REDES DE NUEVA GENERACIÓN

TEMA 3

Encaminamiento externo: BGPv4

1º Introducción a BGP

– Internet se construye a través de la interconexión de Sistemas Autónomos mediante protocolos de encaminamiento que permiten transmitir la información de unos a otros de manera resumida. Estos protocolos se denominan protocolos de pasarela de frontera, como BGP (Border Gateway Protocol).

Def. Un Sistema Autónomo es un conjunto conexo de redes IP y encaminadores que se encuentran bajo el control de una o varias organizaciones y que comparten una política de encaminamiento común.

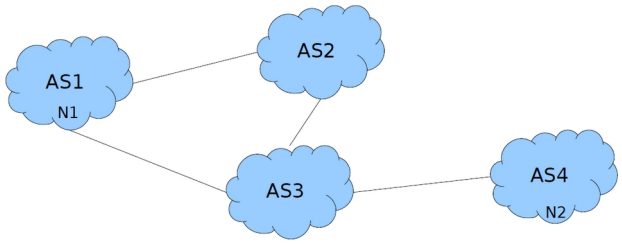
-- Cada Sistema Autónomo esta identificado por un número único de 32 bits denominado ASN, los cuales son delegados por la IANA (Internet Asociation Number Authority) a cada uno de los 5 RIR (Regional Internet Registries). Los RIR asignan un ASN a cada organización de forma individual.

-- Para un buen entendimiento de BGP debemos tener en cuenta las siguientes definiciones:

- **Vecinos (Neighbours):** Se considera que dos Sistemas Autónomos son vecinos si intercambian información de encaminamiento entre sí. También consideraremos que dos encaminadores son vecinos si intercambian información en de encaminamiento.
- **Anuncio (Announce):** Envío de información de encaminamiento a un vecino. Los anuncios contienen información sobre rutas.
- **Aceptación (Accept):** Uso de la información recibida mediante el anuncio proveniente de un vecino. La aceptación o descarte de información se lleva a cabo mediante un proceso algorítmico.
- **Originar (Originate):** Insertar información de encaminamiento en un anuncio.
- **Parejas (Peers):** Encaminadores que se encuentran en Sistemas Autónomos vecinos o en el mismo Sistema Autónomo, los cuales intercambian información de encaminamiento y políticas.

-- En BGP el envío de datos y el anuncio de rutas entre dos AS siempre se lleva a cabo en sentido contrario. Para que un AS pueda transmitir información a través de otro AS vecino, este segundo debe haber anunciado primero la ruta a utilizar al primero, el cual debe haberla aceptado.

Para que N1 pueda enviar datos a N2
- **AS4 debe originar y anunciar N2 a AS3**
- **AS3 debe aceptar el anuncio de AS4**
- **AS3 debe anunciar N2 a AS2 y/o AS1**
  - **AS2 debe aceptar el anuncio de AS3**
  - **AS2 debe anunciar N2 a AS1**
- **AS1 debe aceptar el anuncio de AS2 y/o AS3**



-- Los Sistemas Autónomos pueden ser de tres tipos:

- **Multihomed:** Sistemas Autónomos que se encuentran conectados a más de un AS, por lo que pueden permanecer conectados a internet en el caso de que una de las dos conexiones presente un fallo. No permite el tráfico de tránsito, es decir, todo aquel que no vaya dirigido al propio AS.
- **Transit:** Se trata de un Sistema Autónomo proveedor que proporciona internet a otros AS, de modo que permite el paso del tráfico de tránsito y puede establecer políticas que lo restrinjan. Tanto los ISP (Internet Service Provider) como las troncales de internet son de tipo Transit.
- **Stub**: Son Sistemas Autónomos clientes que únicamente están conectados a otro AS y no permiten tráfico que no este dirigido hacia el mismo. Puede que este tipo de AS establezcan relaciones con otros AS, las cuales no se reflejan en los servidores públicos de rutas (por ejemplo, puede darte en entornos financieros o empresariales).

1.1 La herramienta Whois

-- Whois es una herramienta que nos permite realziar consultas para obtener información a cerca de diferentes elementos que componen la red, como: Una dirección IP concreta, una ASN determinado, una persona registrada etc.

