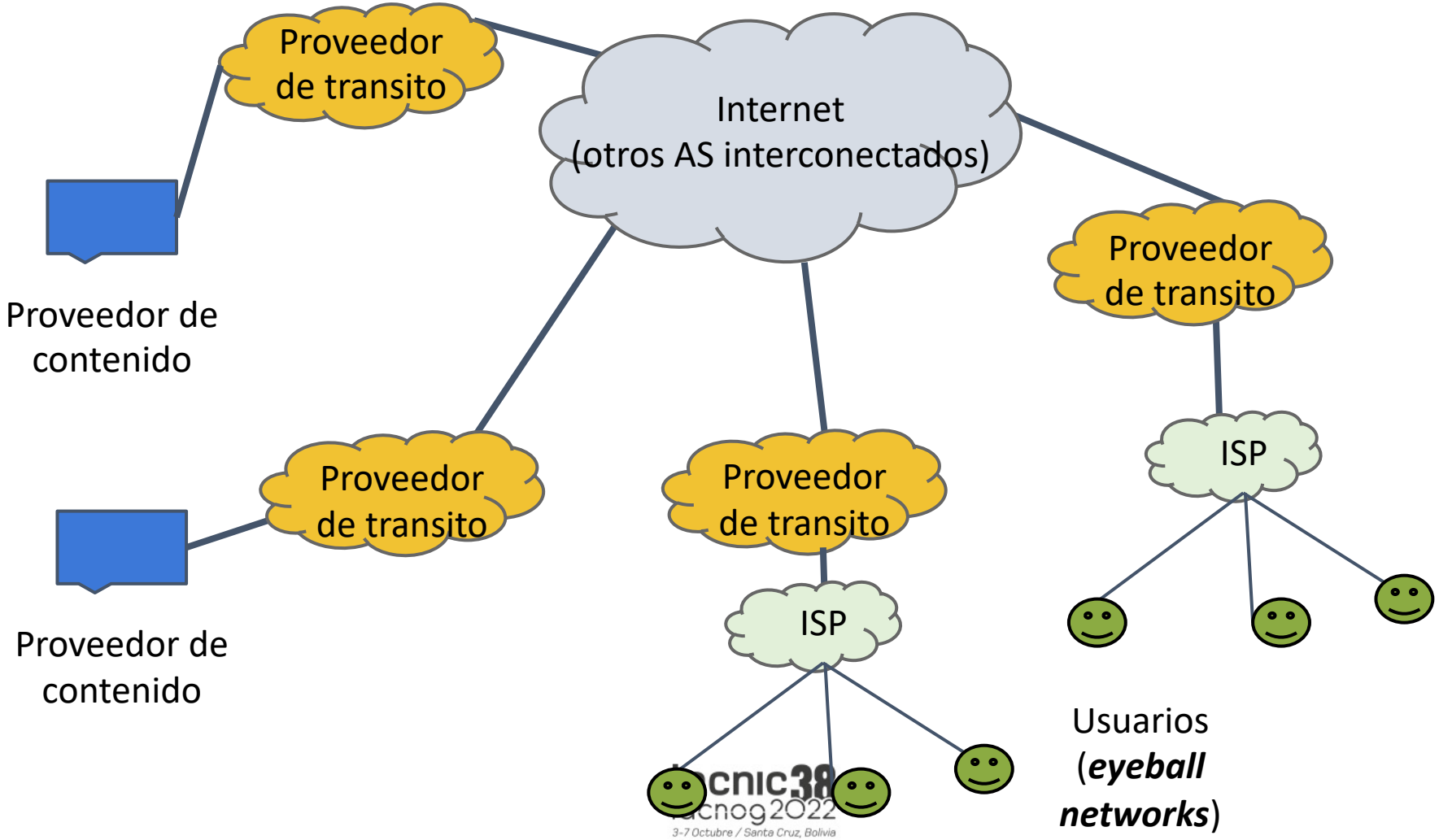
lacnic38
lacnog2022
3-7 Octubre / Santa Cruz, Bolivia

Interconexión y peering más seguros

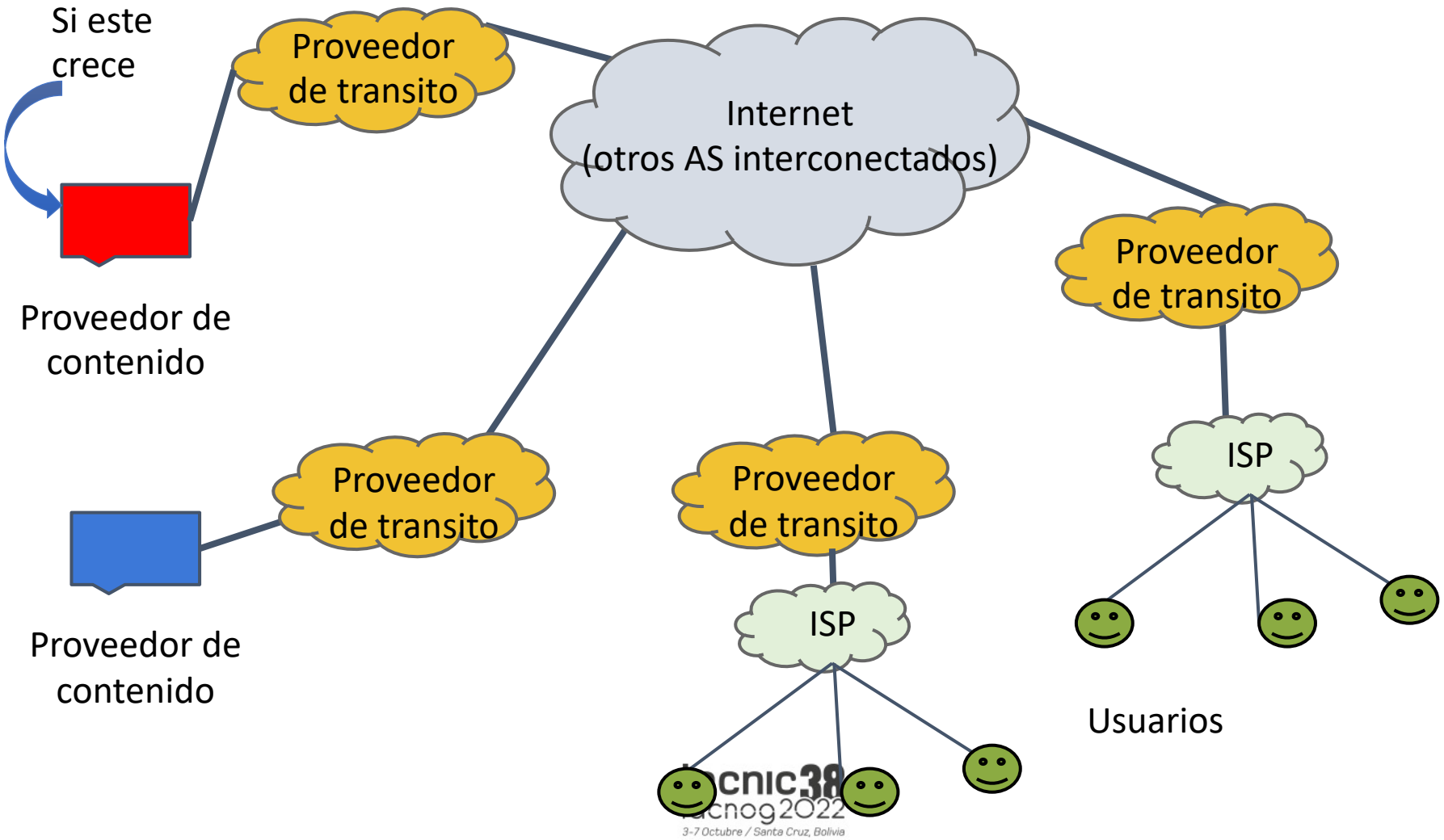
Erika Vega – evega@nog.lat
Guillermo Cicileo - guillermo@lacnic.net

lacnic lacnog Internet Society Capítulo Bolivia

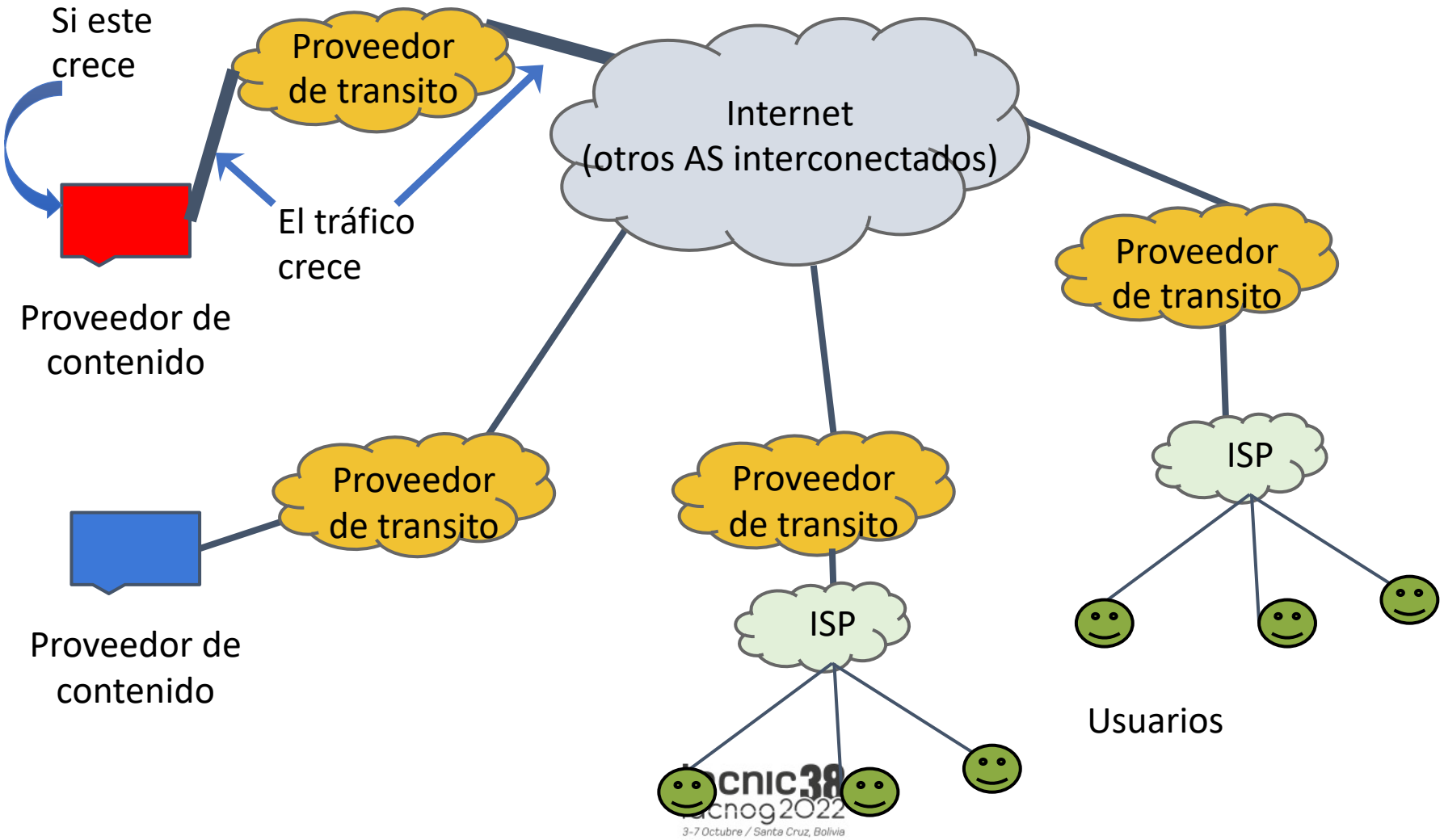
¿Cómo se encamina el tráfico?



