LA IMPORTANCIA DE LA SEGURIDAD EN EL RUTEO ENTRE ISPs

REUNIÓN DE OPERADORES DE REDES MÉXICO

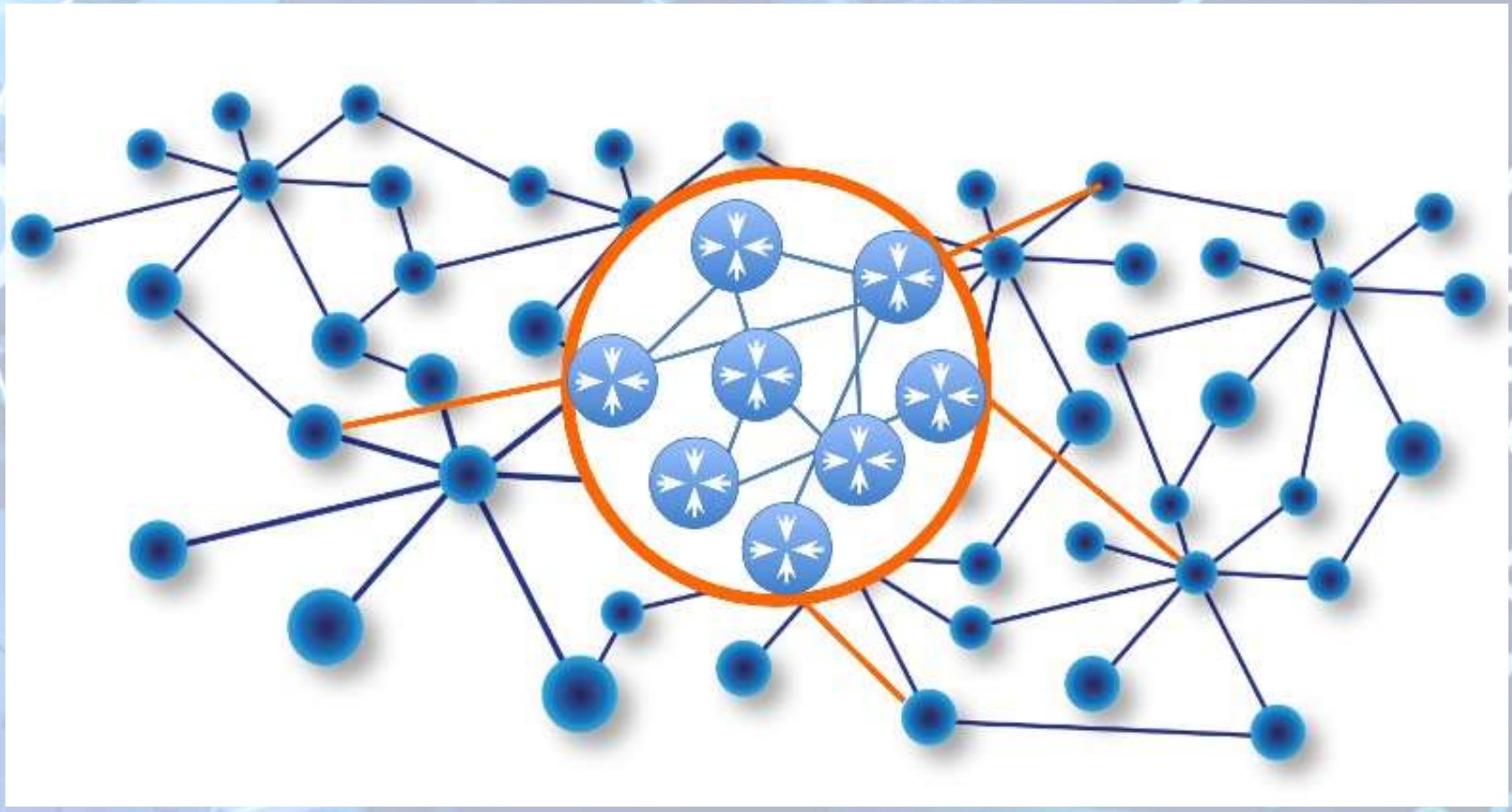
NIC MÉXICO

cudi

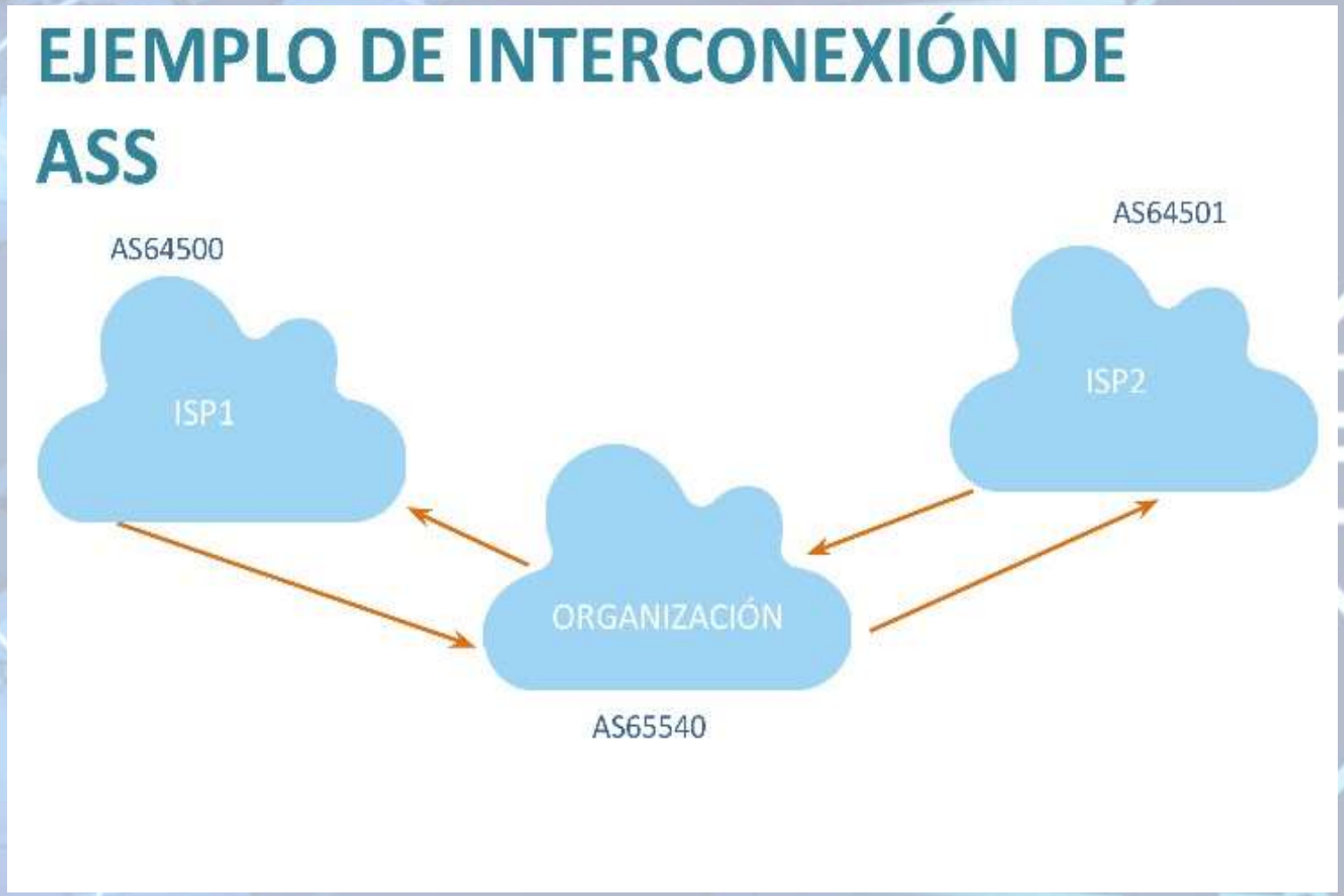
BGP
(Border Gateway Protocol)