-- La base de datos de Whois se encuentra mantenida por los RIR mantienen información sobre las redes que existen en Internet, sus propietarios etc. La base de datos de Internic, la cual mantiene la información sobre los nombres de dominio, también es accesible a través d ella herramienta Whois

```
$ whois AS27733

aut-num:     AS27733
owner:       Centro Nacional de Computacion
ownerid:     PY-CNCO-LACNIC
responsible: Gustavo Amarilla
address:     Campus Universitario - San Lorenzo, 1,
address:     1439 - San Lorenzo - ce
country:     PY
phone:       +595 21 585550 []
owner-c:     GUA4
routing-c:   GUA4
abuse-c:     GUA4
created:     20040823
changed:     20050810

nic-hdl:     GUA4
person:      gustavo amarilla
e-mail:      gamarila@CNC.UNA.PY
address:     san lorenzo, 1432,
address:     1432 - san lorenzo - dc
country:     PY
phone:       +000 00 585550 []
created:     20031224
changed:     20031224
```


```
$ whois AS27733

aut-num:     AS27733
owner:       Centro Nacional de Computacion
ownerid:     PY-CNCO-LACNIC
responsible: Gustavo Amarilla
address:     Campus Universitario - San Lorenzo, 1,
address:     1439 - San Lorenzo - ce
country:     PY
phone:       +595 21 585550 []
owner-c:     GUA4
routing-c:   GUA4
abuse-c:     GUA4
created:     20040823
changed:     20050810

nic-hdl:     GUA4
person:      gustavo amarilla
e-mail:      gamarila@CNC.UNA.PY
address:     san lorenzo, 1432,
address:     1432 - san lorenzo - dc
country:     PY
phone:       +000 00 585550 []
created:     20031224
changed:     20031224
```


1.2 Encaminamiento entre Sistemas Autónomos

-- El encaminamiento entre Sistemas Autónomos con lleva mantener una entrada en la tabla de encaminamiento para cada uno de los posibles destinos de internet. Esto es un problema en IPv4, ya que únicamente permite el encaminamiento jerárquico en 2 niveles (netid y hostid) y las direcciones de clase C permiten un total de mas de 2 millones de redes diferentes, lo que conlleva un coste de cómputo muy elevado para recorrer las tablas de encaminamiento.

-- Para solventar esto se implementó el protocolo CIDR (Classless Interdomain Routing), el cual consiste en agrupar las redes de clase C no asignadas en bloques con máscaras de redes menores a /24, los cuales son delegados a los RIR. De esta manera conseguimos que una sola entrada en la tabla de encaminamiento pueda agrupar a miles de redes.

-- Para realizar el encaminamiento entre Sistemas Autónomos debemos considerar múltiples factores, como las organizaciones que gestionan cada AS implicado, decisiones económicas, conectividad física etc. Esto conlleva que utilizar encaminamiento por siguiente salto no sea adecuado, ya que se puede querer evitar pasar por determinados Sistemas Autónomos.

-- Debemos tener en cuenta que cuando se recibe una ruta hacia un destino determinado, se deben de conocer los Sistemas Autónomos que componen dicha ruta.

2º El protocolo BGP

2.1 Mensajes del protocolo BGP

-- Los mensaje de BGP se transmiten mediante TCP a través del puerto 179. Tipos de mensajes:

- **Mensaje OPEN:** Establece la sesión BGP entre encaminadores fronteras de Sistemas Autónomos. Este mensaje contiene el ASN del encaminador originaste y su identificador BGP, además de una propuesta para el valor *hold timer*.
- **Mensaje KEEPALIVE:** Confirma la recepción de un mensaje OPEN y se envían periódicamente para mantener abierta la sesión. En el caso de que un encaminador no reciba un mensaje KEEPALIVE durante el tiempo estipulado por la variable *hold timer*, se supondra que ha ocurrida un problema y se cerrará la sesión.
  - En la RFC 4271 se recomienda enviar los mensaje KEEPALIVE cada 30 segundos y establecer el valor de *hold timer* en 90 segundos
- **Mensaje UPDATE:** Transporta información de encaminamiento hacia redes conocidas y alcanzables o sobre aquellas rutas concretas que deben dejar de utilizarse. Se utiliza tras la recepción del mensaje OPEN para enviar la información de la tabla de encaminamiento completa al nuevo vecino y cuando se producen modificaciones en la red.
- **Mensaje NOTIFICACTION:** Se envía para notificar de que se ha producido una condición de error y posteriormente se cierra la sesión BGP. Cuando un encaminador recibe este tipo de mensaje, marca todas las rutas asociadas a dicho vecino como invalidas.
  - El mensaje contiene un código de error y un subcódigo con los que se puede identificar el tipo de error producido. Algunos errores son: Error en la cabecera del mensaje, error en el mensaje OPEn, error en el mensaje UPDATE, *Holt timer* superado, cierre administrativo etc.