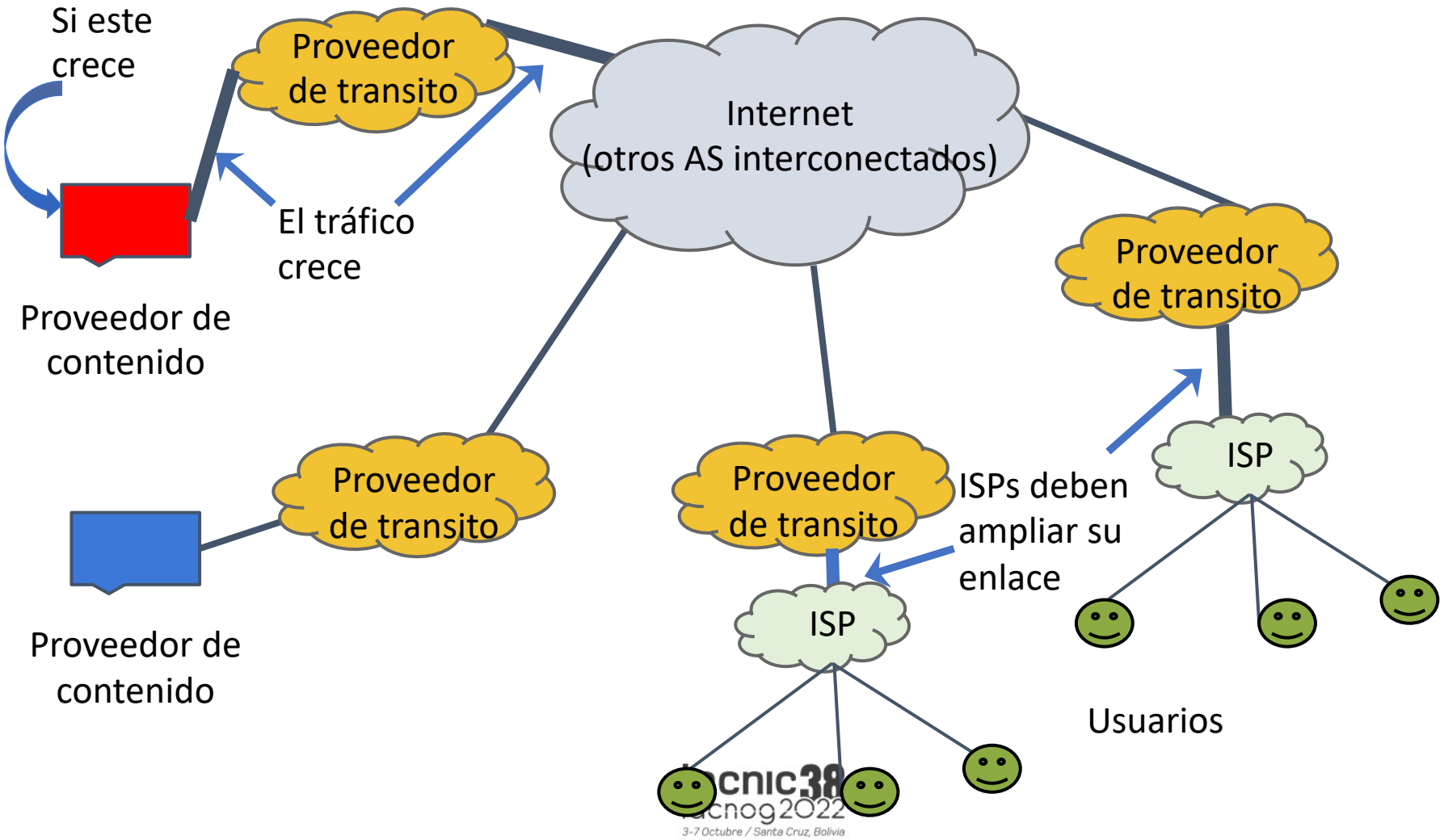
¿Cómo se encamina el tráfico?



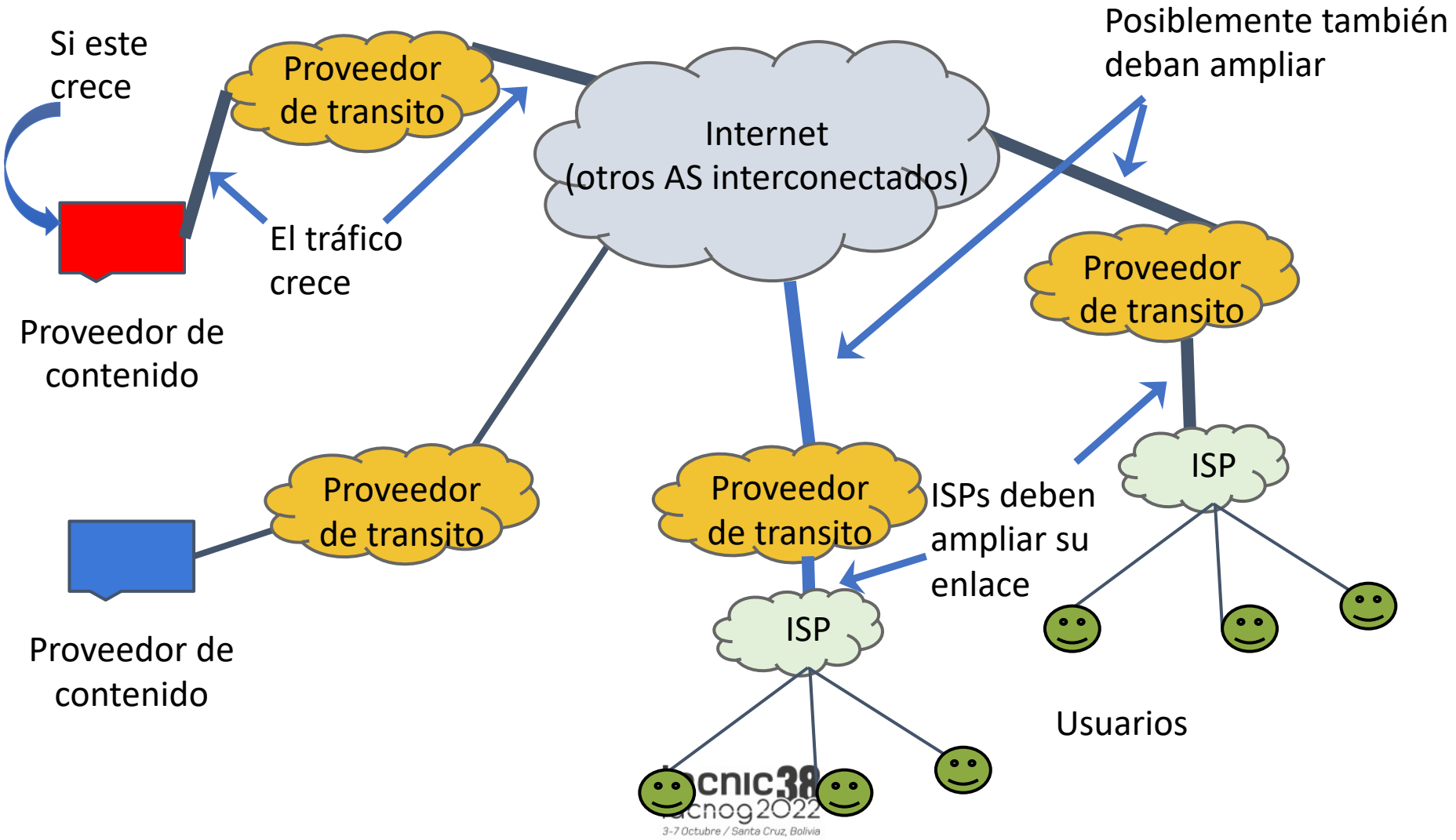
¿Cómo se encamina el tráfico?



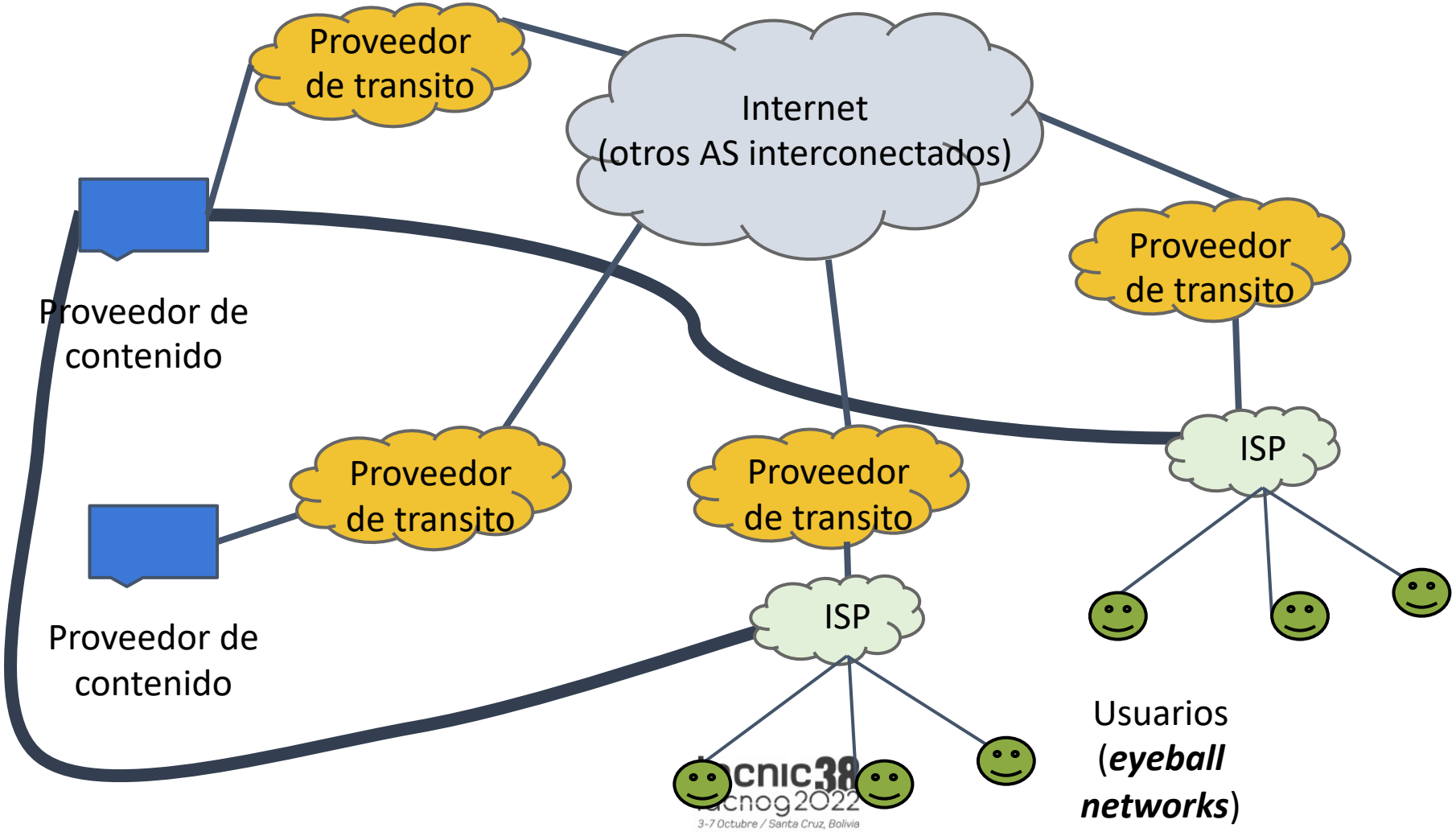
¿Cómo se encamina el tráfico?



