

lacnic
lacnog 2018

30

24/28 SETIEMBRE 2018
ROSARIO • ARGENTINA

BGP: novedades y temas en discusión

Guillermo Cicileo - guillermo@lacnic.net

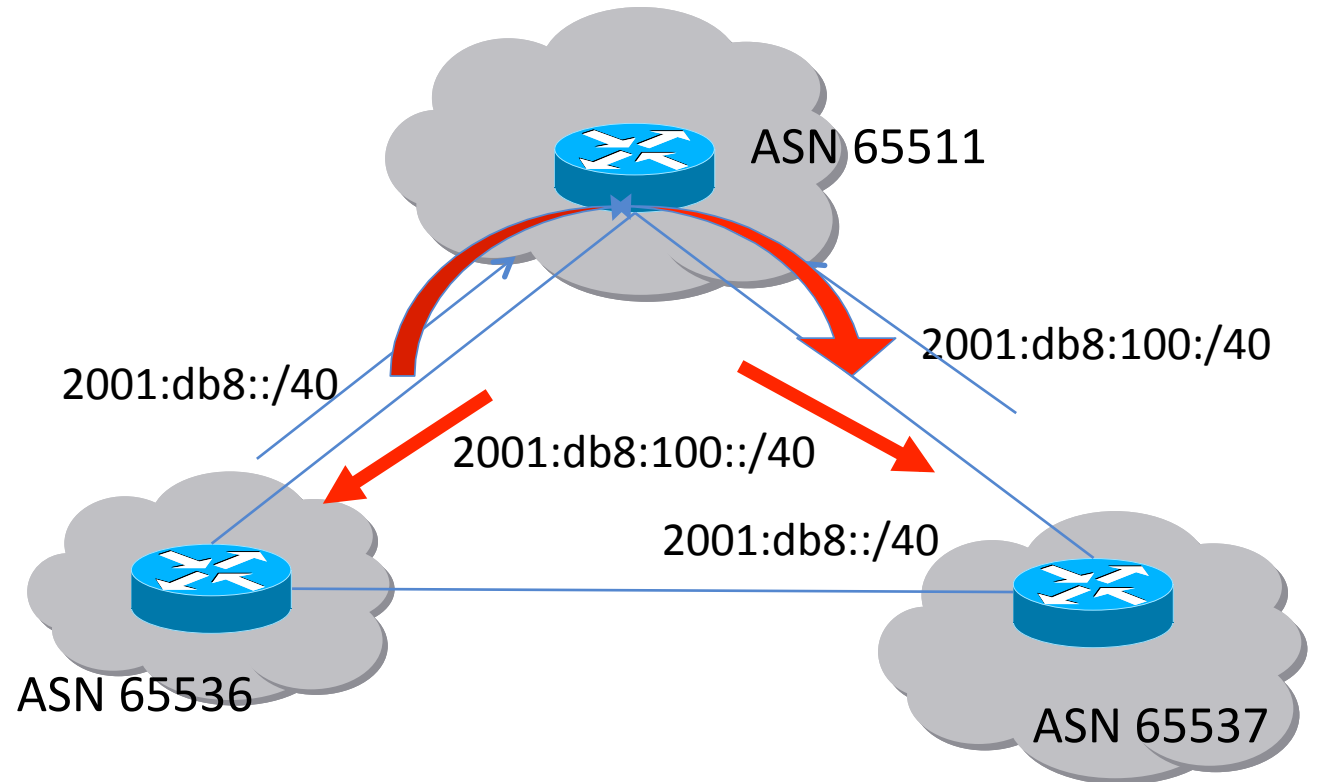
Algunas novedades en BGP

- Cambio de política BGP por default
- Roles para prevención de route-leaks
- Novedades en RPKI
 - Validation reconsidered
 - AS Cones
 - ASPA
- Uso de BGP en datacenters de gran escala

Route leaks

BGP default policy

- Comportamiento por default en BGP (muchas implementaciones): re-anunciar automáticamente todo lo que se aprende por eBGP