2.1 Anuncio de rutas

-- Cuando un encaminador recibe un mensaje UPDATE con varias rutas hacia una misma red, este selecciona la ruta a utilizar en función de los dominios que considera oportunos atravesar para llegar a dicha ruta. Por defecto se considera que la mejor ruta es aquella que atraviesa un menor número de dominios, pero pueden existir factores adicionales a tener en cuenta.

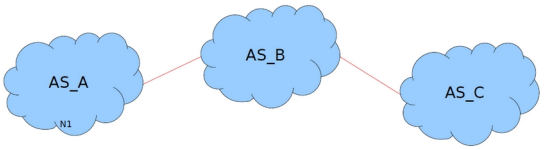
-- Los mensajes UPDATE constan de un prefijo y uno o varios atributos, los cuales influyen sobre la toma de decisión de la ruta a utilizar. Podemos diferenciar cuatro tipos de atributos:

- **Bien conocidos y obligatorios:** Estos atributos deben ser conocidos por todas las implementaciones de BGP y estar presentes en todos y cada uno de los mensajes UPDATE. En el caso de que un mensaje no tenga todos los atributos de este tipo, será descartado.
- **Bien conocidos y no obligatorios:** Estos atributos deben ser conocidos por todas las implementaciones de BGP, pero su presencia en los mensajes UPDATE es opcional.
- **Opcionales transitivos:** No se requiere que sean conocidos por todas las implementaciones de BGP, pero deben ser reenviados a otros vecinos. Aunque no se conozca el router emisor, estos atributos deben ser reenviados junto a la propagación del mensaje UPDATE.
- **Opcionales no transitivos:** No se requiere que sean conocidos por todas las implementaciones de BGP, además de poder ignorarse y no ser reenviados a otros vecinos. Normalmente, si no se reconoce un atributo de este tipo, el router lo descartará no lo reenviará en la porpagación del mensaje UPDATE.

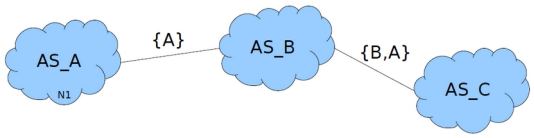
2.1.1 Atributos más comunes

- **ORIGIN:** Atributo bien conocido y obligatorio que identifica el origen de una ruta. Puede ser:
  - **IGP:** El origen de la ruta se encuentra en el propio Sistema Autónomo.
  - **EGP:** La ruta es externa el Sistema Autónomo (se encuentra obsoleto).
  - **Incomplete:** La ruta ha sido inyectada a BGP por algún otro método, como OSPF. Si se reciben dos anuncios de la misma ruta, uno con IGP y otro incomplete, se elegirá el primero.

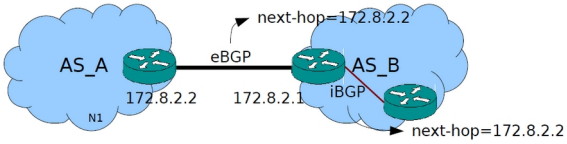
Ejemplo:
- AS_A anuncia la red N1 como interna (IGP).
- AS_B propaga el anuncio de la red N1.



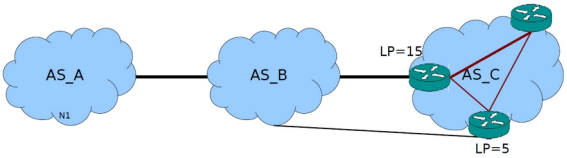
- **AS_PATH**: Atributo bien conocido y obligatorio que incluye información (el ASN) sobre los Sistemas Autónomos que deben atravesarse para alcanzar el destino. Cuando un encaminador es el que origina la ruta, incluye en la misma su propio ASN, mientras que los encaminadores que anuncian dicha ruta, lo hacen añadiendo su propio ASN al final del atributo.
  - Para evitar producir bucles, si un encaminador recibe un mensaje UPDATE con su propio ASN en el atribute AS_PATH, lo descarta directamente



- **NEXT_HOP:** Atributo bien conocido y obligatorio que establece la dirección IP del encaminador frontera que debe utilizarse como siguiente salto en la ruta.
  - Cuando se recibe a través de eBGP (BGP exterior) el parámetro contendrá la dirección del encaminador que se encuentra en el AS remoto. Esto es debido a que el encaminador frontera de dicho AS cambia el valor del NEXT_HOP por su dirección IP.
  - Cuando se recibe a través de iBGP (BGP interior) el parámetro no sufre ningún cambio. El encaminador debe tener una ruta hacia la dirección especificada en el NEXT_HOP.