¿Cómo se encamina el tráfico?

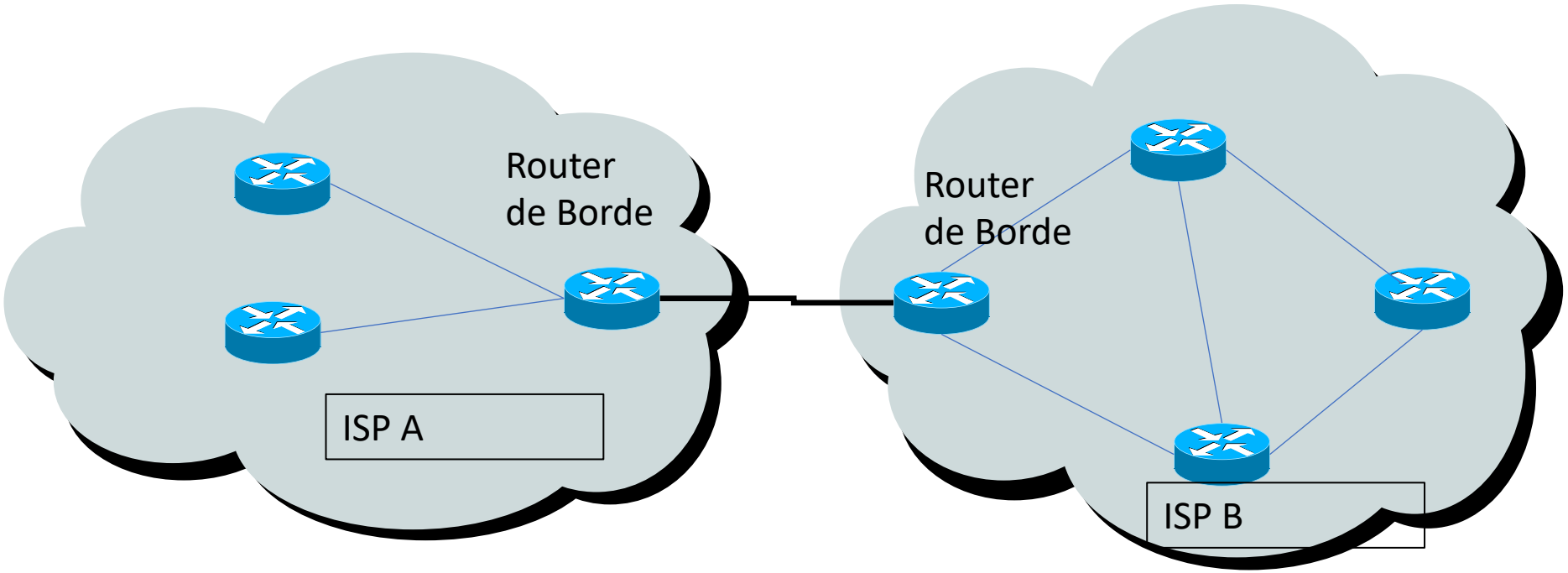


Alternativa: peering

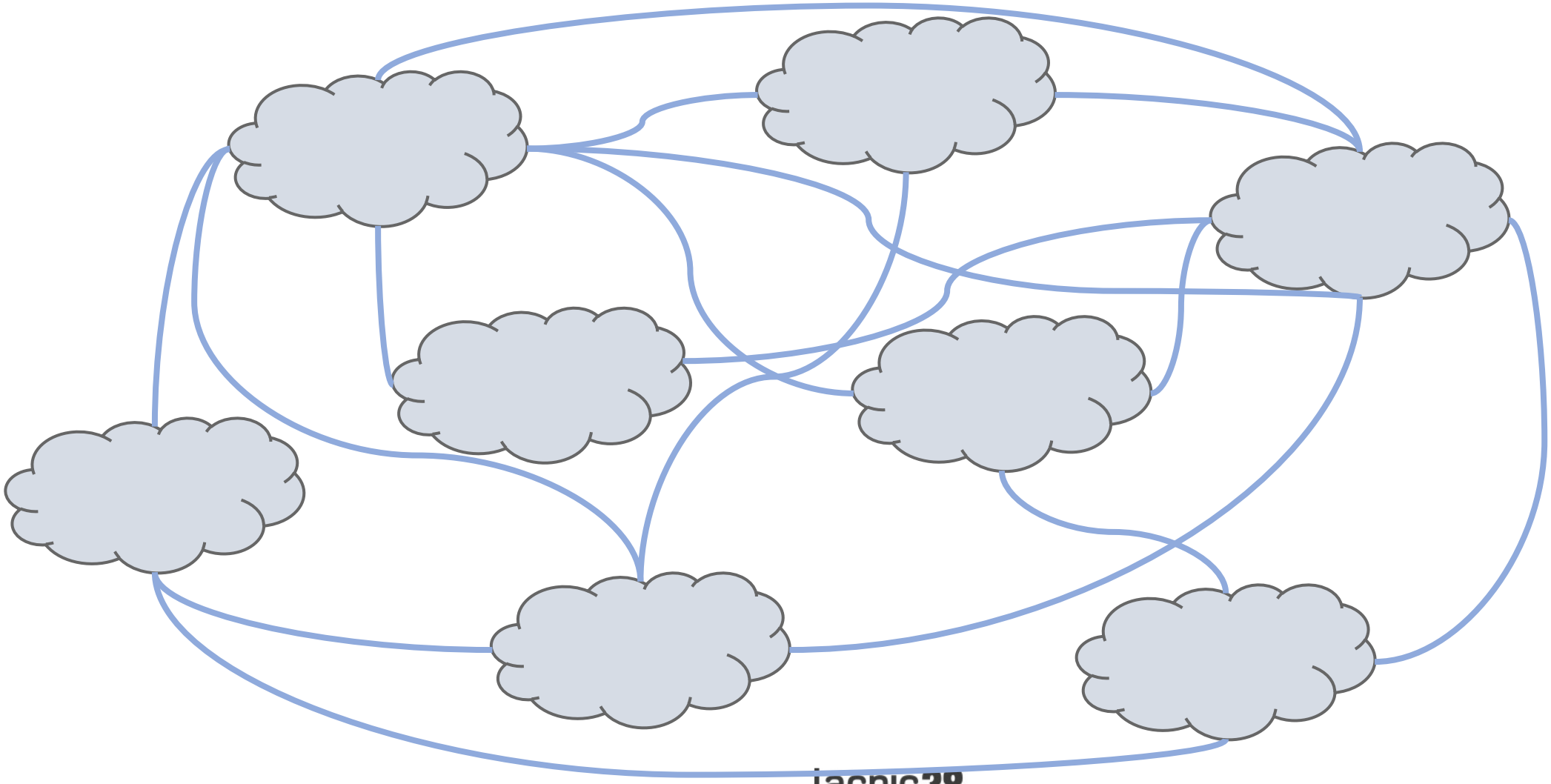


Modalidades de interconexión

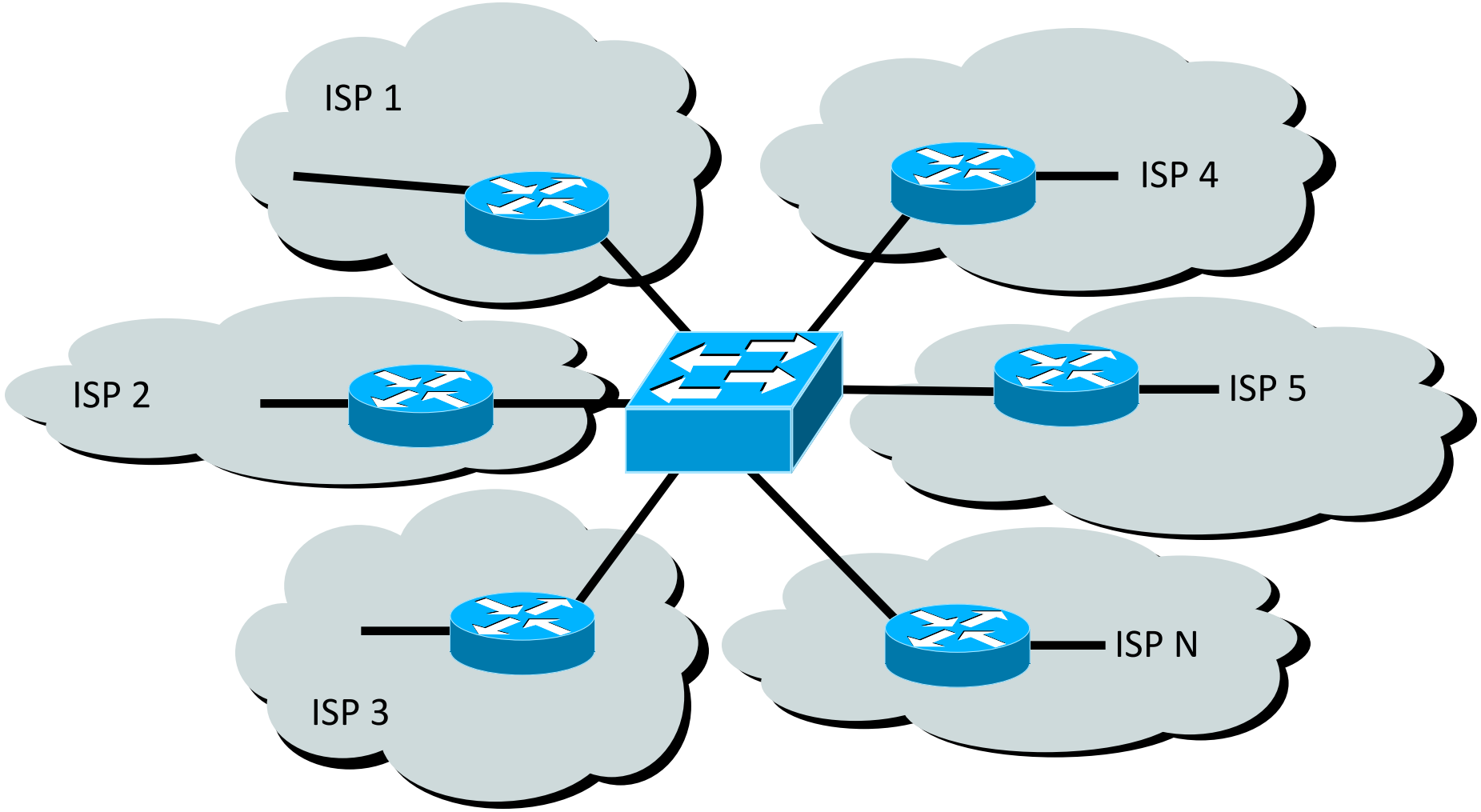
Interconexión directa: Peering



Interconexión directa: puede ser compleja

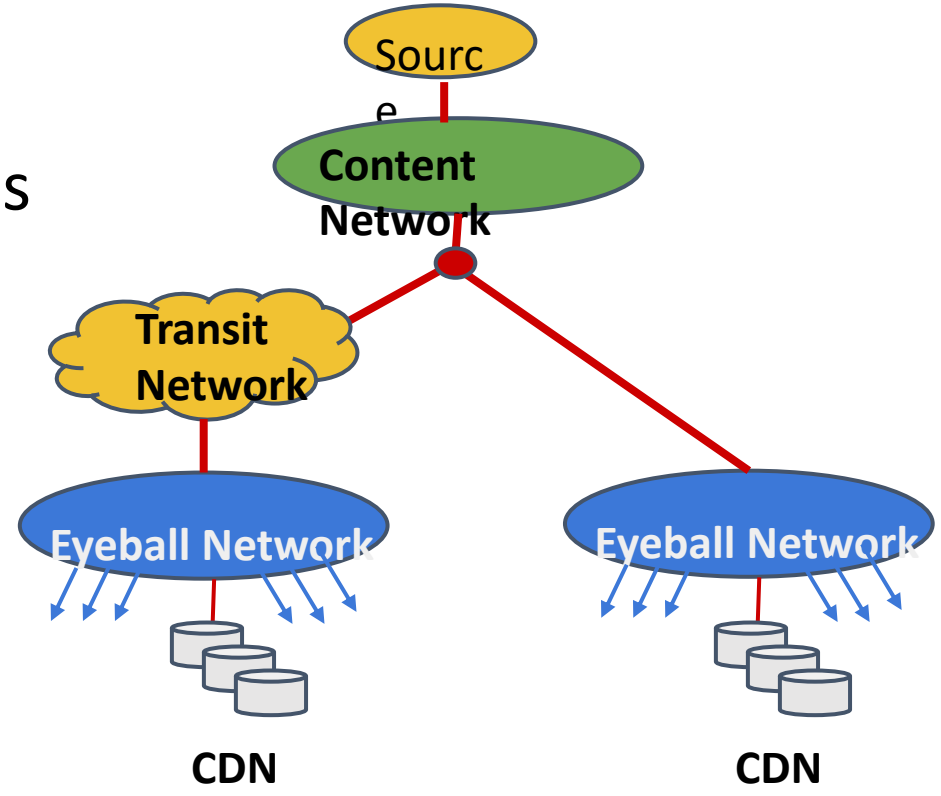


Interconexión pública



Qué es una CDN (Content Delivery Network)?

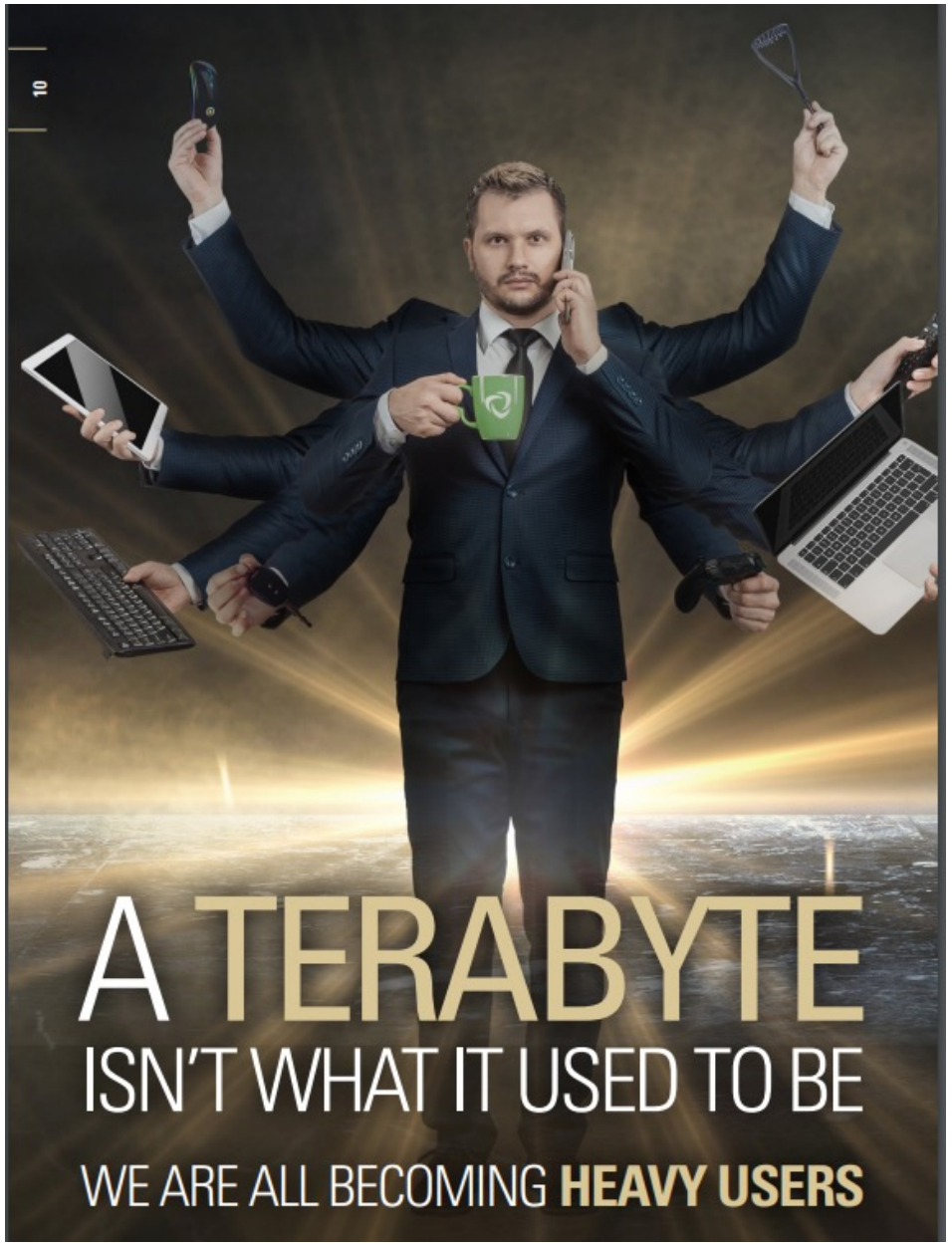
- Plataforma distribuida para entrega de contenido
- Sirve contenido más cerca de los usuarios
- Mejora el desempeño de los servicios a los usuarios
- Menor costo para el proveedor de contenido y el ISP



