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?)

Generación de prefijos

- En lo posible evitar **redistribuciones** desde IGP (evitar propagar hacia afuera problemas internos… y hacia adentro del IGP problemas externos)

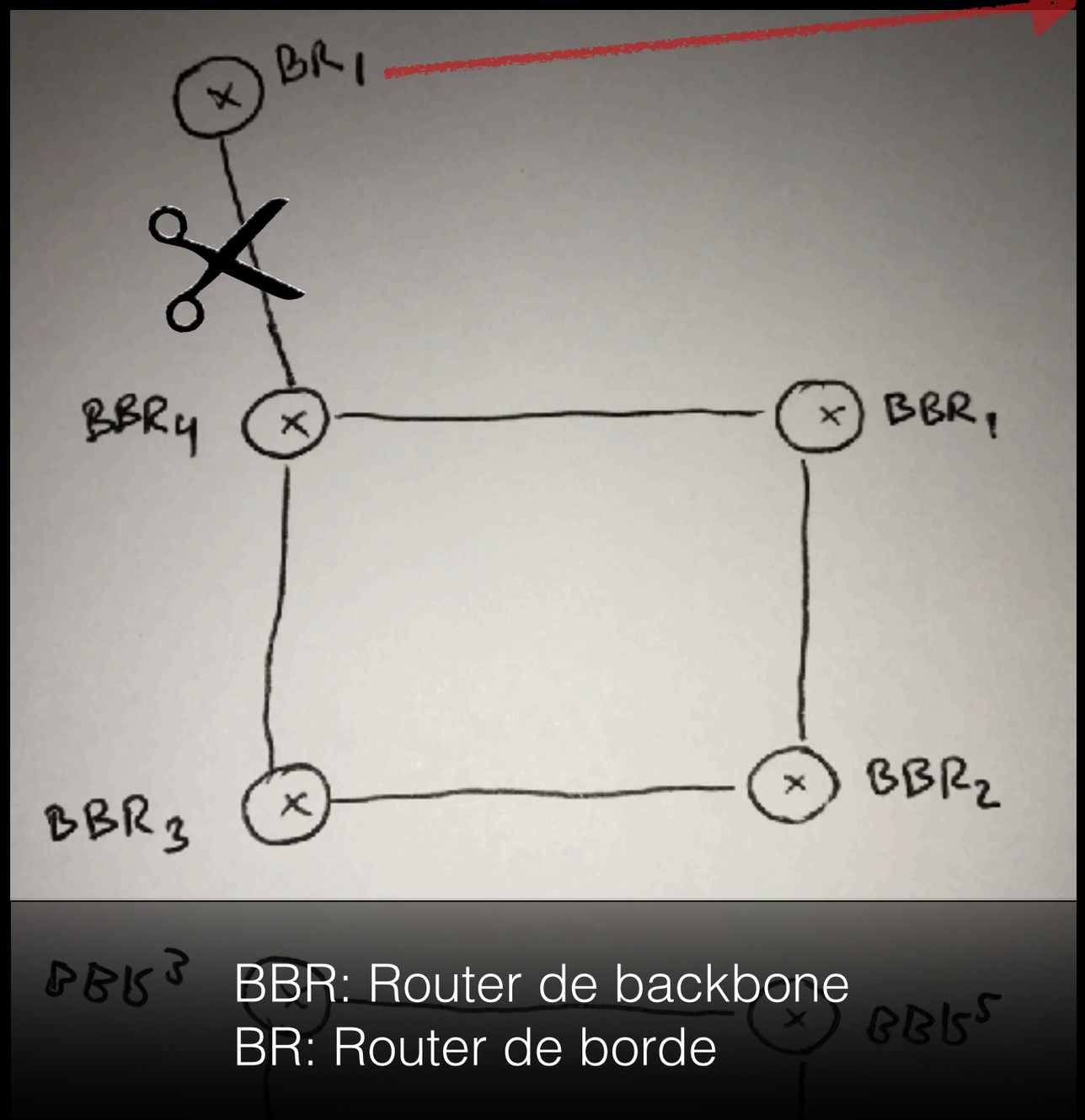
- Posibilidad de gestión centralizada de publicaciones

- Uso interno de comunidades

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

Generando rutas para publicaciones BGP…

¡Resistiendo la tentación!



ruta estática a *null*

BBR: Router de backbone
BR: Router de borde

¿Problemas?