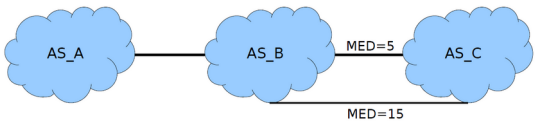


- **LOCAL_PREF:** Atributo bien conocido no obligatorio que indica la preferencia local hacia las rutas externas y tiene mayor preferencia el valor más alto. Solo es válido entre encaminadores BGP que se encuentran dentro de un mismo Sistema Autónomo (solo en iBGP, no en eBGP).
  - Cuando se recibe un mensaje UPDATE desde un encaminador de otro AS, este no contiene el LOCAL_PREF, luego se presupone un valor de 100 (este valor es configurable por defecto).



- **MULTI_EXIT_DISC:** Atributo opcional no transitivo (MED) utilizado cuando existe más de una cone-xión entre dos AS, donde el encaminador que envía el mensaje UPDATE utiliza el atributo para sugerir al otro extremo cual es la conexión predefinida. Es preferible el de menor valor.

Por ejemplo, AS_B **sugiere** a AS_C que la ruta con MED=5 es preferible a la que tiene MED=15 cuando encamine a través de AS_B.



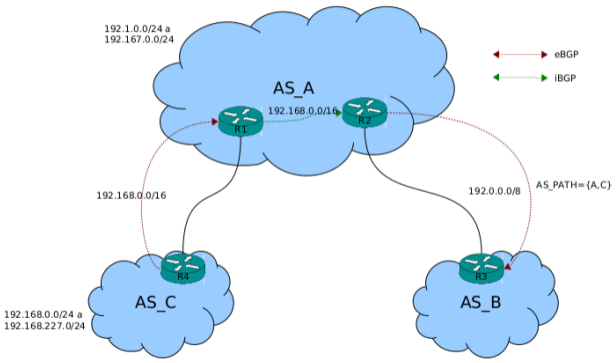
2.1.2 Proceso de decisión

-- Cuando un encaminador recibe varios anuncios de rutas para un mismo destino, es necesario decidir cual de ellos se va a utilizar para encaminar el tráfico hacia el mismo. El proceso de selección cuenta con un número de pasos, de modo que si el paso actual no es capaz de decidir la ruta a utilizar, se pasa a comprobar el siguiente.

-- A partir del 5 paso, ya no se tienen en cuenta a los vecinos en sí, sino a los protocolos utilizados y su coste. A partir de paso 7 se utilizan para descartar, pues las rutas tienen el mismo peso.

1. Se elige aquella ruta que tenga un valor mayor en el LOCAL_PREF.
2. En caso de igualdad, se elige el que se haya originado localmente (es decir, en el propio encaminador).
3. En caso de igualdad, se elige el que tenga el AS_PATH más corto.
4. En caso de igualdad, se elige el que tenga el ORIGIN menor (IGP<EGP<Incomplete).
5. En caso de igualdad, se elige el que tenga menor MED.
6. En caso de igualdad, se elige el que provenga de eBGP frente al que venga de eBGP.
7. En caso de igualdad, se elige el que tenga un coste de salto al siguiente IGP menor.
8. En caso de igualdad, se elige el que vaya hacia un vecino BGP con identificador menor.
9. En caso de igualdad, se elige el que vaya hacia un vecino BGP con IP menor.

-- La ruta que no ha sido elegida no se descarta, sino que se almacena para ser utilizada posteriormente, en el caso de que la ruta elegida deje de utilizarse o sufra algún error.



3º Problemas de BGP

-- BGP es un protocolo de encaminamiento global, sin embargo las decisiones se toman localmente en ellos encaminadores. Esto conlleva que se produzcan una serie de problemas como: Inconcurrencias, comportamientos no deterministas (wedgies), oscilaciones que evitan que se produzca la convergencia o la no recuperación ante los fallos.