Ejemplos de CDNs

- CDNs Tradicionales y Telco
  - Akamai
  - Cloudflare
  - Level3
  - Limelight Networks
- Content Provider own-CDNs
  - Google
  - Netflix
  - Facebook

Realidad del tráfico de Internet en la actualidad



- El uso global de BW aumentó un 34% de 2019 a 2020 y un 29% más en 2021
- La transmisión de vídeo, representa el 53,72% del total de tráfico

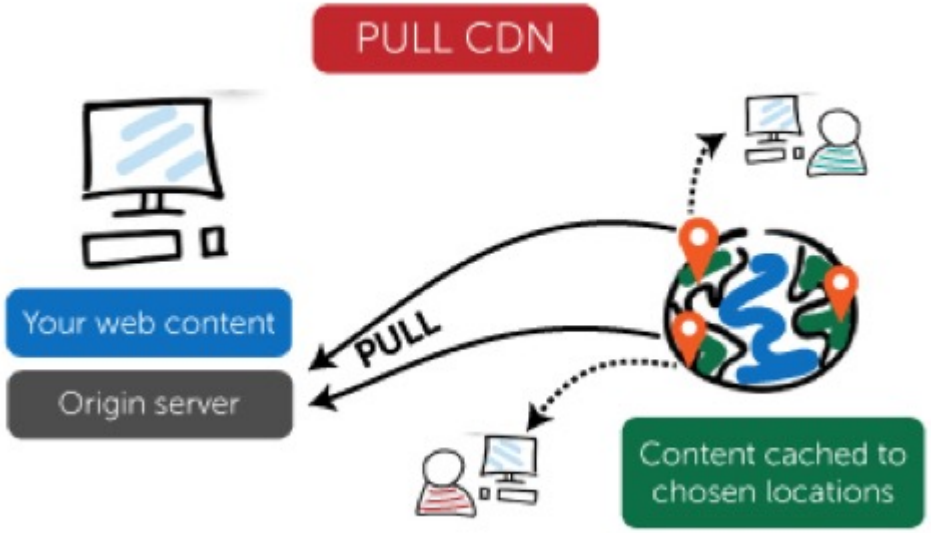
	Category	Total Volume
1	Video	53.72%
2	Social	12.69%
3	Web	9.86%
4	Gaming	5.67%
5	Messaging	5.35%
6	Marketplace	4.54%
7	File Sharing	3.74%
8	Cloud	2.73%
9	VPN	1.39%
10	Audio	0.31%

