobre el cual deberá publicarse el DNS secundario. El vínculo del ISP 1, será utilizado como un enlace de respaldo para el acceso a los servicios, además de proveer el servicio de DNS y ser quien realice los chequeos de disponibilidad para evaluar la conmutación del tráfico.

[15] http://www.isc.org/downloads/bind/
[16] http://www.icinga.org

4.2 Esquema de pruebas

La arquitectura de red planteada, permite la detección de fallas en diversos escenarios. Con el fin de abarcar la mayor cantidad de casos, es importante respetar la ubicación de las componentes, teniendo en cuenta que el servidor DNS primario y el que realiza los chequeos de disponibilidad debe ser ubicado en el enlace de respaldo, mientras que el servidor DNS secundario debe publicarse sobre el enlace principal.

Las posibles fallas que el sistema puede detectar y sobre las que puede actuar son:

- Problema en el vínculo de comunicación del ISP 2: Al realizar el chequeo de disponibilidad desde el ISP 1, ICINGA detectará que el servicio publicado con la IP del ISP 2 no es accesible, con lo cual disparará la convergencia actualizando la zona del servidor DNS primario con la IP del ISP 1 para los servicios www y mail. Como el vínculo con ISP 2 no se encuentra disponible, la actualización de zona no se verá reflejada en el DNS secundario. Al encontrarse caído el vínculo de ISP 2, los requerimientos de resolución de nombres, solo serán atendidos por el servidor DNS 1 que es el único accesible en la red.
- Problema en un nodo intermedio de la red: Al realizar el chequeo de disponibilidad desde el ISP 1, ICINGA detectará que el servicio publicado con la IP del ISP 2 no es accesible. Esta situación podría deberse a un inconveniente de comunicación entre ISP 1 e ISP 2. ICINGA detectará que el servicio publicado con la IP del ISP 2 no es accesible, con lo cual disparará la convergencia del mismo modo que ocurrió en el caso anterior, salvo que esta vez, el problema no se encuentra en el vínculo final del ISP 2, sino que el problema reside en un nodo intermedio que causa que la red InterNet se encuentra parcialmente fragmentada. Bajo esta situación, las configuraciones de los servidores DNS no se encontrarán sincronizadas, y los clientes que puedan acceder al DNS publicado a través del ISP 1, resolverán la dirección IP de este proveedor para los servicios www y mail; mientras que los clientes que puedan acceder al DNS publicado a través del ISP 2 resolverán la dirección IP de este último y accederán al servicio por este enlace.
- Problema en el vínculo de comunicación del ISP 1: Al realizar el chequeo de disponibilidad desde el ISP 1, ICINGA detectará que el servicio publicado con la IP del ISP 2 no es accesible, con lo cual disparará la convergencia actualizando la zona del servidor DNS primario con la IP del ISP 2 para los servicios www y mail Como el vínculo con ISP 2 no se encuentra accesible desde InterNet, la actualización de zona no se verá reflejada en el DNS secundario. Al encontrarse caído el vínculo de ISP 1, los requerimientos de resolución de nombres, solo serán atendidos por el servidor DNS 2 que es el único accesible en la red.
- Caída del servidor www o mail: Al realizar el chequeo de disponibilidad desde el ISP 1, ICINGA detectará que el servicio publicado con la IP del ISP 2 no es accesible. El servicio de monitoreo, podrá chequear a través de la dirección privada el servidor. Al detectar que el mismo no es accesible en un entorno de LAN, podrá tomar la decisión de no disparar la convergencia, ya que el servicio no será accesible a través de ningún ISP por presentar una falla o baja temporal localmente.

En todos los casos planteados, ICINGA continuará monitoreando los servicios. Ante la detección de un cambio como ser que el servicio es nuevamente accesible

mediante la dirección IP del vínculo primario, se disparará la convergencia nuevamente para volver a operar bajo una situación normal.

4.3 Conmutación del tráfico

La conmutación del tráfico es disparada mediante el servicio de monitoreo ICINGA. El mismo permite que sobre un servicio de monitoreo configurado, se pueda definir un manejador ante un evento dado. Los principales eventos en el chequeo de un servicio pueden ser "up" (el servicio se encuentra funcionando correctamente) o "down" (el servicio está presentando fallas). El manejador se ejecutará cada vez que ocurra un cambio en el estado de un servicio y permitirá ejecutar un comando configurado que se encargará de disparar la convergencia.

La elección de ICINGA se basa en la posibilidad de consultar a través de una interfaz bien definida utilizando REST el estado de un chequeo determinado. Esta tecnología permite definir una interfaz de comunicación estándar para obtener datos de monitoreo o bien cambiar políticas sobre los chequeos.