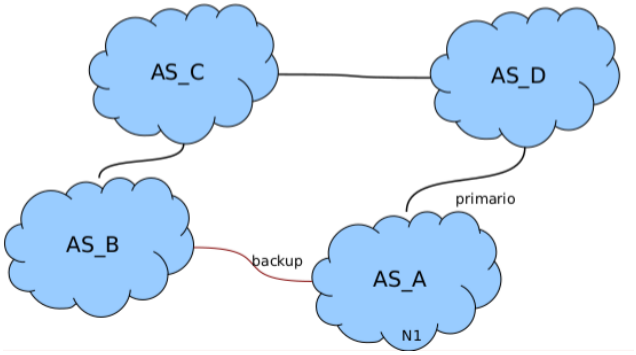
3.1 Wedgies

– Los routers BGP tienen instaurado un comportamiento determinista, sin embargo, cuando empezamos a conectar varios que se comunican entre sí, este comportamiento pasa a ser no determinista. Estos comportamientos no determinista se denominan w*edgies*, y algunos de ellos son:

- Ante la misma situación en la red elegir rutas diferentes.
- Los encaminadores pueden estar en estados que no son los esperados.
- El tráfico sigue rutas que no son las intencionadas.

EJEMPLO 1:

En el siguiente ejemplo podemos ver que AS_A tiene dos enlaces, uno con AS_D y otro con AS_B, siendo este último un enlace de *backud*, de modo que el tráfico que se dirige hacia N1 (dentro de AS_A) desde el resto de Sistemas Autónomos, debe seguir el enlace primario entre AS_A y AS_D.



Para lograr este escenario, el administrador del Sistema Autónomo B debe haber indicado que el transito se realizará desde AS_C. Esto se logra poniendo el atributo LOCAL_PREF de los mensajes que vienen desde AS_C con un valor mayor que los que vienen desde AS_A.

Supongamos que se produce un fallo en el enlace primario entre AS_A y AS_D:

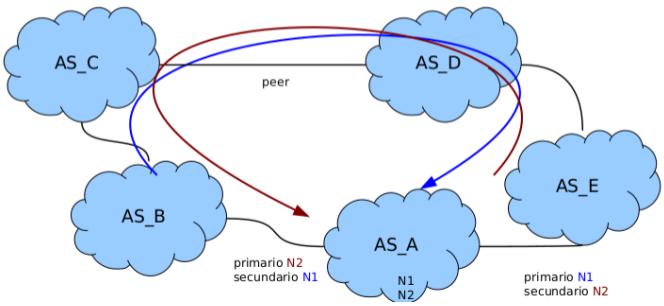
1. AS_D marca la ruta hacia N1 como inaccesible y anuncia el cambio a AS_C.
2. AS_C anuncia el cambio a AS_B.
3. AS_B elige utilizar el enlace de *backud* y anuncia la dicha ruta hacia N1 a AS_C.
4. AS_C anuncia la nueva ruta a AS_D.

Cuando se restablece el enlace primario entre AS_A y AS_D, este último anunciará dicha ruta a AS_C, sin embargo, como AS_C ya dispone de un camino activo para llegar a N1, desestimará el mismo. Debido a este, AS_C este no retransmitirá dicha ruta a AS_B, por lo que ambos seguirán retransmitiendo por la ruta que inicialmente era el *backup*.

Para volver a la situación inicial, AS_A deberá cerrar la sesión BGP con AS_B, de esta manera, la ruta que estaban utilizando para llegar hasta N1 dejará de estar disponible y tanto AS_B como AS_C la eliminarán de su tabla de rutas. Ambos volverán a utilizar la ruta inicial debido a que la guardaron cuando recibieron el mensaje anterior.

EJEMPLO 2:

En el presente ejemplo podemos ver una situación en la que el Sistemas Autónomo AS_A se encuentra balanceando el tráfico entre sus dos enlaces, de modo que los mensajes enviados hacia N1 se realizan a través de AS_E y los enviados a N2 a través de AS_B. Por otra parte, el enlace entre AS_C y AS_D es de tipo *peer*.



En el caso de que se produjera un error en el enlace entre AS_C y AS_D y este deja de ser funcional, AS_C comenzaría a encaminar todos los mensajes a través de AS_B y AS_D haría lo mismo pero a través de AS_E.