BGP (Border Gateway Protocol) es un protocolo clave en las comunicaciones de internet. Este protocolo es utilizado para intercambiar información de enrutamiento entre los distintos proveedores de servicios registrados en internet. Garantizando que dichas rutas estén libres de bucles y representan el camino más corto entre dos extremos de una comunicación.

BGP
(Border Gateway Protocol)



BGP interconecta Sistemas Autónomos (AS)



Secuestro de rutas (Hijacking)

¿ Cómo funciona un ataque de secuestro de rutas BGP ?

Internet se basa en la interconexión de otras muchas redes de forma más o menos jerárquica. En los routers frontera de cada una de esas redes, funciona el protocolo BGP, encargado de encaminar el tráfico por una u otra red, dependiendo de cual sea el camino más corto hasta llegar a un determinado destino.

Secuestro de rutas (Hijacking)

Un ataque de secuestro BGP ocurre cuando un router frontera de una de estas redes anuncia de forma intencionada (o por un fallo de configuración) rutas pertenecientes a otra red distinta como si fuese una ruta propia.

Si esta falsa afirmación es aceptada por el resto de redes vecinas, entonces el tráfico se encaminará al atacante en lugar de su destino legítimo.

Fuga de rutas (Route leak)

El RFC 7908 indica que "el resultado de una fuga en la ruta puede ser la redirección del tráfico a través de una ruta no deseada que puede permitir la escucha o el análisis del tráfico y puede o no provocar una sobrecarga o un agujero negro. Las fugas en la ruta pueden ser accidentales o maliciosas pero con mayor frecuencia surgen de configuraciones erróneas accidentales ".

El enrutamiento inseguro es uno de las caminos más comunes para las amenazas maliciosas…

“Todos los Operadores de Red son corresponsables de la estabilidad del ruteo global”.

¿Qué podemos hacer?

- Por lo general se tienen diferentes maneras de atacar la alta inseguridad a través del internet, una de ellas es el **AS PATH Filtering**, este consiste básicamente en filtrar los prefijos de las redes vecinas, acotándolas dependiendo de las necesidades del operador de red, como, por ejemplo: Aceptar solo prefijos de AS conectados directamente, aceptar solo prefijos de AS conectados directamente y con un AS detrás del primero, negar ciertos AS de tránsito, etc.

¿Qué podemos hacer?

- También es posible validar los datos RPKI globales, políticas de ruteo, etc. mediante herramientas como RPKI validator, IRR toolset, IRRPT, BGPQ3 para la toma de decisiones BGP, así como en la configuración de sus routers.

- En el año 2017, La IETF (Internet Engineering Taks Force) lanzó un protocolo de seguridad denominado BGPsec el cual consiste en una extensión del BGP que proporciona confianza y seguridad a los AS mediante el envío de mensajes BGP UPDATE, estos mensajes contienen firmas digitales de seguridad haciendo más confiable las rutas a través de los AS.

¿Qué podemos hacer?

- **MANRS** (Mutually Agreed Norms for Routing Security) es una iniciativa comunitaria organizada por Internet Society, que tiene como objetivo mejorar la seguridad y la estabilidad del sistema del enrutamiento global. Es una forma en que los operadores de red trabajen juntos para crear un nuevo estándar de un enrutamiento más seguro y resistente.

MANRS sigue 4 acciones:

1. Filtrado
2. Anti-Spoofing
3. Coordinación
4. Validación global

¿Qué podemos hacer?