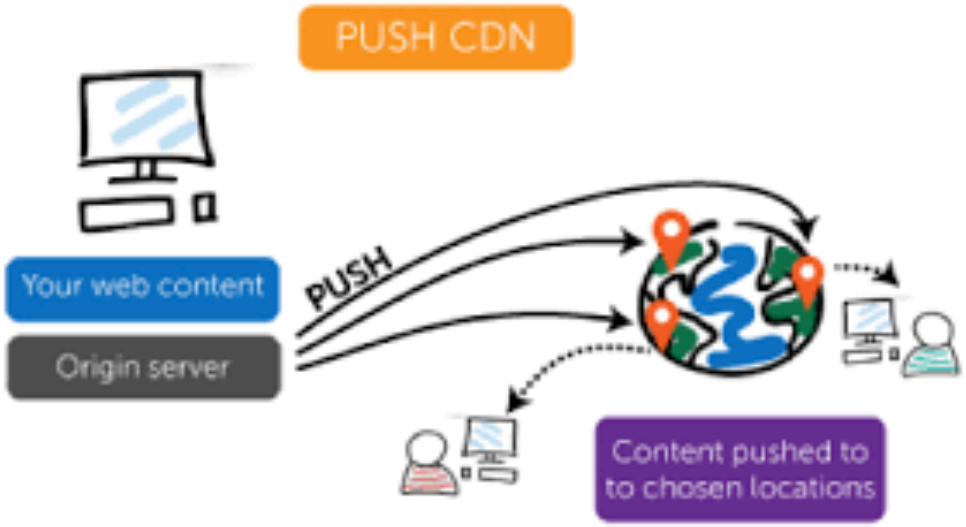
Plataformas OTT

- Cantidad de usuarios en Internet
- Contenido de Streaming
- Calidad de video 4k- 16 k

	Video	Games	Social	Messaging	Enterprise Conferencing
1	YouTube	Player Unknown's Battlegrounds	Facebook	WhatsApp	Zoom
2	Netflix	ROBLOX	TikTok	Discord	Microsoft Teams
3	Facebook video	League of Legends	Instagram	Facebook Messenger	Webex
4	TikTok	Fortnite	Wordpress	LINE	Blackboard Collaborate
5	HTTP media stream	Minecraft	Snapchat	Skype	Amazon Chime
6	Disney+	Garena Free Fire	Twitter	Zoom	Canva
7	Amazon Prime	Call of Duty	Reddit	Microsoft Teams	Udemy
8	Twitch	Mobile Legends	Wattpad	Telegram	Cisco Spark
9	Hulu	Candy Crush	Pinterest	WebEx	GoToMeeting
10	HBO	War Thunder	GIPHY	WeChat	Steam

Modelos de entrega de contenido en las CDN





Definiciones básicas

Definiciones

Tránsito

- Transmisión de tráfico a través de una red, regularmente por un costo

Peering

- Intercambio de información de enrutamiento y tráfico

Default Free Zone (DFZ)

- Sistemas autónomos que no requieren una ruta default para alcanzar cualquier destino en Internet

Tránsito vs Transporte

Tránsito

- Usualmente servicio en capa 3 (IP).
  - Puede ser BGP o no
- Costo en base a Mbps
- Utilizado para enviar tráfico a muchos sitios
- El tráfico depende de quien da el servicio como upstream provider

Transporte

- Usualmente servicio en capa 2: Metro Ethernet, SDH, etc.
- Costo fijo por capacidad de enlace (1Gbps, 10 Gbps).
- Utilizado para conectar dos sitios
- El tráfico queda acotado entre las organizaciones que establecen el transporte

Puntos de Intercambio de tráfico: IXPs

Importancia y Beneficios

Características de un IXP

Un IXP es un sitio donde los ***operadores de red*** se interconectan

- Otros nombres: PIT, PTT, NAP (anteriormente)

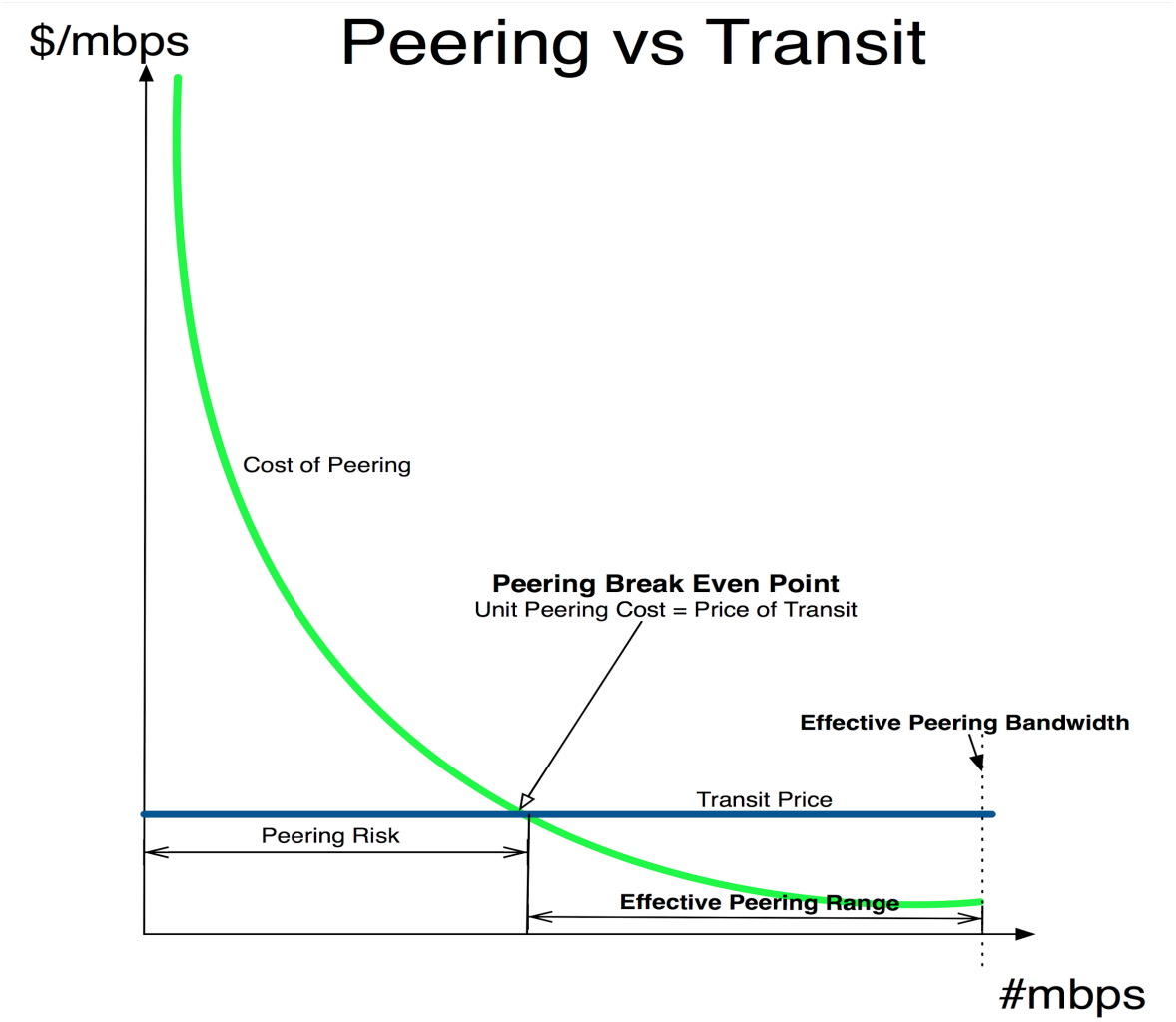
- Infraestructura compartida intercambiar tráfico:
  - ISPs, Proveedores de Contenido, Universidades, Medios, Bancos, etc.
- Normalmente habrá varios AS que se interconectan, lo que lo distingue de un peering privado que se hace entre dos redes.
- Un IXP es distinto de una red de acceso y de una red de tránsito/carrier
  - La función del IXP es interconectar redes, no proveer acceso ni actuar como un proveedor de tránsito o carrier.
  - Un IXP permite interconectar redes que son organizaciones separadas: sistemas autónomos independientes.
  - Un IXP no requiere que el tráfico entre dos AS pase por un tercero

Comparación de costos

Transporte al sitio del IX	Costo fijo por cierta capacidad
Colocation	Fijo
Hardware	Fijo
X-connect	Fijo
IXP fee	Fijo