Cuando se restablece el enlace, debido a que se prefieren las rutas a través de conexiones cliente-servidor y no las *peer*, ni AS_C ni AS_D vuelven a usar las rutas anteriores. Para solventar esta situación, lo único que puede hacer AS_A es dejar de anunciar las rutas secundarias, de modo que con el tiempo, el resto de Sistemas Autónomos eliminarán dichas rutas y volverán a encaminar por las rutas primarias.

4º Encaminamiento basado en políticas

- BGP nos permite definir varios tipos de filtros, los cuales actúan sobre alguno de los campos de los mensajes para determinar que hacer con los mismos. Cada uno de los filtros que creamos lo asociaremos a un identificador, pudiendo tener más de un filtro asociado a un mismo identificador.

- Los filtros se asocian sobre los vecinos BGP que pertenecen a otros Sistemas Autónomos, de modo que si queremos aplicar una serie de restricciones sobre los mensajes que enviamos o recibimos de un determinado SA, únicamente necesitaremos crear los filtros correspondientes, asociarlos bajo un mismo identificador y aplicar este a los encaminadores de dicho Sistema Autónomo.

- Los filtros vinculados a un mismo identificador se organizan en forma de lista, de modo que su efecto se va aplicando uno sobre el otro de manera consecutiva. Finalmente, la acción llevada a cabo por el conjunto de filtros será la resultante de dicha aplicación ordenada.

- Los filtros pueden aplicarse de forma independiente a los mensajes de entrada desde un determinado AS o los de salida hacia el mismo. Esto lo indicamos en el momento de vincular el filtro a un vecino en concreto.

4.1 Herramienta prefix-list

- La herramienta prefix-list nos permite realizar un filtrado de los prefijos, diferenciando aquellos que son emitidos por el Sistema Autónomo donde nos encontramos de los que llegan desde otros Sistemas Autónomos vecinos.

- La acción principal de estos filtros es la de permitir o rechazar los mensajes BGP que se dirigen hacia un determinado vecino o que provienen del mismo. También nos permite hacer esta discriminación mediante condiciones sobre los mismos mensajes.

"ip\|ipv6" prefix-list "id" "deny\|permit" "red/n\|any" "condition"

ip|ipv6	*Indicamos si el filtro se aplica sobre prefijos IPv4 o IPv6.*
id	*Identificador al cual asociaremos el filtro.*
deny|permit	*Rechazamos o permitimos el paso de los prefijos filtrados.*
red/n	*Indicamos el prefijo sobre el que vamos a aplicar el filtro, (la palabra **any** hace referencia a todos los prefijos).*
condition	*Condición que especificará los mensajes a los que vamos a aplicar el filtro, los cuales pertenecen al prefijo indicado.*

- La condición que podemos especificar sirve para indicar la extensión del prefijo de red sobre aquellos mensajes a los cuales queremos aplicar dicho filtro. La condición puede estar formada por más de una opción concatenada, las cuales son:
  - **ge "n":** El filtro se aplicará a aquellos mensajes cuyo prefijo sea mayor que el número indicado.
  - **le "n":** El filtro se aplicará a aquellos mensajes cuyo prefijo sea menor que el número indicado.

4.2 Herramienta filter-list

- La herramienta filter-list nos permite realizar el filtrado de mensajes BGP en base a la información que contienen dentro de tu atributo AS_PATH, pudiendo así especificar aquellos mensajes a los que aplicar el filtro según la ruta que estos realizan.

bgp as-path access-list “id” “deny|permit” “expression”

id	*Identificador al cual asociaremos el filtro.*
deny|permit	*Rechazamos o permitimos el paso de los prefijos filtrados.*
expression	*Expresión que se comparará con todos los ASN que se encuentran en el AS_PATH. El filtro se aplicara en el aso de que coincida con alguno de ellos.*

– La expresión se conforma mediante el uso de comodines, los cuales pueden ser:

- **1-9** Coincidente con el número correspondiente.
- **.** Cualquier carácter.
- ***** Cero o más apariciones del patrón indicado.
- **+** Una o más apariciones del patrón indicado.
- **?** Cero o una aparición del patrón indicado.
- **^** Comienzo de línea.
- **$** Final de línea.
- **{}** Delimitadores de inicio y final de conjunto.
- **()** Delimitadores de inicio y final de confederación.
- **_** Coincide con cualquier separador: Espacio, coma, delimitador de conjunto, delimitador de confederación, principio de línea y final de línea.