MANRS en lo referente a **Filtrado**, que tiene como objetivo evitar la propagación de información de enrutamiento incorrecta, espera de los Operadores de Red las siguientes acciones relevantes:

- Definir una política de enrutamiento clara.
- Implementar un sistema que garantice la corrección de sus propios anuncios y los anuncios de sus clientes a redes adyacentes con prefijo y granularidad de rutadel AS.
- Verificar la exactitud de los anuncios de sus clientes.
- Verificar específicamente que el cliente posee legítimamente el AS y el espacio de direcciones que anuncia.

Filtrado

- Un error común es un error tipográfico en las direcciones IP anunciadas, lo que hace que las direcciones incorrectas se anuncien desde un ASN permitido. Por lo tanto, el filtrado de los anuncios BGP de los clientes por los filtros As-path solo, es insuficiente para evitar problemas de enrutamiento catastróficos a nivel sistémico

Repaso BGP - Selección del mejor camino

1. Evaluación del NH

   El NH es alcanzable?

   SÍ → Evalúa synchronization

   NO → Ruta se descarta

2. Evaluación de synchronization

- iBGP
- Synch habilitado
- No hay entrada en la tabla de ruteo

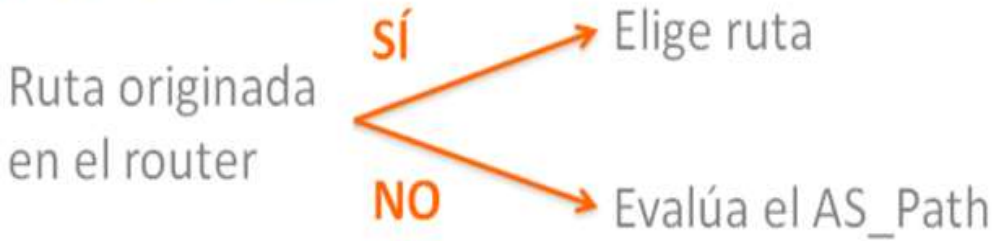
   SÍ → Ruta se descarta

   NO → Continúa el proceso de evaluación

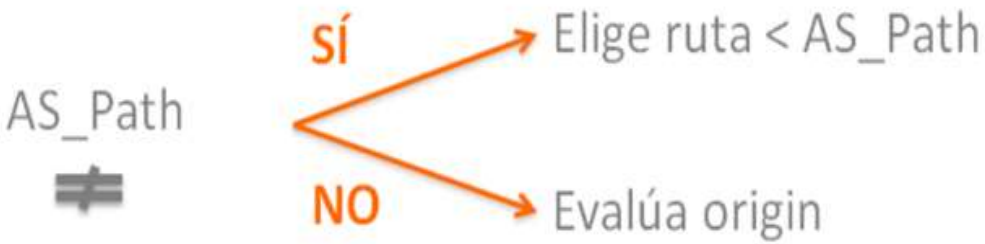
Repaso BGP - Selección del mejor camino

Repaso BGP - Selección del mejor camino

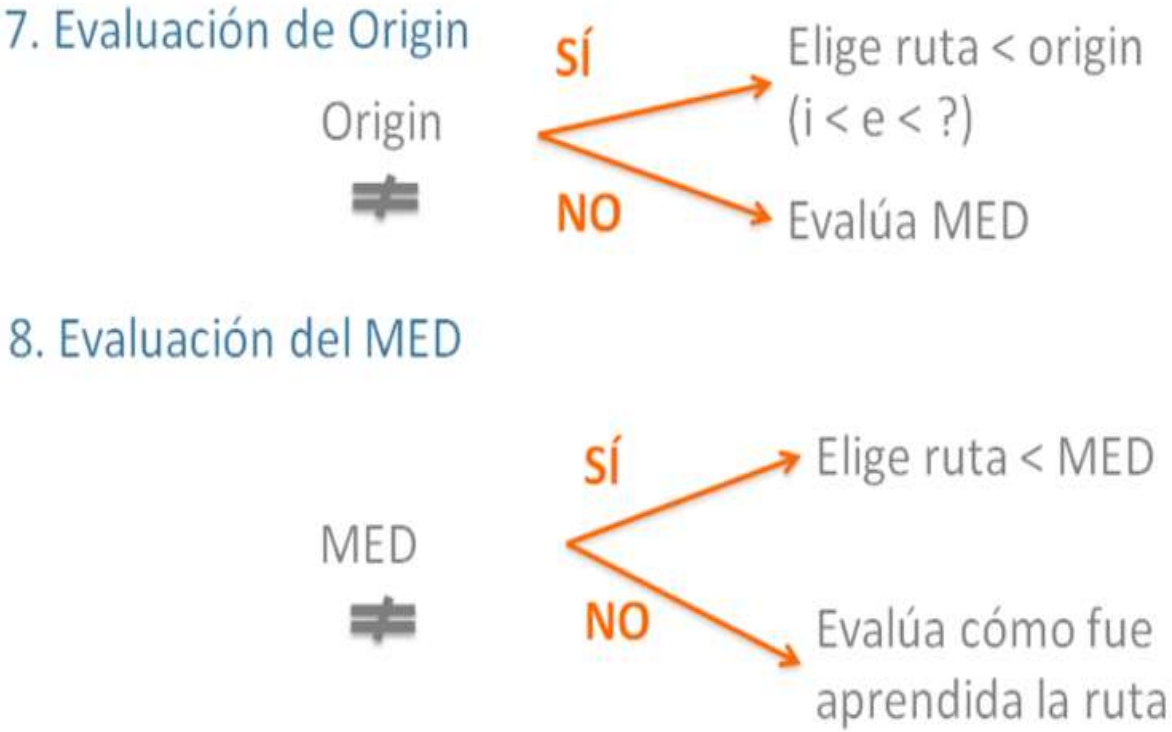
5. Origin de la ruta



6. Evaluación del AS_Path



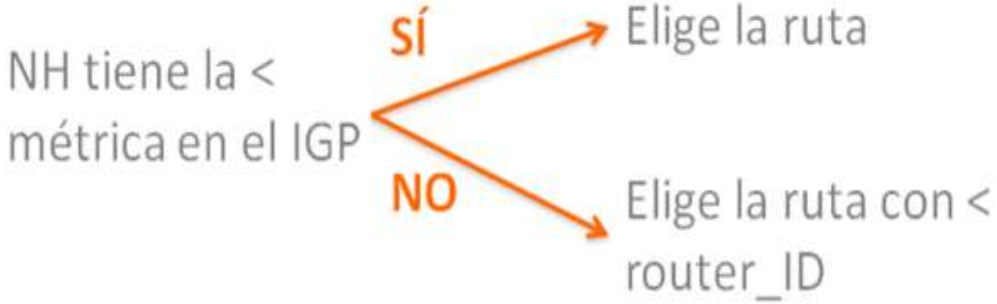
Repaso BGP - Selección del mejor camino



Repaso BGP - Selección del mejor camino

9. Evaluación de cómo fue aprendida la ruta

10. Evaluación de la métrica del NH



BGP – Filtrado de rutas

Antes de crear filtros, es importante aplicar las acciones debidas y verificar si la información proporcionada por el cliente sobre su identidad y recursos es correcta.

BGP – Filtrado de rutas

- Proceso muy importante a fin de garantizar la estabilidad de nuestro AS y los AS vecinos.
  - **Filtrado de entrada**: es aplicado a rutas aprendidas
    - Entonces la rutas no se incluyen en nuestra tabla de ruteo.
  - **Filtrado de salida**: se aplica a rutas previamente a ser anunciadas a un vecino.
    - Entonces las rutas no se incluirán en las tablas de ruteo remotas.

