lacnic 26 lacnog`16

26/30 setiembre - san josé, costa rica

BGP

¿Qué hacemos?

¿Qué no hacemos?

¿Qué podemos hacer?

¿Qué no debemos hacer?

@ nantoniello

DEFCON

... Un posible criterio !

- Te pido lo mínimo !

- Estaría bueno tenerlo

- Modo paranoico (… lo que quiero ser cuando sea grande)

- Lo que no debo hacer

BGP

- BGP multihop: no poner más hops de los necesarios

- Utilización de MD5 para autenticar al peer

- Utilizar listas de acceso para permitir actualizaciones solo de los peers (¿alguien lo realiza?)

- Control de TTL (¿alguien lo realiza?)

Generación de prefijos

- En lo posible evitar **redistribuciones** desde IGP (evitar propagar hacia afuera problemas internos)

- Posibilidad de gestión centralizada de publicaciones

- Uso interno de comunidades

- ¿Como estamos generando las publicaciones? (rutas a null0; ¿Donde?; pros y contras en cada caso)

eBGP en general...

- Filtrado de prefijos publicados

- Filtrado de prefijos recibidos (¿uso de IRR?) ¿Escalabilidad?
  Cuidado **extra** con la ruta por defecto (0.0.0.0/0 o ::/0)

- Filtrado de AS (para clientes "no tránsito")
  (¿uso de IRR?) ¿Escalabilidad?

- Publicar AS privados (uso de remove-private)

- Publicar redes privadas

- Cuando hacemos peering con caches para informar prefijos
  es saludable configurar una lista de acceso de tipo “nada-in”

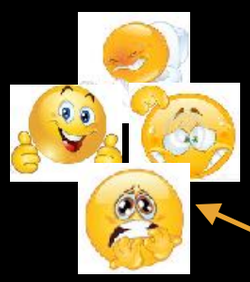
en general...

- No propagar comunidades de uso interno

- Si implementa filtrado de Bogon, mantenerlo actualizado

- RPKI (el uso por el momento solo permite validar origen)
  ¿Qué sucede si quisiera validar el camino?
  En el caso de validación de origen, ¿disparo **alarmas** o filtro prefijos automáticamente?

- Poner **alarmas** de máximo de prefijos (cuidado con bajar la sesión cuando se alcanza el máximo)



- ¿Dampening? (¿algo terrible o algo últil? ¿Tendríamos que analizar el timeout configurado?)

Posible trastorno bipolar !

Más tips...

- RTBH (remote triggered black hole)
  Requiere soporte por parte del proveedor de tránsito

- Local Black Hole

- No desagregar más de los necesario (¿balanceo de tráfico en casos de Multihoming-Multiproveedor?)

- Uso de comunidad no-export para balanceo en caso de múltiples enlaces con un mismo proveedor (bloques específicos con no-export + bloque sumarizado sin no-export)

- Uso de comunidades acordadas entre peers

Más tips...

- ¿Uso de prepend?

- ¿Uso de local-preference?

- Reflectores de rutas ¿pros y contras? ¿cuando? ¿donde? ¿cuantos?

- BGP multi path vs. Múltiples sesiones BGP vs. balanceo en capas inferiores (Bunddle)

Crisis de identidad!

Pura vida !

BGP y otros…

- MPBGP

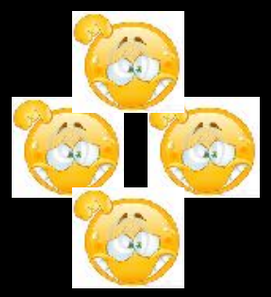
RFC 4798

Crisis de los 50!

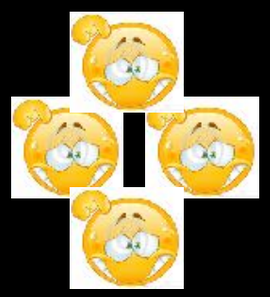
- Uso de 6pe (requiere MPLS)
- Full mesh BGP o uso de reflectores: ¿Cuándo? ¿Consideraciones?
- Usos de iBGP
- Políticas y técnicas de ruteo para intercambio de tráfico regional

Otros

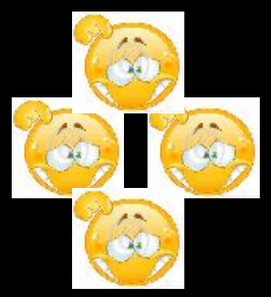
No propio de BGP pero relativo...



- Balanceo de tráfico por múltiples enlaces (resolver el problema de tener routers de borde en sitios remotos, conectados con enlaces de diferentes anchos de banda)



- Políticas, técnicas y modelos de intercambio de tráfico en IXPs
  ¿Inter IXPs?



- ¿Donde se realiza y realizará fuerte intercambio de tráfico? ¿Que políticas y gestión se necesitan?

#Lacnic26

#Lacnog16