**Pregunta 1.** Explica que es una política de encaminamiento y como se implementa.

Asumiendo una sub-red perteneciente a un AS, una política de encaminamiento es la decisión de un AS de anunciar rutas a otros AS’s (Export Policy ), y la política de este de recibir rutas de otros AS’s (Import Policy).

Estas políticas se implementan mediante un protocolo de encaminamiento llamado BGPv4. BGPv4, funciona bajo TCP, por lo que es necesaria una conexión TCP para cada dirección.

BGP envía diferentes mensajes para cumplir su propósito, tales como:

* OPEN -> Crea conexiones BGP.
* KEEPALIVE -> Comprueba que la conexión TCP, siga activa.
* UPDATE -> Envía rutas y atributos.
* NOTIFICATION -> Notifica un error.

**Pregunta 2.** Explica como escala la tabla de encaminamiento BGP en función de la cantidad de AS’s a los que está conectado un AS.

Un AS, puede estar conectados a N AS’s, por tanto recibirá N updates, con N rutas,por lo tanto utilizaremos un proceso de decisión para escalar las tablas de encaminamiento.

Este proceso de decisión se basa en:

* Implementación del fabricante.
* Mantenimiento de una BD para cada sesión BGP.
* El símbolo “>”, indica la mejor ruta.
* La mejor ruta será la que será anunciada al resto.

**Pregunta 3.** ¿Pará que sirve definir una dirección de loopback en un router? ¿Qué tipo de dirección es?

Si no se hace, y se da el caso de que un enlace físico cae, se detectaría que no hay ninguna interfice activa, cosa que haría que la sesión BGP finalizara.

Para evitar esto, definimos una interface de loopback, la cual tiene que ser una dirección publica/privada diferente de 127.0.0.0/8.

Resumiendo, se utiliza la interface de loopback para evitar que la sesión BGP caiga si un enlace físico cae.

**Pregunta 4.** ¿Cómo resuelve BGP el problema de los blucles?

Mediante el AS\_PATH\_VECTOR. Si se detecta un bucle, no se anunciara la ruta.

**Pregunta 5.** ¿Qué diferencia hay entre IBGP e EBGP?

I-BGP -> Se utiliza como protocolo de enrutamiento dentro de un mismo AS para anunciar las redes internas.

E-BGP -> Se utiliza como protocolo de enrutamiento entre AS’s, según la política, se puede decidir que redes internas se desea compartir, si es que se desea compartir alguna de ellas.

**Pregunta 6.** ¿Qué diferencia hay entre las redes que anuncia OSPF y las que anuncia BGP (e.g. con el comando network)?

OSPF -> Se utiliza para anunciar las redes publicas y privadas SIEMPRE dentro de un mismo AS.

BGP -> Se utiliza para anunciar redes publicas que se desea que sean accesibles desde otros AS’s.

El comando Network activa el protocolo OSPF en todas las interfaces del router que su dirección IP estén dentro del rango de la red

Este proceso en BGP no es igual, cuando introducimos el comando network, BGP busca en la tabla de rutas un prefijo y longitud exactamente igual del que hemos introducido en network y si existe, BGP pone esa ruta en la tabla BGP, por lo que será publicada. Por ejemplo, si en la configuración de BGP escribimos el comando “network 128.107.0.0 mask 255.255.255.0”, entonces BGP buscará en la tabla de rutas esa red con misma máscara, y si existe, la agrega a la tabla BGP para así publicarla.

**Pregunta 7.** Explica la diferencia entre un atributo BGP conocido (“well-known”) y otro opcional. Idem si el atributo es mandatorio y discrecional. Menciona algún atributo que tenga la característica de ser conocido y discrecional, otro que sea conocido y mandatorio y otro que sea opcional y transitivo.

Los atributos well-known, deben de ser soportados pro cualquier implementación de BGP, mientras que los opcionales no.

Los atributos mandatorios siempre son enviados en los mensaje UPDATE, mientras que los que son discrecionales no.