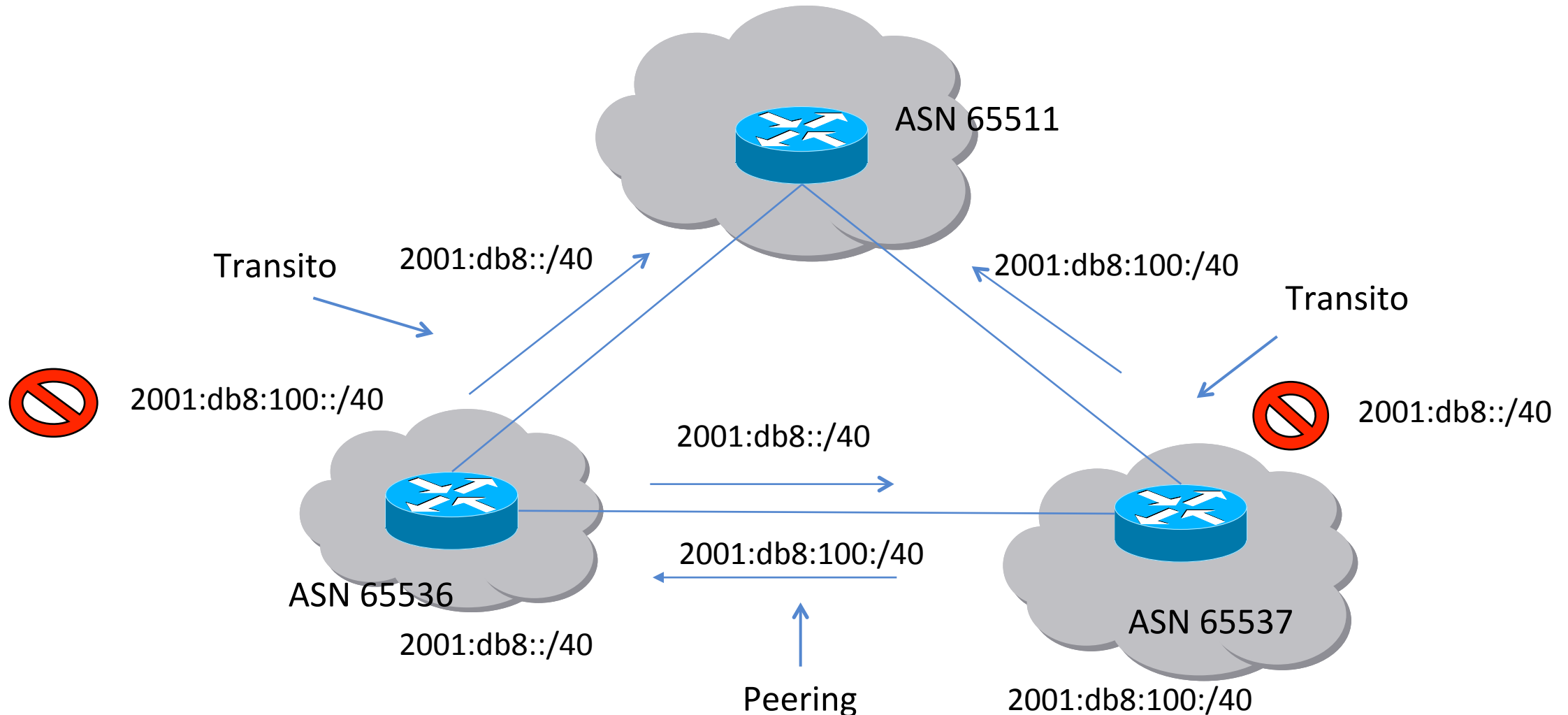


Si no hay filtros configurados, esto trae problemas

BGP default policy

- **RFC8212** especifica que si no hay una política configurada explícitamente, no se aprenderá nada ni se anunciará nada por eBGP (solo BGP externo)
- Esto contribuye a disminuir muchos problemas ocasionados por errores de configuración
- Fuerza a pensar en una política de entrada/salida
- Ver en <https://github.com/bgp/RFC8212> el estado de cumplimiento de las implementaciones de BGP