Generando rutas para publicaciones BGP…

¡Mejorando bastante!

BBR: Router de backbone
BR: Router de borde

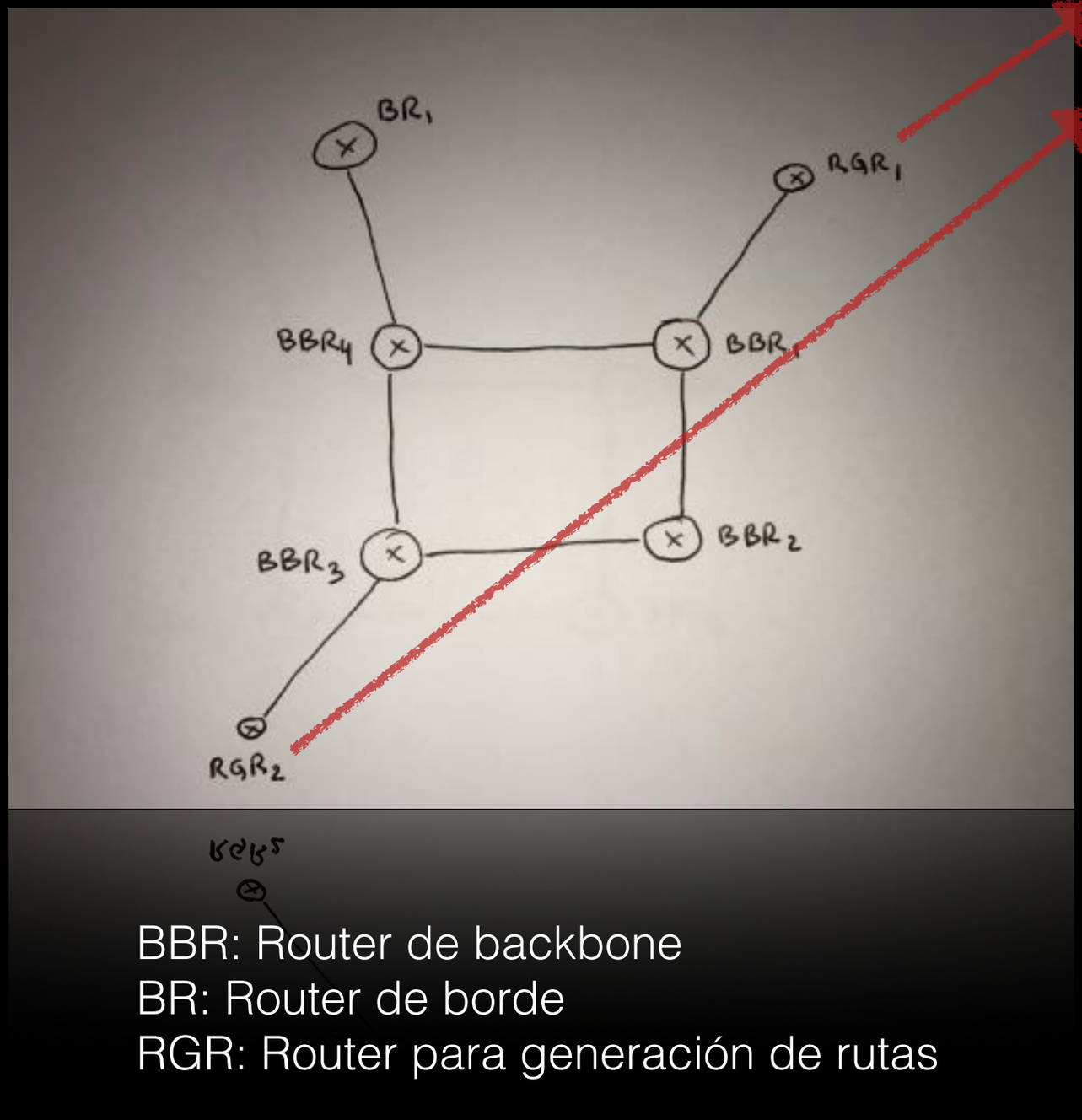
ruta estática a *null*

¿Ventajas y desventajas?

Generando rutas para publicaciones BGP…

¡Mejorando bastante!