Ejemplos:

* Well-known & mandatory -> AS\_PATH
* Well-known & discrecional -> LOCAL-PREFERENCE
* Opcional & transitivo -> COMMUNITY

**Pregunta 8.** ¿Qué significa que en una tabla BGP aparezca el atributo ORIGEN como incompleto? ¿Qué acción ha ejecutado el administrador del sistema para que aparezca como incompleto? ¿Qué efectos tiene dicha acción?

**Pregunta 9.** ¿Qué relación hay entre los atributos ATOMIC AGGREGATE y AGGREGATOR?

* AGGREGATOR -> Se utiliza para agregar una nueva red.
* ATOMIC AGGREGATE -> Se utiliza para avisar a los componentes de la red BGP de que alguna información se ha perdido a causa de la agregación de una ruta, y que por tanto el camino actual podría no ser el mejor para llegar al destino.

**Pregunta 10.** Qué diferencia hay entre una política BGP inbound y una outbound. Qué atributo BGP te permite generar una política outbound?

En la política inbound, se escoge cual es el enlace de entrada.

En la política outbound se escoge cual es el enlace de salida.

El atributo que se utiliza para generar políticas de outbound es

LOCAL-PREFERENCE

El atributo utilizada para escoger el enlace de entrada -> MULTI-EXIT-DISCRIMINATOR

**Pregunta 11.** ¿Qué es una política de “AS-path-prepending?. Explica mediante un ejemplo sencillo como un ISP puede usar esta política. ¿Qué atributo BGP permite definir a un ISP una política de tráfico de tipo “outbound”? Explica mediante un ejemplo sencillo como un ISP puede usar esta política.

Consiste en forzar una ruta, dado que BGP por defecto escoge la ruta más corta, y existen casos en los que no deseamos que se realice de esta forma.

Lo haremos utilizando el atributo LOCAL-PREFERENCE

**Pregunta 12.** Explica la diferencia entre una comunidad “NO-EXPORT” y una comunidad “NO-ADVERTISE”. Pon un ejemplo de uso de cada una de ellas.

* NO-EXPORT -> Todas las rutas con este atributo NO DEBEN SER anunciadas fuera de nuestro AS.
* NO-ADVERTISE -> Todas las rutas con este atributo NO DEBEN SER anunciadas a los otros vecinos BGP dentro de nuestro AS.

**Pregunta 13.** ¿Qué diferencia hay entre asignar un “route-map” con el comando neighbor en modo “in” o en modo “out”? ¿Qué efectos tienen ambas acciones sobre la tabla BGP?

La diferencia está en si la route-map se comprueba de salida o de entrada.

Indicamos la dirección del router vecino BGP, el nombre del route-map que queremos que actúe y la dirección en la que queremos que actúe IN o OUT:  
- IN: para mensajes BGP que entran en el router. Condiciones-acciones se incluirán en la tabla BGP  
- OUT: para mensajes BGP que salen del router. Condiciones.acciones se incluirán en el mensaje de salida de BGP

Los efectos en la tabla BGP dependeran de las condiciones-acciones que se apliquen a los route-map.

**Pregunta 14.** Justifica porqué los routers BGP tienen que estar i-BGP totalmente mallados y explica la diferencia entre el funcionamiento i-BGP y e-BGP respecto al anuncio de rutas.

Los routers BGP nunca anunciaran las redes que aprenden por IBGP, por lo tanto deben estar en una red mallada si o si.

La principal diferencia entre I-BGP i E-BGP son:

* I-BGP se utiliza únicamente para anunciar rutas dentro de nuestro AS.
* E-BGP se utiliza únicamente para anunciar rutas fuera de nuestro AS.
* Las redes aprendidas por I-BGP, solo serán anunciadas por E-BGP (en caso de no ser internas).
* Las redes aprendidas por E-BGP, serán anunciadas tanto por I-BGP como por E-BGP.