Transito	Basado en el uso

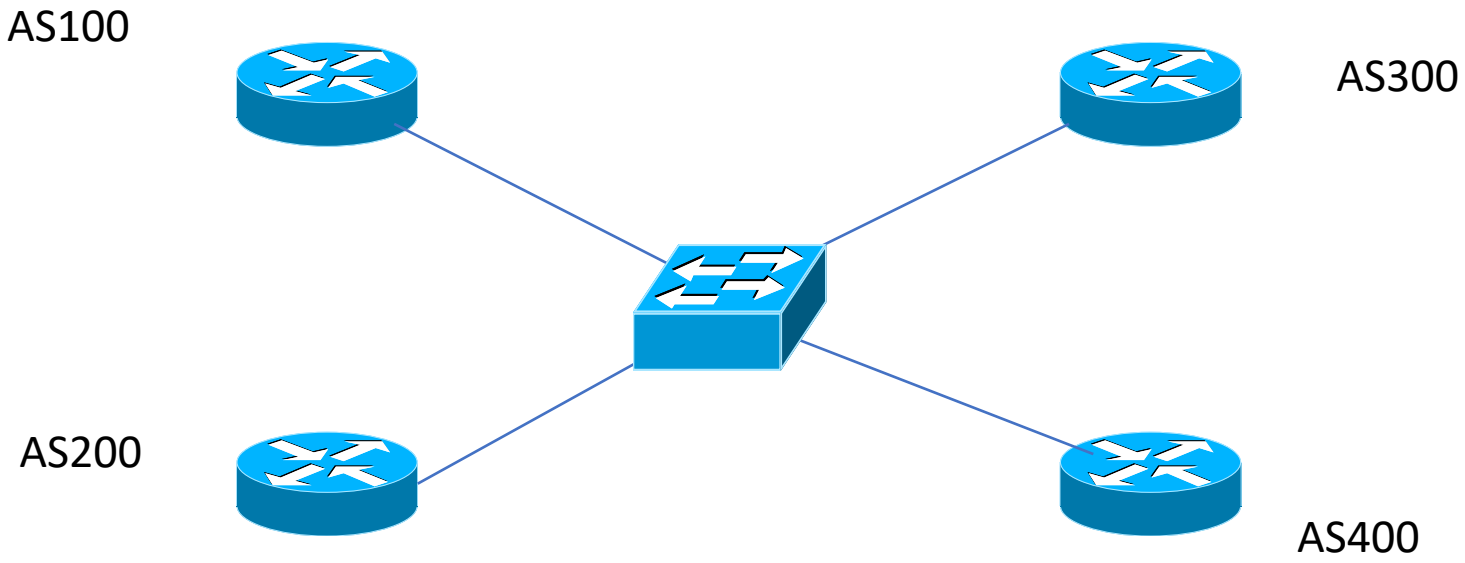
Peering vs. Transito: costos comparados



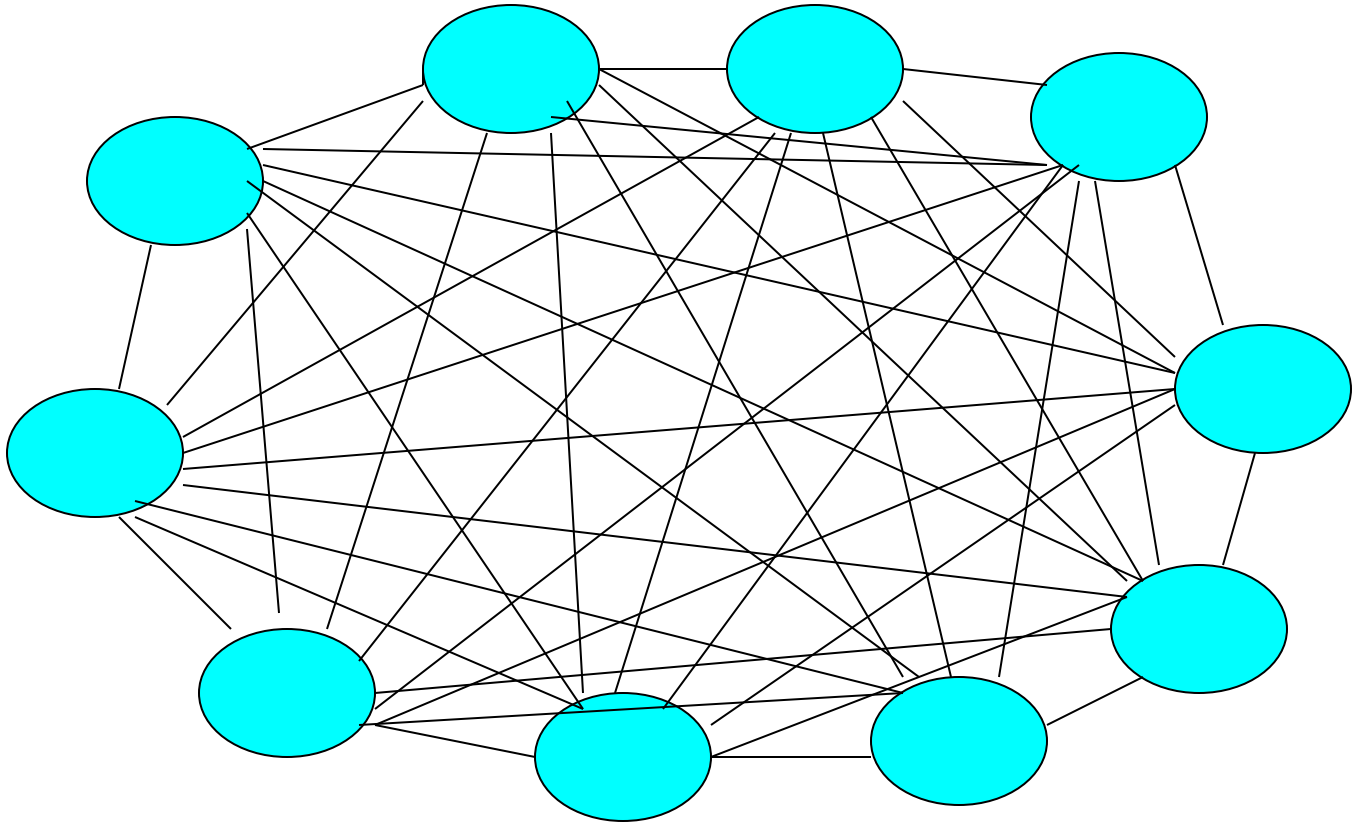
Source: Dr Peering

Esquema básico de un IXP

Esquema básico de un IXP

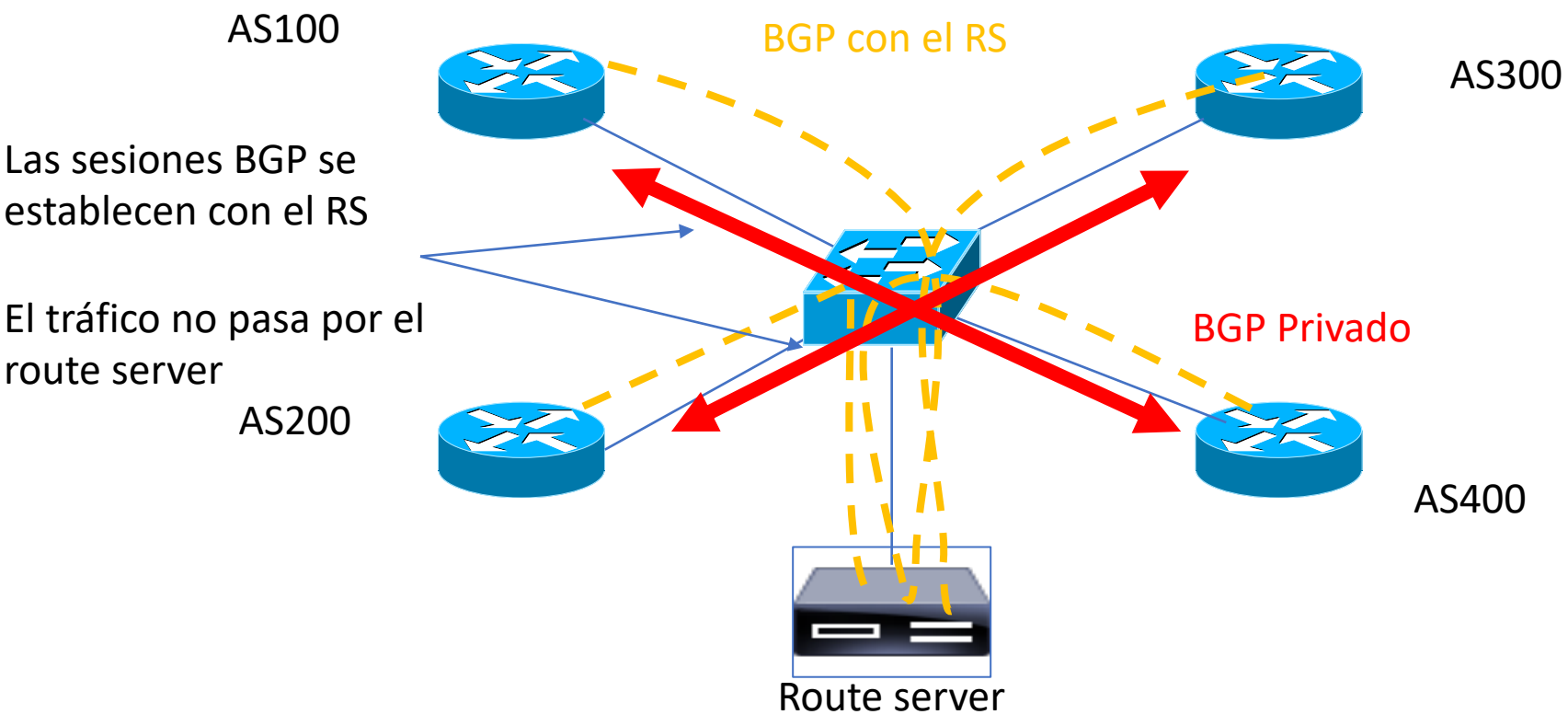


Sin route-server: malla N-cuadrado



ROUTE SERVERS (RS)

Uso de route server en un IXP



Route Servers ¿Qué es?

- Normalmente es un Servidor Unix que corre software de Enrutamiento.
  - Existen soluciones Open Source para esto
- Ruteador que activa la funcionalidad de BGP
- Intercambia la información de ruteo con ruteadores de proveedores de servicio en un IXP basado en políticas
- No envía paquetes – unicamente maneja la lógica de ruteo
- Evita una enorme cantidad de sesiones de BGP
  - Número de seciones = n(n-1)

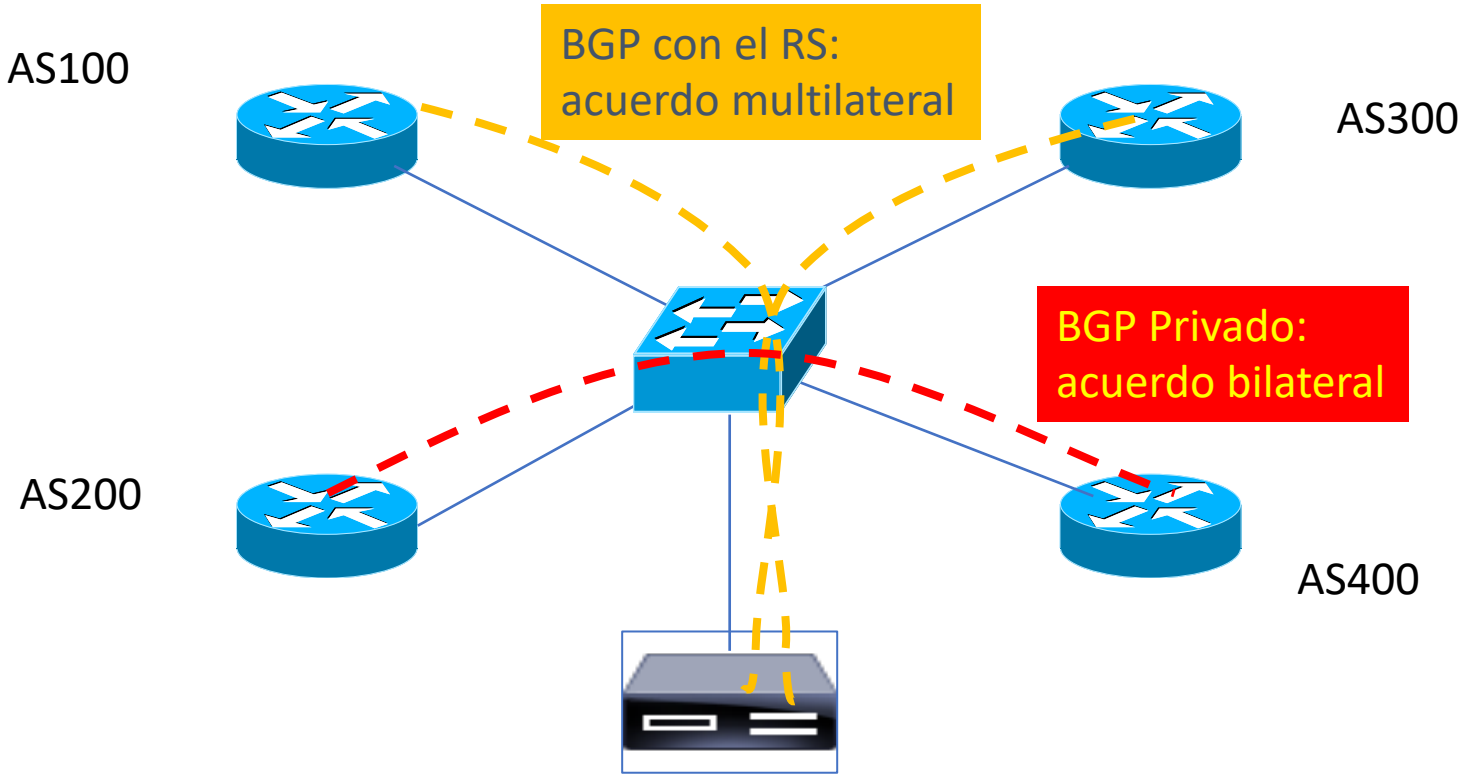
Seguridad: ventajas de un route server

- Medidas básicas: filtrado de ASNs y prefijos bogon, filtros por cliente, etc.
- Evita route-leaks que pueden provenir de errores de configuración
  - Ejemplo: si se filtra una full-table al RS
  - Es un beneficio aún para ISPs que no hacen peering con el RS: sus rutas no se fugarán al resto de los ISPs.
- Posibilidad de implementar filtros por RPKI, por IRR, whois, etc.