Los comandos a ejecutar desde ICINGA, pueden ser desde simples scripts escritos en bash[17] a complejos programas escritos en Perl[18] o cualquier lenguaje de programación que permitan realizar consultas a bases de datos. Al momento de invocar el comando, pueden pasarse parámetros al mismo indicando el nombre del servicio que acaba de cambiar, su estado y variables predefinidas en el chequeo como por ejemplo la nueva IP a la que debe conmutarse el tráfico. Con estos datos, se puede crear un simple script de bash que se encargue de actualizar la información en el servicio DNS a través del comando *nsupdate*. Un ejemplo simple de script sería:

```
#!/bin/bash
cat<<EOF | /usr/bin/nsupdate -D -y
tm:xq6tQuPF8b8NAVlUYtko4xclMN57eeJXHiiMnY4y67+NjUv0iXnG
ST0QIdCSlIlN9ClzPEKpbDHsoUkWPnMhJw==
server localhost
zone ejemplo.com.ar
prereq yxdomain www.ejemplo.com.ar
update delete www.ejemplo.com.ar A
update add www.ejemplo.com.ar 60 A 190.40.66.10
send
EOF
```

5 Conclusiones: Ventajas y Desventajas de uso de la solución planteada

La utilización de tecnologías para brindar esquemas de alta disponibilidad en el acceso resulta necesaria para cualquier organización que provea servicios en InterNet.

[17] http://www.gnu.org/software/bash/
[18] http://www.perl.org/

El protocolo BGP permite conmutar el tráfico de red de un proveedor a otro fácilmente debido a su naturaleza. El principal problema de las soluciones basadas en BGP, radica en los requerimientos necesarios para obtener un bloque de direcciones IP propio, un número de sistema autónomo y la infraestructura de comunicaciones necesaria con el fin de procesar las tablas de ruteo, además del costo económico asociado. Otro factor importante a tener en cuenta en el uso de BGP es que la conmutación del tráfico no puede realizarse parcialmente en organizaciones pequeñas debido a los impedimentos planteados de no publicar redes con una máscara inferior a los 24 bits. De esto resulta que la conmutación en BGP debe realizarse para 254 direcciones IP en una misma operación como mínimo. Por último, es importante tener en cuenta que reiteradas actualizaciones de BGP causadas por un enlace de red inestable, pueden causar una penalización para las organizaciones debido al procesamiento que ello implica, lo que puede generar que la información no sea propagada por los vecinos.

La solución propuesta brinda alta disponibilidad en el acceso basada en el protocolo DNS, lo cual implica menores requerimientos al momento de realizar el registro de un dominio, menores costos de mantenimiento y una infraestructura de red más sencilla. La misma es más accesible a pequeñas organizaciones que no cuentan con la debida infraestructura para afrontar los requerimientos impuestos para la obtención de un bloque de direcciones IP propio. Adicionalmente, permite que la conmutación del tráfico pueda realizarse parcialmente para un único servicio, basándose en tantas métricas como chequeos puedan realizarse (disponibilidad, ancho de banda, horarios, etc.). El tiempo de propagación de cambios puede variar dependiendo del tipo de cliente que realice la resolución y las configuraciones locales definidas. Es importante publicar registros de DNS con tiempos de expiración cortos, lo que generará una mayor cantidad de consultas, pero permitirá actualizar las caches intermedias con mayor frecuencia. Otro factor importante a tener en cuenta es que los cambios de DNS no sufren de penalizaciones en caso de ser reiterados como en el caso de la actualización continua en BGP.

Por último es importante destacar que si bien la tecnología propuesta dota a las pequeñas organizaciones de una herramienta importante al momento de evaluar un esquema de alta disponibilidad en el acceso, la misma puede resultar muy útil en combinación con el protocolo BGP para las grandes organizaciones. Los grandes ISP pueden utilizar el protocolo BGP para converger tráfico de red de un vínculo a otro ante una caída global, mientras que ante una situación puntual y de menor envergadura, puede ser útil converger utilizando el protocolo de resolución de nombres.

6 Referencias

1. Douglas E. Comer. Internetworking with TCP/IP Volume One (6th Edition). 2013. ISBN-13: 978-0136085300
2. Liu C; Albits P. DNS and BIND (5th Edition) 2006. ISBN 978-0-596-10057-5
3. Iljitsch Van Beijnum BGP. O'REILLY. 2002. ISBN 978-0-596-00254-1
4. RFC 2460. Internet Protocol, Version 6 (IPv6). Specification
5. RFC 791. Internet Protocol.

6. RFC 1774. Border Gateway Protocol. Superada por la RFC 4271
7. RFC 4271. Border Gateway Protocol 4, Enero 2006. Deja obsoleta RFC 1774
8. RFC 1034. Domain names - Concepts and facilities
9. RFC 1035. Domain names - Implementation and specification
10. ISC BIND: http://www.isc.org/software/bind
11. Border Gateway Protocol: http://www.bgp4.as/