**Pregunta 15.** Explica que es multi-homing y explica como se puede implementar una línea de back-up con un ISP.

El Multi-Homing, es cuando un cliente X, dispone de conexiones con más de un ISP.

Una línea de backup con un ISP, se implementaría cambiando la prioridad de las líneas, de forma que la de backup tendrá menos prioridad que la principal.

Si la línea principal cae, su prioridad se elimina y la línea de backup pasara a ser la principal.

**Pregunta 16.** Explica que significa que el encaminamiento externo e interno estén sincronizados.

Significa que E-BGP, espera a que todo tu AS aprenda todas las rutas por I-BGP, antes de anunciar las redes a diferentes AS por E-BGP.

**Pregunta 17.** Asume que tienes un ISP con 100 routers BGP. Indica cuantas sesiones I-BGP necesita para funcionar correctamente. Indica que técnicas hay para reducir el número de sesiones I-BGP y explica brevemente el funcionamiento de una de ellas. Pon un ejemplo de las técnicas que has explicado enseñando la reducción de sesiones BGP a los 100 routers.

Necesitaremos (100\*99)/2 = 4950 sesiones BGP.

Podemos reducir en numero de sesiones BGP mediante el uso de:

* Route Reflectors -> split-horizon rule is modified in order the route reflector may propagate routes learnt by I-BGP connections under certain conditions reducing the number of I-BGP sessions in the AS.
* Confederaciones -> Crea Sub-Sistemas Autónomos usando números de AS privados dentro del AS. Cada Sub AS tiene que formar una malla completa y necesita sesiones IE-BGP con el resto de sub AS’s. Desde el punto de vista de un AS externo, este lo percibe como un solo AS al uso.

**Pregunta 18.** Asume que tienes un ISP con 50 routers BGP. Para que funcionen correctamente necesitas una red totalmente mallada i-BGP implicando 50\*49/2=1225 sesiones i-BGP. Explica una técnica que sea capaz de reducir el número de sesiones i-BGP y pon un ejemplo con los 50 routers BGP en que se muestre dicha reducción.

Creamos 5 confederaciones de 10 routers cada una.

Crearíamos (10\*9)/2 = 45 conexiones I-BGP en cada sub AS.

Como tenemos 5 sub AS => 45\*5 = 225, después, los mensajes E-BGP entre los sub AS, (5\*4)/2 = 10, en total 235 conexiones BGP.

**Pregunta 19.** Explica el funcionamiento de los reflectores de rutas en BGP.

* La regla de Split-Horizon que indica que las rutas aprendidas por I-BGP no se propagan se modifica para que los reflectores de rutas puedan hacerlo con los routers con los que mantiene sesiones I-BGP.
* Cada router reflector mantiene una sesión I-BGP con cada usuario (routers del cluster)
* Los routers reflectores tienen que formar una red mallada entre ellos, pero los usuarios no necesitan formarla.
* Si el mensaje BGP proviene de un vecino no cliente (Por ejemplo otro RR), entonces el RR la refleja a todos sus clientes dentro de su clúster.
* Si el mensaje BGP proviene de un cliente, el RR la refleja a todos los vecinos clientes y no clientes.
* Si el mensaje BGP se aprende de un vecino E-BGP, éste se envía a todos los vecinos clientes y no clientes.

**Pregunta 20.** Explica el funcionamiento de las confederaciones en BGP.

* Se cren sub AS’s utilizando nombres privados de AS, dentro de nuestro AS.
* Cada sub AS debe crear una red mallada con sesiones I-BGP con sus routers.
* Cada sub AS necesita sesiones E-BGP con los otros sub AS’s.
* Desde el punto de vista de un AS externo, nuesto AS es percibido como uno solo (Sin sub AS’s).