Ejemplos de route-servers por software

- arouteserver: http://arouteserver.readthedocs.io
  - Herramienta en Python para generar configuración para route servers
  - Produce configuraciones para BIRD y OpenBGPd
  - Soporta IRR, RPKI, WHOIS
  - Soporta PeeringDB para obtener los AS-SETs
  - Simple de integrar con otros sistemas
- IXP manager: https://www.ixpmanager.org
  - Es un Sistema de administración completo para IX
  - Incluye un portal para administración del IXP y para los miembros
  - Produce configuraciones para BIRD

Interconexión en un IXP



Tipos de Acuerdo

Acuerdos Bilaterales

- Cada proveedor establece la relación que necesite con otros proveedores en el IXP
- Los enrutadores de borde de los ISP establecen sesiones de BGP con los enrutadores de borde de otros proveedores

Acuerdos Multilaterales

- Cada proveedor establece sesiones con el concentrador
- Los enrutadores de borde de los ISP tienen como vecino al IXP

Referencias

- Cursos de Campus de LACNIC: https://campus.lacnic.net (BGP y RPKI)
- Tutorial de BGP y RPKI de LACNIC32: https://www.lacnic.net/3900/52/evento/tutoriales

- Internet Exchange BGP Route Server – https://tools.ietf.org/html/rfc7947
- Internet Exchange BGP Route Server Operations - https://tools.ietf.org/html/rfc7948
- A Border Gateway Protocol 4 (BGP-4) - https://tools.ietf.org/html/rfc4271

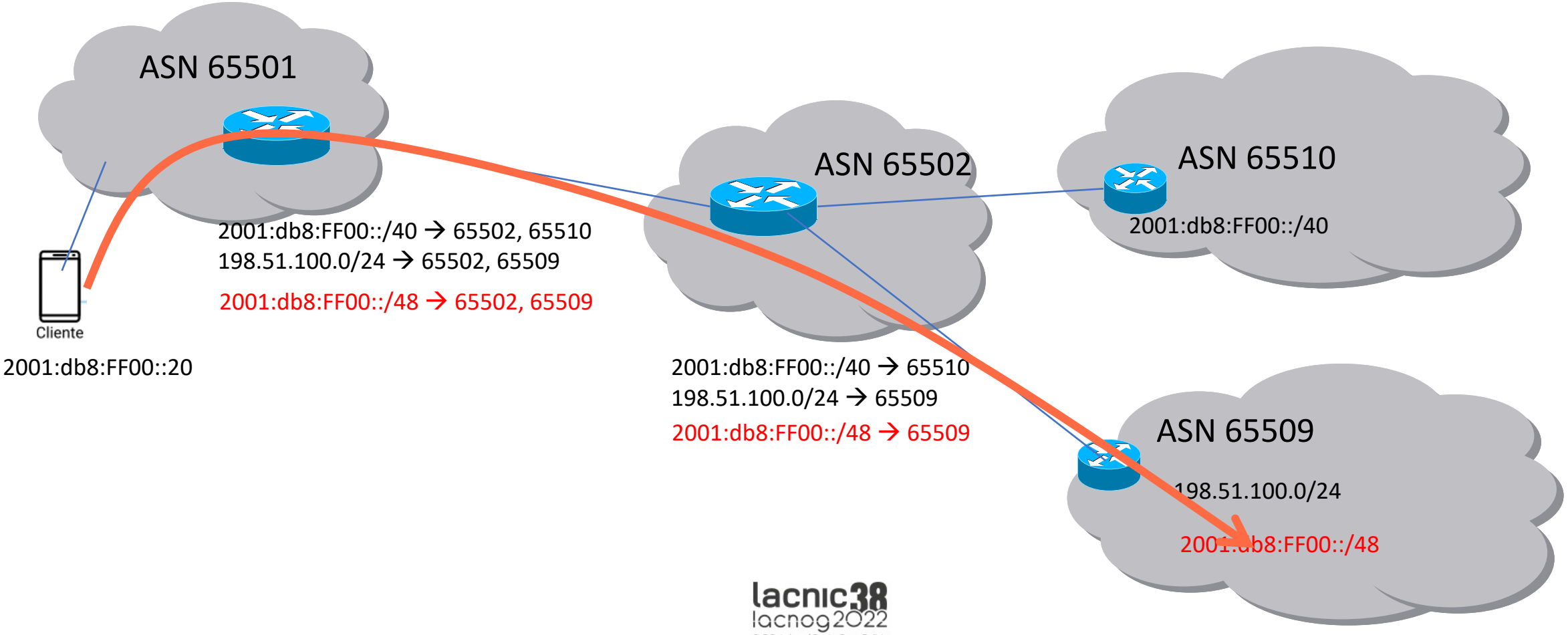
¿Preguntas hasta acá?

Seguridad en ruteo

Secuestro de rutas

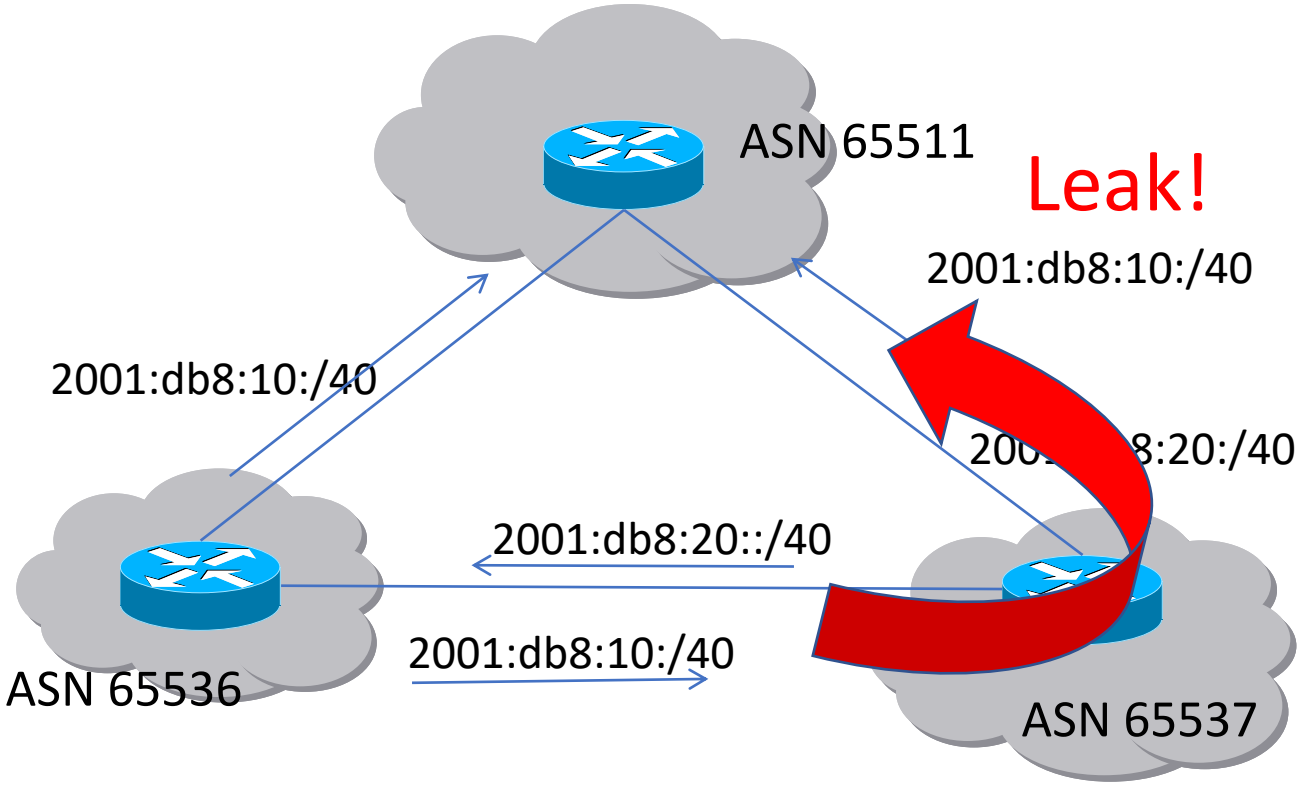
Secuestro de rutas:
Acción de anunciar
prefijos NO autorizados

- Intencional.
- Por error en la operación.