Sugerencia: agregar *route reflectors* para evitar *full mesh* BGP



BBR: Router de backbone
BR: Router de borde
RGR: Router para generación de rutas

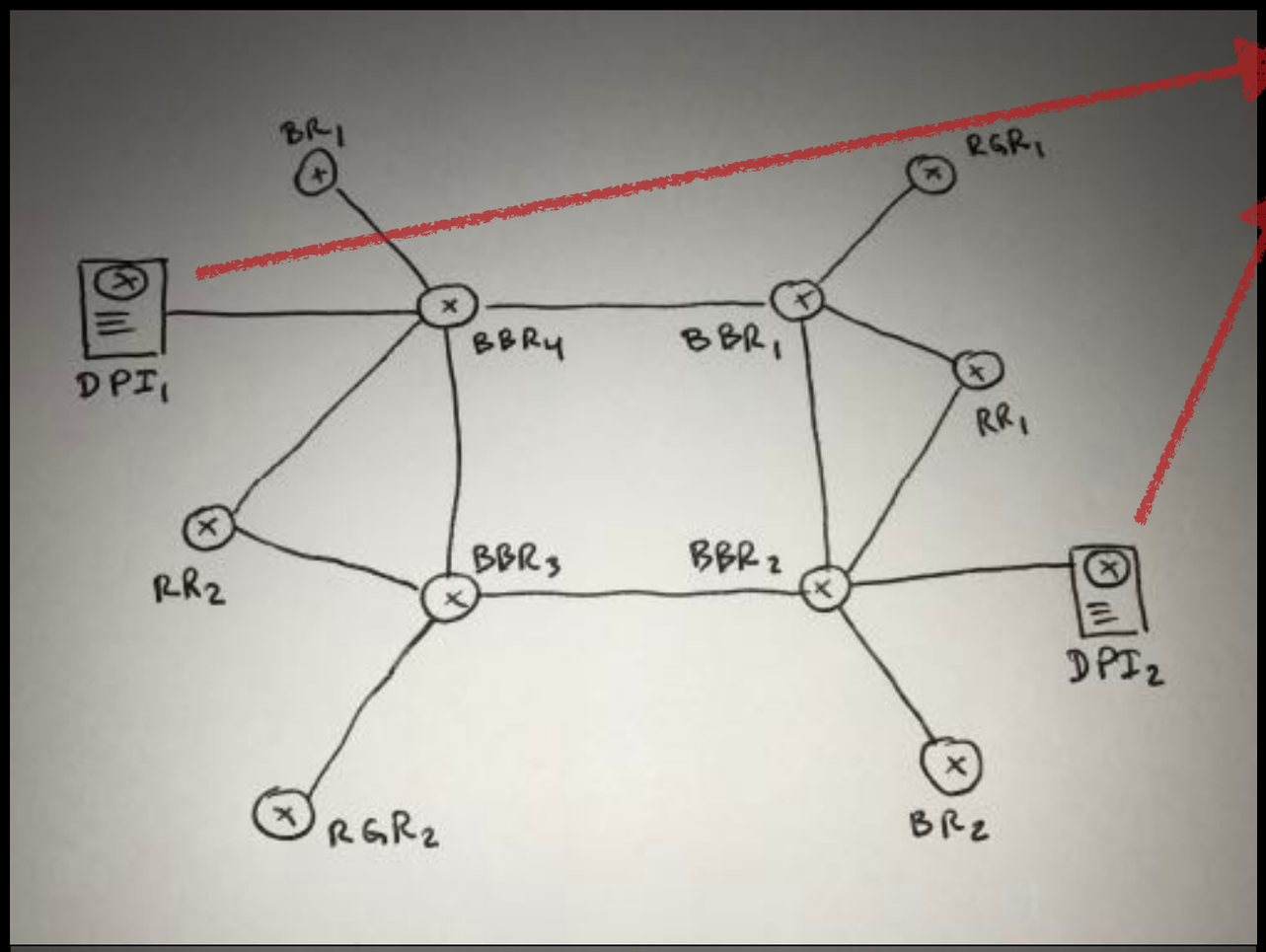
defino aquí las rutas poniendo como *next hop* una que a su vez se define como ruta a *null* en todos los routers de borde