BGP – Filtrado de rutas

- Lo más importante es asegurar los anuncios de enrutamiento entrante, particularmente desde las redes de clientes, mediante el uso de filtros explícitos de nivel de **prefijo** (**prefix-list**) o mecanismos equivalentes.

- En segundo lugar, los filtros de ruta por **AS** (**as-path**), que se pueden usar para exigir que las redes del cliente o del ISP sean explícitas acerca de qué Sistemas Autónomos (AS) están más debajo de ellos.

BGP – Filtrado de rutas

Filtros con **prefix-list**

Access-list (ACL)	**Prefix-list**
access-list <nro_access-list> permit|deny ip <prefijo> <máscara de wildcard>	ip prefix-list <nombre_prefix-list> <nro_seq> permit|deny <red/prefijo> [**ge** length | **le** length]
access-list 101 permit ip 10.0.0.0 0.255.255.255 access-list 101 permit ip 203.0.113.0 0.0.0.255 access-list 101 permit ip 192.0.2.0 0.0.0.255	ip prefix-list Entrada seq 5 deny 10.0.0.0/8 le 32 ip prefix-list Entrada seq 10 deny 203.0.113.0/24 le 32 ip prefix-list Entrada seq 15 permit 0.0.0.0/0 le 32

Cómo se aplica el prefix-list a la sesión BGP?

neighbor **<ip-address|peer-group>** prefix-list <nombre_prefix-list> in|out

Filtros con **prefix-list** – Ejemplo

Prefix-list

```
router bgp 64496
  neighbor 203.0.113.100 remote-as 65551
  neighbor 203.0.113.100 prefix-list PEER-IN in
  neighbor 203.0.113.100 prefix-list PEER-OUT out
!
ip prefix-list PEER-IN deny 198.51.100.0/24
ip prefix-list PEER-IN permit 0.0.0.0/0 le 32
ip prefix-list PEER-OUT permit 192.0.2.0/24
```

Filtros con **Filter-list** (AS-PATH)

El filtro actúa según el **camino** hecho por los prefijos

- **Dos pasos:**

  1. Crear sentencia con expresión regular.

  ip as-path access-list **<nro_filtro>** permit|deny <regexp>

  2. Aplicar el filtro

  neighbor **<IP_neighbor>** filter-list **<nro_filtro>** in|out

Filtros con **Filter-list** - Ejemplo

```
...
 neighbor 198.51.100.22 filter-list 11 out
...


ip  as-path access-list  11 deny 64496$
ip  as-path access-list  11 deny ^645
ip as-path  access-list  11 permit _64497_64498_
...
```

Expresiones Regulares

Caracter	Función
^	empieza con
$	termina con
.	cualquier caracter
_	cualquier delimitador (espacio, comienzo, fin, coma)
[0-9]	rango del 0 al 9
[123]	1, 2 ó 3
( )	asocia
|	ó
*	cero o más veces
?	cero o una vez
+	una o más veces
\#	llama a la expresión ubicada en la posición # del regexp

Filtros utilizando Route-map

- Los route-map son similares a las sentencias de un lenguaje de programación,

  “if ……. then ……”

- Cada instancia del route-map tiene un número de secuencia.
- Son ejecutados en orden desde la sentencia con menor número de secuencia hasta el más alto. Es posible editarlos o modificarlos utilizando este número de secuencia.
- Si en un route-map, una sentencia con un determinado criterio de coincidencia resulta verdadera, la ejecución del route-map se detiene.
- Se puede utilizar route-map para permitir o denegar según el criterio encontrado por la sentencia ***match***.

Filtros utilizando Route-map

- Si no existiera una sentencia *match* dentro de una instancia de un route-map, todas las rutas resultan con criterio verdadero. Las sentencias *set* son aplicadas a todas las rutas.
- Si no existiera una lista de acceso para la sentencia *match* dentro de la instancia del route-map, todas las rutas resultan con criterio verdadero. Las sentencias *set* se aplican a todas las rutas.
- Tal como con las listas de acceso, una denegación implícita es incluida al final del route-map.
- Si múltiples sentencias *match* son utilizadas dentro de una instancia de un mapa de ruteo, todas las sentencias *match* deben resultar verdaderas para que de la instancia surja un resultado verdadero.