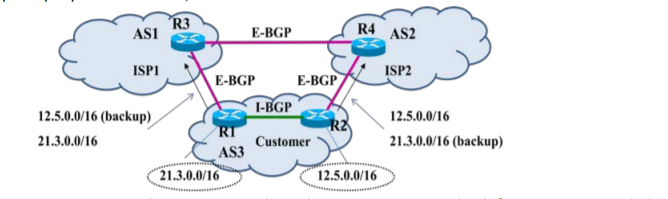
**Pregunta 21.** Explica los conceptos de escalabilidad, sincronización y convergencia en BGP y como se solucionan cada uno de ellos.

La *escalabilidad* es una propiedad deseable en un sistema, red o proceso, ya que nos indica su habilidad para reaccionar y adaptarse a los cambios (expansión, reducción o cambio de la red) sin perder capacidades y/o calidad.

La sincronización, se da cuando todas las rutas I-BGP y E-BGP se han propagado, y todos los routers conocen la topología de la red. Los routers no comunican las rutas por E-BGP hasta que todos los routers BGP de un AS están sincronizados internamente.

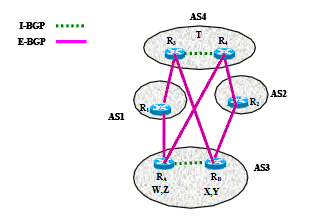
En el caso de que se de un cambio en la topología, los routers deben recalcular las rutas y actualizar sus tablas de enrutamiento, entonces, llamaremos convergencia a que todo los routers de una red conozcan la topología de la misma. Como conseguiremos esto ¿?, esperando.

**Pregunta 22.** Explica cómo puede el AS3 forzar que la línea R3-R1 es backup para la red 12.5.0.0/16 y principal para la 21.3.0.0/16 y la línea R4-R2 es backup para la red 21.3.0.0/16 y principal para la 12.5.0.0/16.

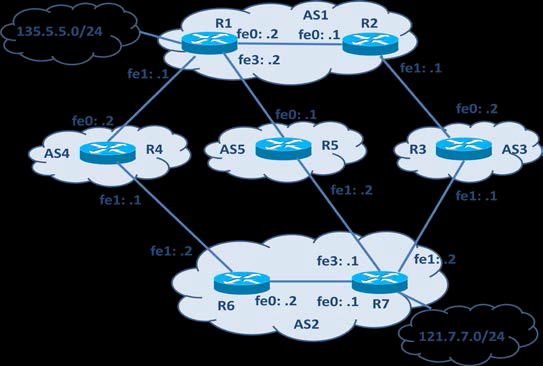


Lo conseguiremos configurando routing-maps y comunidades, y en los enlaces de backup, bajaremos la LOCAL-PREFERENCE.

**Pregunta 23.** Asume que tienes la siguiente red. Explica como AS3 puede definir una comunidad para que el tráfico que va desde AS4 hacia las redes X,Y en AS3, vaya preferentemente vía R3-RB en vez de usar otras rutas y que el tráfico que va desde AS4 hacia las redes W,Z en AS3, vaya preferentemente vía R4-RA.



**Pregunta 24.** Asume que tienes la arquitectura de la figura. Explica como AS2 puede definir una comunidad para que el tráfico que va desde la red 135.5.5.0/24 en el router R1 vaya a la red 121.7.7.0/24 conectada al router R7 preferentemente vía R1-R5 como primera opción, vía R1-R2 como segunda opción y finalmente vía R1-R4 como tercera opción



Los routers del AS2 tendran que ejecutar un send-comunity, y usar el route-map en los out, y según la dirección de origen, hara un set LOCAL-PREFERENCE según se desee.

En nuestro caso, lo que llegue de R5 tiene un LOCAL-PREFERENCE más grande que R2, el cual tendrá a su vez un LOCAL-PREFERENCE mayor que lo que provenga de R4

**Pregunta 25.** Asume que tienes un ISP con 100 routers BGP. Para que funcionen correctamente necesitas una red totalmente mallada i-BGP. Obten el número total de sesiones iBGP necesarias para que funicione correctamente el AS. Definimos ahora una configuración con 5 confederaciones: en las 3 primeras confederaciones se configuran reflectores de routers (4 Reflectores con 4 clientes cada uno), mientras que en las 2 últimas confederaciones no hay reflectores. Obten el numero total de sesiones i-BGP de cada confederación y el total de la nueva configuración en el AS.