4.3 Herramienta route-map

– La herramienta route-map nos permite filtrar y modificar los atributos que se encuentran especificados dentro de los mensajes BGP. Podemos especificar un número de secuencia para indicar el orden de ejecución de los filtros.

route-map “id” “deny|permit” “seq” [description “desc”]
[no] match {“expresion” | …}
[no] set {“expresion” | ...}

id	*Identificador al cual asociaremos el filtro.*
deny|permit	*Rechazamos o permitimos el paso de los prefijos filtrados.*
seq	*Número de secuencia asociado al filtro.*
desc	*Texto de descripción del filtro.*
match{…}	*Bloque de sentencia match.*
set{…}	*Bloque de sentencia set.*

– Los filtros cuentan con dos clausulas bien diferenciadas:

- **Clausula match:** Describe las condiciones que debe cumplir el mensaje para que se pueda aplicar el filtro al mismo. Cada clausula match puede contener una única condición, pero un mismo filtro puede contener varias clausulas match.

- **Clausula set:** Describe las acciones que deben llevarse a cabo sobre el mensaje cuando este cumple con todas las condiciones descritas en cada una de las secciones match. Cada clausula set puede contener una única acción, pero un mismo filtro puede contener varias clausulas set.

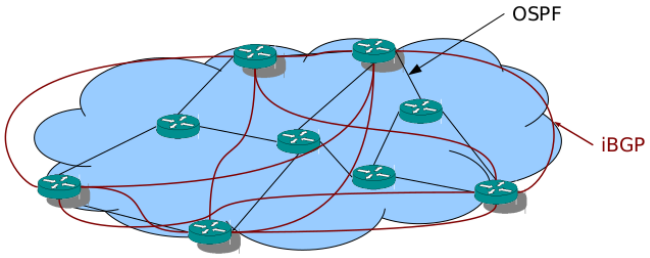
```
[no] match {
    as-path <as_path>|
    community {<1-99>|<100-500>|<nombre>}|
    ip {address|next-hop|route-source}{<access_list>|prefix-list
    <prefix_list>}|
    ipv6 {address|next-hop} {<access_list>|prefix-list <prefix_list>}|
    metric <valor>|
    origin {egp|igp|incomplete}|
    pathlimit as <asn>|
    peer {<A.B.C.D>|<X:X::X:X>|local}
    }
```

```
[no] set {
    as-path exclude .<1-4294967295>|
    set as-path prepend .<1-4294967295>|
    community {<AA:NN>|none}|
    ip next-hop {<A.B.C.D>|peer-address}|
    ipv6 next-hop {global|local} <X:X::X:X>|
    local-preference <0-4294967295>|
    metric [{+|-}]<0-4294967295>|
    originator-id <A.B.C.D>|
    pathlimit ttl <1-255>|
    vpnv4 next-hop <A.B.C.D>|
    weight <0-4294967295>|
    }
```

5º El protocolo Internal BGP (iBGP)

– El protocolo iBGP se utiliza para la comunicación entre encaminadores que forman parte del mismo Sistema Autónomo. La correcta implementación de iBGP implica que todos los encaminadores frontera que conforman el Sistema Autónomo estén comunicados entre sí (full-mesh).

– Esta restricción se implementa para que todos los routers frontera puedan recibir todos los anuncios que llegan al Sistema Autónomo, de modo que puedan decidir entre el camino más óptimo de entre todos los que llegan al mismo destino. En caso contrario, se perderá información para el correcto direccionamiento de los mensajes.



– Debido a que el número de conexiones entre los encaminadores fronteras puede crecer de manera cuadrática, se utilizan mecanismos para reducir el número de conexiones activas:

- **Reflectores de rutas:** Se configuran encaminadores como Router Reflector (RR) mientras que el resto de routers del AS se configuran como clientes de estos. Cuando un encaminador recibe una actualización mediante sBGP, la reenvía al router RR y este la reenvía al resto de routers clientes.
  - Por otra parte, cuando un encaminador recibe una actualización mediante iBGP, solo la reenvía mediante eBGP, asegurando así que llegue al router RR.
- **Confederaciones:** Consisten en subdividir un mismo Sistema Autónomo en varios subsistemas, los cuales, de cara al exterior continúan comportándose como un solo AS.
  - Cada uno de los subsistemas tiene asignado un ASN privado, los cuales no se anuncian en los mensajes que se dirigen hacia el exterior del AS. Esto se lleva a cabo haciendo que cuando un mensaje va a salir al exterior, el router frontera cambie el número de confederación en el AS_PATH por el número correspondiente al AS.