Route-map – Ejemplo con **Prefix-list**

```
router bgp 64496
  neighbor 203.0.113.10 route-map infilter in
!
route-map infilter permit 10
  match ip address prefix-list HIGH-PREF
  set local-preference 120

!
route-map infilter permit 20
  match ip address prefix-list LOW-PREF
  set local-preference 80
!
route-map infilter permit 30
!

ip prefix-list HIGH-PREF permit 192.0.2.0/25
ip prefix-list LOW-PREF permit 192.0.2.128/25
```

Route-map – Ejemplo con AS-PATH

```
router bgp 64496
  neighbor 203.0.113.10 route-map filter-on-as-path in
!
route-map filter-on-as-path permit 10
  match as-path 1
  set local-preference 80
  set weight 200
  set metric 127
  set next-hop 192.0.2.10
!
route-map filter-on-as-path permit 20
  match as-path 2
  set local-preference 200
  set weight 500
  set metric 327
  set next-hop 192.0.2.100

!
route-map filter-on-as-path permit 30
!

ip as-path access-list 1 permit _64505$
ip as-path access-list 2 permit _64510_
```

BGP Buenas prácticas

- Es importante que los prefijos que anunciamos fuera de nuestro AS estén sumarizados.
- Qué anuncios no debería recibir?
  - No recibir los prefijos definidos en el RFC 1918
  - No aceptar mis propios prefijos
  - No aceptar el default (a menos que se requiera)
  - No aceptar prefijos mayores de /24

¿Qué prefijos no debería recibir?

```
router bgp 64496

   network 192.0.2.0 mask 255.255.255.0
   neighbor 203.0.113.100 prefix-list in-filter in
   remote-as 64505
   neighbor 203.0.113.100
!


 ip    prefix-list  in-filter  deny  0.0.0.0/0              ! Block default
 ip    prefix-list  in-filter  deny  0.0.0.0/8 le 32
 ip    prefix-list  in-filter  deny  10.0.0.0/8 le 32
 ip    prefix-list  in-filter  deny  101.10.0.0/19 le 32    ! Block local prefix
 ip    prefix-list  in-filter  deny  127.0.0.0/8 le 32
 ip    prefix-list  in-filter  deny  169.254.0.0/16 le 32
 ip    prefix-list  in-filter  deny  172.16.0.0/12 le 32
 ip    prefix-list  in-filter  deny  192.0.2.0/24 le 32
 ip    prefix-list  in-filter  deny  192.168.0.0/16 le 32
 ip    prefix-list  in-filter  deny  224.0.0.0/3 le 32     ! Block multicast
 ip    prefix-list  in-filter  deny  0.0.0.0/0 ge 25       ! Block prefixes >/24
 ip  prefix - list  in-filter  permit 0.0.0.0/0 le 32
```

Dentro de las acciones se deben realizar algunas pruebas para diagnosticar el ASN que desea incorporarse:

- **Filtrado**: El objetivo del filtrado es evitar la propagación de información de ruteo erróneo.
  - Comprobar que el ASN no anuncia bogons (direccionamiento falso), para esto se puede utilizar informe CIDR:

    https://www.cidr-report.org/as2.0/

  - Comprobar que el ASN no estuvo implicado en incidentes recientes:

    https://bgpstream.com/

GRACIAS !

Silvia Nora Chávez Morones
NOC – CUDI
http://www.cudi.edu.mx/noc-cudi
silvia@cudi.edu.mx
noc@cudi.edu.mx
(0155)5211-3049

REUNIÓN DE OPERADORES DE REDES MÉXICO

NIC MÉXICO

cudi