(100\*99)/2 = 4950 -> Sesiones I-BGP, sin uso de confederaciones.

Si creamos:

* 5 confederaciones con 20 routers cada una.
* 2 sin reflectores = (20\*19)/2 \* 2 I-BGP’s
* 3 de estas confederaciones tendrán 4 reflectores con 4 clientes cada uno:
  + 4\*4 I-BGP para que los reflectores se comuniquen con sus clientes
  + (4\*3)/2 = 6 EI-BGP
  + Cada confederación tendrá -> 6+16 = 22 sesiones BGP
* En total 22\*3 + 190\*2 = 446 sesiones BGP.

**Pregunta 26.** Calcula el throughput medio y el “oversubscription ratio” de un conmutador con 8 enlaces de 10 Gb/s en el nivel de agregación y 192 puertos de 1Gb/s de capacidad en el nivel de acceso. Si los 192 servidores del nivel de acceso ocupan un 55% del enlace, ¿Está bien diseñada la red (justifica tu respuesta)?. Si la respuesta es no, indica como debería ser el conmutador para soportar los 192 servidores del nivel de acceso.

Throughput -> 8\*10/192\*1 = 416’6 Mbps

Oversupscription ratio -> 1/0,4166 = 1’8:1

Lo que los servidores necesitan:

55% de enlace -> 1 Gb/s \* 0’55 = 550 Mbps para cada enlace

Oversupscription ratio -> 1/0,55 = 1,8:1

Como podemos observar, no es suficiente, necesitamos más throughput.

Oversupscription ratio per server -> Average of servers to occupy a link capacity

Eg -> If a server occupies 60% of the link, then 1/0,6=1,666, Oversupscription ratio is of 1,66:1

**Pregunta 27.** Explica que es el “flapping”. ¿Para qué sirven las técnicas de “slow-down” en BGP? Explica el “exponential back-off”.

Flapping -> Un link canvia constantemente de un estado a otro (up/down), provocando mensajes de update, cosa que provoca low convergence, bucles y errores en la red.

Slow-Down -> Es el método que utilizamos para solventar el flapping, básicamente la solución al problema es reducir la frecuencia con la que se envían los updates del link.

Exponencial Back-Off -> Es el algoritmo que se utiliza para aplicar el Slow-Down. Cuantos más eventos de update, más aumenta el tiempo en el que se envían, si no se envían mensajes update, se reduce el tiempo de slow-down.

**Pregunta 28.** Explica que es el dampening en BGP y para qué sirve. Explica el mecanismo de dampening y la relación entre el temporizadores half-time, max-supress-limit y el valor máximo del supress-limit (dampening threshold).

Dampening -> No reportar un evento si este ocurre frequentemente.

Cada vez que ocurre un evento, se incrementa el value de penaly value, si este llega al “damp treshold”, el evento entra en DAMPENED state, y el link y la ruta pasan a estar en “down state”.

Cada vez que “no ocurre” el evento, el contador se decrementa.

Si el contador llega al “reuse treshold” el link y la ruta pasan a “up state”.

**Pregunta 29.** ¿Qué es y que implicaciones tiene el max-penalty en dampening? Si tienes un penalti = 1000, un reuse-limit = 2000, un half-life = 15 minutos, y un max-supress-limit = 60 minutos, ¿Cuál es el valor máximo del supress-limit (dampening theshold) que puedes configurar?

Es un value oculto en dampening que se usa para asegurar que no se ha entrado en valores dempening que no van a funcionar.

max-penalty = resue-limit \* 2^(max-supress-time/half-life)

max-penalty = 2000 \* 2^(60/15) = 32.000