Este sistema permite centralizar fácilmente el mecanismo de publicaciones BGP (muy útil en caso de administrar múltiples enlaces eBGP)

A su vez permite realizar fácilmente el manejo de *black holes* en forma centralizada (tanto locales como remotos)

¿Ventajas y desventajas?

Alguna idea adicional utilizando BGP...



BBR: Router de backbone
BR: Router de borde
RGR: Router para generación de rutas
RR: Reflectores de Rutas
DPI: Equipo para análisis de tráfico

En caso de recibir tráfico no deseado desde un peer (por ejemplo en un DDoS ¿cómo puedo aprovechar una arquitectura de este tipo para investigar lo que sucede?

Los DPIs publicarían una ruta específica (/32 en IPv4 o /128 en IPv6, por ejemplo) para el bloque que está recibiendo el tráfico no deseado (por ejemplo en un caso de ataque), encaminando todo el tráfico destinad a dicho bloque hacia el o los DPIs

¡ Más ideas locas !

eBGP en general...

- Control de prefijos publicados

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

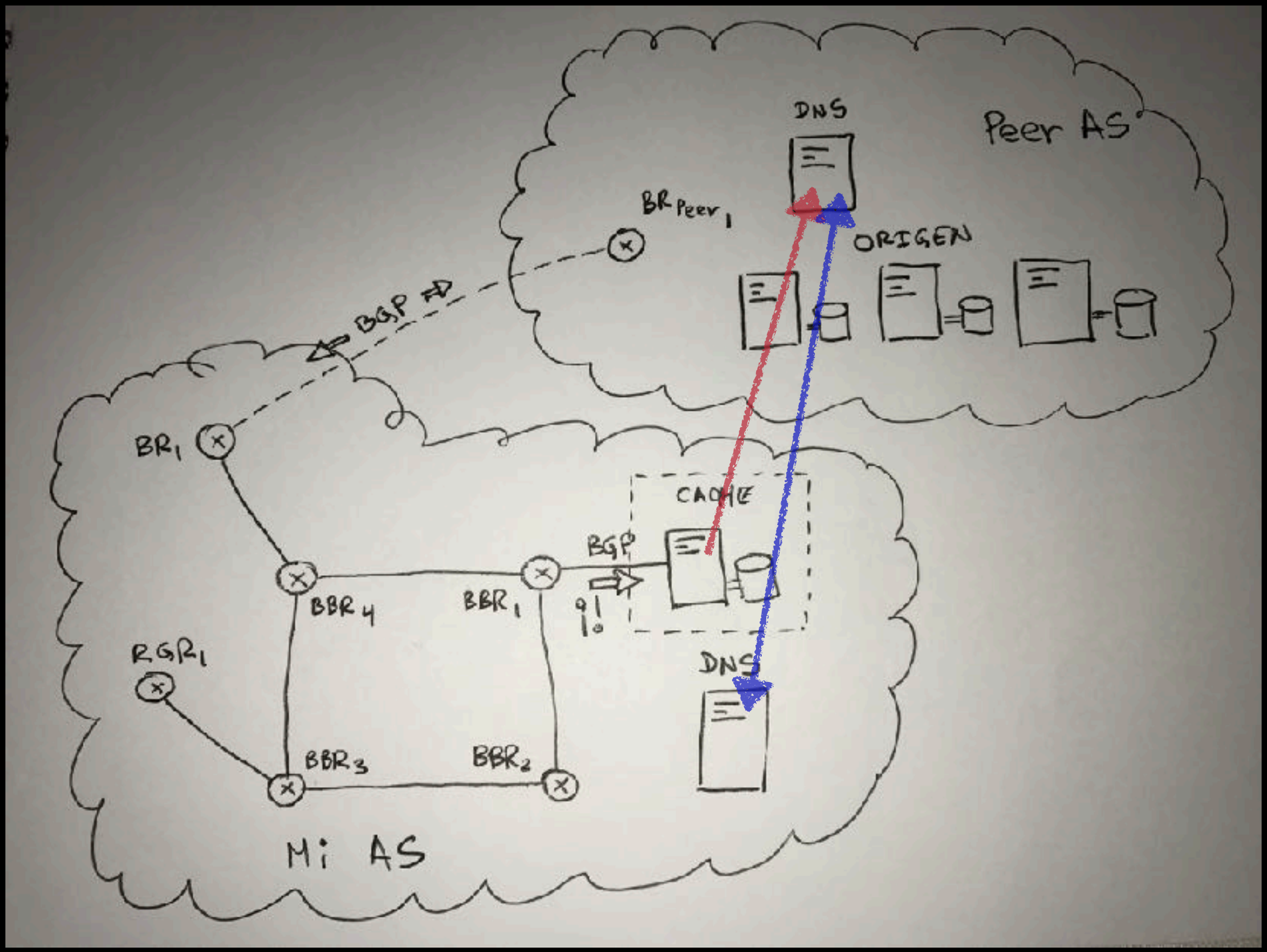
- Filtrado de AS (para clientes "no tránsito")
  (¿uso de IRR?) ¿Escalabilidad?

- Publicar AS privados (uso de remove-private)

- Publicar redes privadas (filtrado de redes privadas)

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

Un modelo general de funcionamiento de cache local



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 (como Bunddle a nivel de capa 2)

Pura vida !

Crisis de identidad!

BGP y otros…

- MPBGP

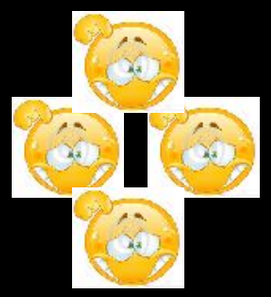
RFC 4798

Crisis de los 50!

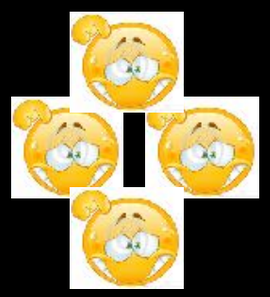
- Uso de 6pe (requiere MPLS)
- Full mesh BGP o uso de reflectores: ¿Cuándo? ¿Consideraciones?
- Usos de iBGP
- Políticas y técnicas de ruteo para intercambio de tráfico regional

Otros

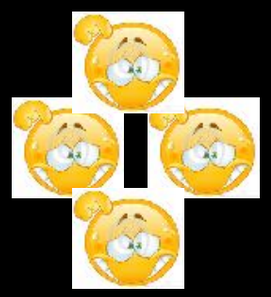
No propio de BGP pero relativo...



- 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?

#lacnic28

#lacnog2017