Roles en BGP para prevenir leaks



Roles en BGP para prevenir leaks

- Intra AS (local al AS):
 - Se definen roles al establecer una sesión BGP:
 - *Provider*
 - *Customer*
 - *Peer*
 - *Internal*
 - Uso de un nuevo atributo (iOTC) para marcar las rutas
 - draft-ietf-idr-bgp-open-policy
- Inter AS (entre AS del path):
 - Dos propuestas en discusión, se busca converger en una única solución
 - Marcar las rutas que se anuncian a *customers* o *peer* con atributo RLP
 - Las rutas que tienen ese atributo no se anunciarán por parte de un neighbor que es *customer* o *peer* (ejemplo: hacia el tránsito)
 - draft-ietf-idr-route-leak-detection-mitigation-09

RPKI

Validation Reconsidered es ahora una RFC

- Es un nuevo modelo de validación en RPKI
- Soluciona problemas que podrían surgir en la PKI de recursos, por ejemplo durante las transferencias
 - Algoritmo actual: si un certificado hace un “overclaim” de recursos con respecto al certificado superior, se invalida toda la cadena de certificados hacia abajo
 - Particularmente problemático cuando está cerca de la raíz
 - Validation reconsidered: solo se invalidan los recursos que no están incluidos en los certificados superiores
- Definido en RFC 8360
- Despliegue: hay dos posibilidades
 - Flag-day
 - Mixed mode

AS Cones

- Propuesta: Implementar en RPKI un concepto similar al de AS-SET
 - draft-ss-grow-rpki-as-cones-00 (ver presentación de Job Snijders)
- La idea es definir un nuevo objeto que describa el “cono” de clientes de un determinado AS
- Estos AS Cones pueden referenciar a otros AS Cones, al igual que los AS-SET pueden contener otros AS-SET
- Este objeto será firmado usando la misma cadena de certificados, tal como los ROAs.

ASPA: AS_PATH Verifcation

- Objetivo: detectar AS_PATHs inválidos o malformados
- Justificación: si una ruta válida se recibe de un cliente o de un peering, tiene que tener solo pares customer-to-provider en el AS_PATH
- Propone crear una base de datos de pares customer to provider
- Ejemplo: AS1 AS2 AS3
 - ASPA {AS1, AS2}
 - ASPA {AS2, AS3}
 - ASPA {AS3, 0}
- De esta forma, si tenemos una base de datos validada de pares (customer, provider) podemos verificar las rutas recibidas de clientes o peers.
- Ver drafts:
 - draft-azimov-sidrops-aspa-profile
 - draft-azimov-sidrops-aspa-verification

BGP en datacenters

Uso de BGP en datacenters

- Tradicionalmente la arquitectura de DC estaba basada en tecnologías L2 y STP.
- En algunos casos se usa L3 con un IGP
- En los datacenter más masivos o de gran escala (cientos de miles de servers) la tendencia es utilizar BGP
- Ventajas:
 - Unico protocolo de ruteo
 - Menor complejidad, más estabilidad
 - Mayor control sobre la información de ruteo
- Ver RFC7938

Otros temas relacionados

- Mecanismo de “neighbor autodiscovery” para BGP
- Es un tema que se está discutiendo en el WG idr
- Hay varias propuestas alternativas, aun no unificado
- El uso de esto sería para Datacenters masivos
- Varias alternativas:
 - LLDP
 - IS-IS link discovery
 - Edge Control Protocol
 - BGP Neighbor Autodiscovery
 - Link State Over Ether

Más información

- Propuestas de cambios al protocolo BGP:
 - Grupo idr de IETF
- Propuestas sobre temas relacionados con la operación de BGP:
 - Grupo grow de IETF

lacnic
lacnog 2018

30

24/28 SETIEMBRE 2018
ROSARIO • ARGENTINA

Muchas gracias!