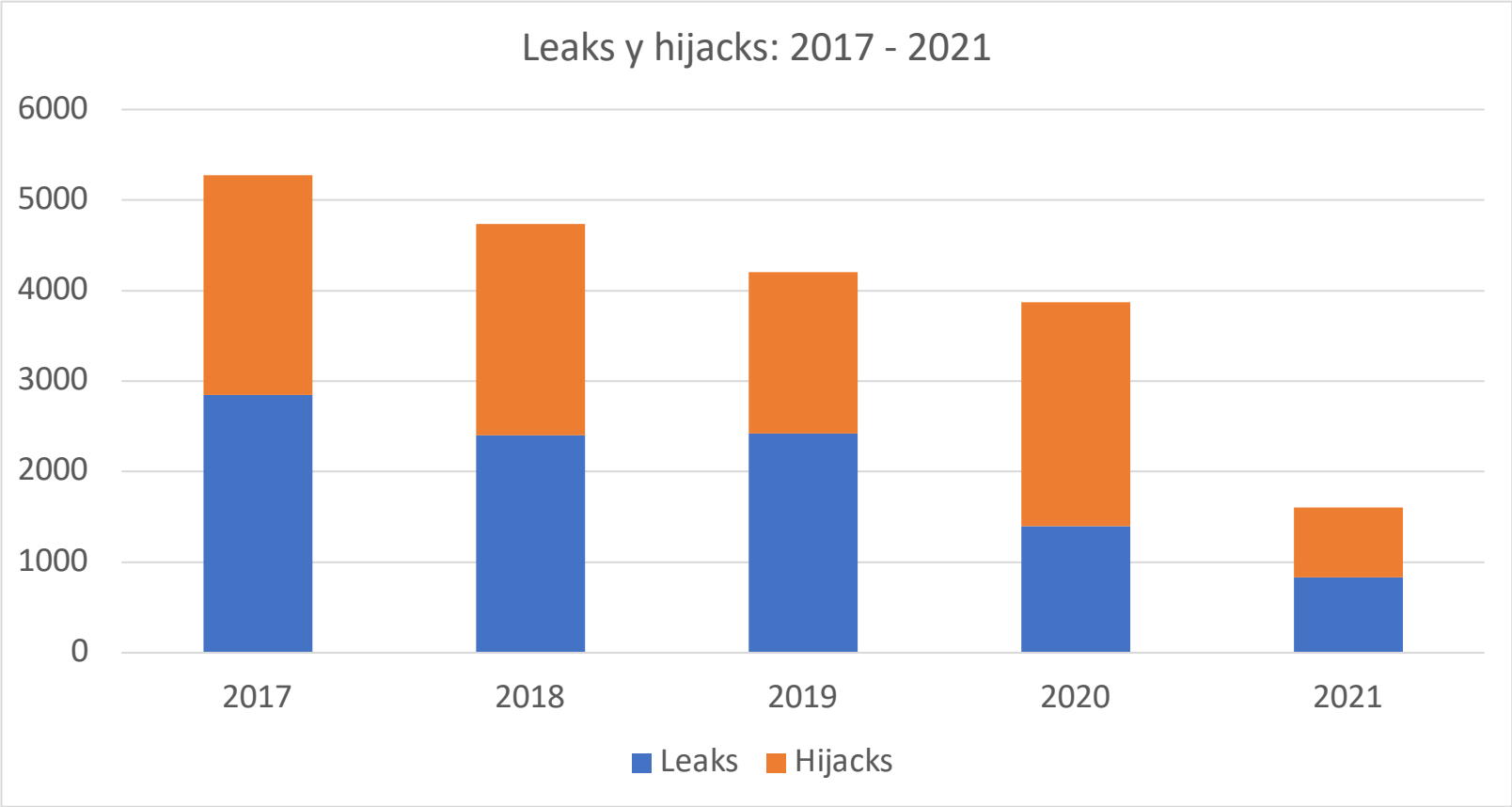
Route leaks – fuga de rutas

- Prefijos aprendidos del ***proveedor*** no deben anunciarse a otro ***peer*** o a otro ***proveedor***
- Prefijos aprendidos de un ***peer*** tampoco se anuncian a otros ***peers*** ni al ***proveedor***
- Esos prefijos solo deberían anunciarse a ***clientes***



Si no hay filtros configurados, esto trae problemas

Principales incidentes de seguridad



Fuentes:

Informe sobre seguridad en el ruteo de LAC – Augusto Mathurín, 2019
https://www.lacnic.net/innovaportal/file/4297/1/fort-informe-seguridad-ruteo-es.pdf

MANRS: https://www.manrs.org/2021/02/bgp-rpki-and-manrs-2020-in-review/

MANRS: https://www.manrs.org/2022/02/bgp-security-in-2021/

¿Qué podemos hacer para mitigar los incidentes?

Acciones acordadas para promover la seguridad del ruteo

MANRS – Routing Manifesto

- Mutually Agreed Norms for Routing Security (MANRS)
- Objetivos
  - Despertar conciencia e impulsar acciones demostrando el compromiso de un grupo creciente de apoyos
  - Promover una cultura de reponsabilidad colectiva para la resiliencia y seguridad del sistema de ruteo global de Internet
  - Demostrar la capacidad de la industria de resolver los problemas de seguridad y resiliencia de Internet
  - Proveer un marco para que los ISPs entiendan y se ocupen de los temas relativos a la resiliencia y seguridad del sistema de enrutamiento global de Internet

MANRS – Routing Manifesto

- Recomendaciones sobre el sistema de ruteo global y recomendaciones a los operadores de red.
- Dar soluciones a tres clases de problemas:
  - Relativos a información de ruteo incorrecta
  - Relativos a tráfico con IP de origen spoofed
  - Relativos a la coordinación y colaboración entre operadores de red

MANRS – Routing Manifesto

- Acciones esperadas
  1. Prevenir la propagación de información de ruteo incorrecta
  2. No permitir tráfico con direcciones falsificadas
  3. Facilitar la comunicación y coordinación global entre operadores de red
  4. Facilitar la validación de la información de ruteo en una escala global
- Participar en:
  - https://www.routingmanifesto.org/signup/

MANRS: IXP Programme

- MANRS: pensado inicialmente para operadores…
- Pero los IXPs juegan un rol importante en Internet:
  - Representan una comunidad con objetivos comunes desde el punto de vista de la operación
  - Contribuyen a una infraestructura de Internet más **resiliente** y **segura**.
  - Pueden ser un punto focal de colaboración para discutir y promover la importancia de la seguridad de enrutamiento.
- Los IXP son socios importantes en la comunidad MANRS
- Para abordar las necesidades y preocupaciones únicas de los IXP, la comunidad creó un conjunto de acciones específicas de MANRS para los miembros de IXP.

Acciones para el IXPP

- **Acción 1. Facilitar la prevención de la propagación de información de enrutamiento incorrecta. (Obligatorio)**
  - El IXP implementa el filtrado de anuncios de ruta en el route server usando IRR y / o RPKI. Los anuncios no válidos se filtran de acuerdo con la política publicada de IXP.
- **Acción 2. Promover MANRS entre los miembros del IXP. (Obligatorio)**
  - El IXP promueve o prove asistencia para que los miembros implementen las acciones de MANRS. (Hay 4 casillas de verificación separadas para diferentes niveles de incentivos, se debe verificar una o más).

Acciones para el IXPP

- **Acción 3. Proteger la plataforma de peering.**
  - El IXP tiene una política publicada de tráfico no permitido en el switch de peering y realiza el filtrado de dicho tráfico. (higiene de capa 2)
- **Acción 4. Facilitar la comunicación y coordinación operativa global entre los operadores de red.**
  - El IXP y cada uno de sus miembros tienen al menos una dirección de correo electrónico válida y activa y un número de teléfono que otros miembros pueden usar para casos de abuso, seguridad e incidentes operacionales.
- **Acción 5. Proporcionar herramientas de monitoreo y depuración a los miembros.**
  - El IXP proporciona un looking glass para sus miembros.

MANRS – Mejores prácticas

MANRS es un conjunto de ”Normas Mutuamente Acordadas para la Seguridad del Enrutamiento”

Acciones propuestas por MANRS para **operadores**:

- Filtrado
- Anti-spoofing
- Coordinación
- Validación global

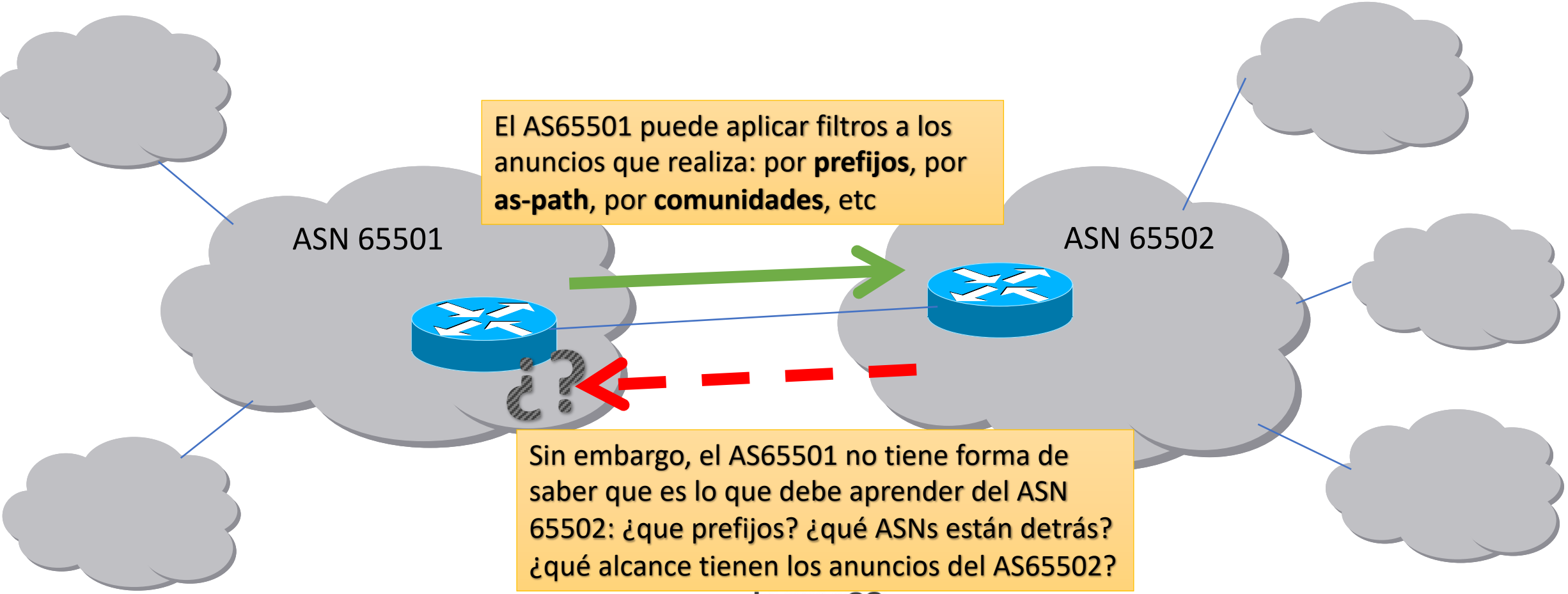
Veremos estas acciones en más detalle a continuación

Hay también un programa específico para **IXPs** y para **CDNs**

https://www.manrs.org

¿Cómo obtener información más allá de nuestro sistema autónomo?

BGP: filtros de salida y entrada



IRRs vs RPKI

- Cómo chequear que la información que recibimos por BGP es correcta?
  - BGP no tiene mecanismos intrínsecos que permitan verificar esto
  - Se deben contrastar los anuncios recibidos por BGP contra fuentes externas

- Existen dos formas:

IRR: Internet Routing Registries

RPKI: Resource Public Key Infrastructure

IRR – Internet Routing Registries

- Existe una gran cantidad de IRRs
  - El más conocido es RADB
  - RADB replica todos los demas IRRs
- Las organizaciones definen sus políticas de ruteo en un IRR
- Los operadores (ISP) utilizan esa información para generar filtros para BGP, muchas veces en forma automática
- Existen herramientas para utilizar esa información y configurar los routers: bgpq3/bgpq4, etc.

- AFRINIC
- ALTDB
- AOLTW
- APNIC
- ARIN
- BELL
- BBOI
- CANARIE
- EASYNET
- EPOCH
- GT
- HOST
- JPIRR
- LEVEL3
- NESTEGG
- NTTCOM
- OPENFACE
- OTTIX
- PANIX
- RADB
- REACH
- RGNET
- RIPE
- RISQ
- ROGERS
- TC

- **Ahora también LACNIC**

Ejemplos de registros

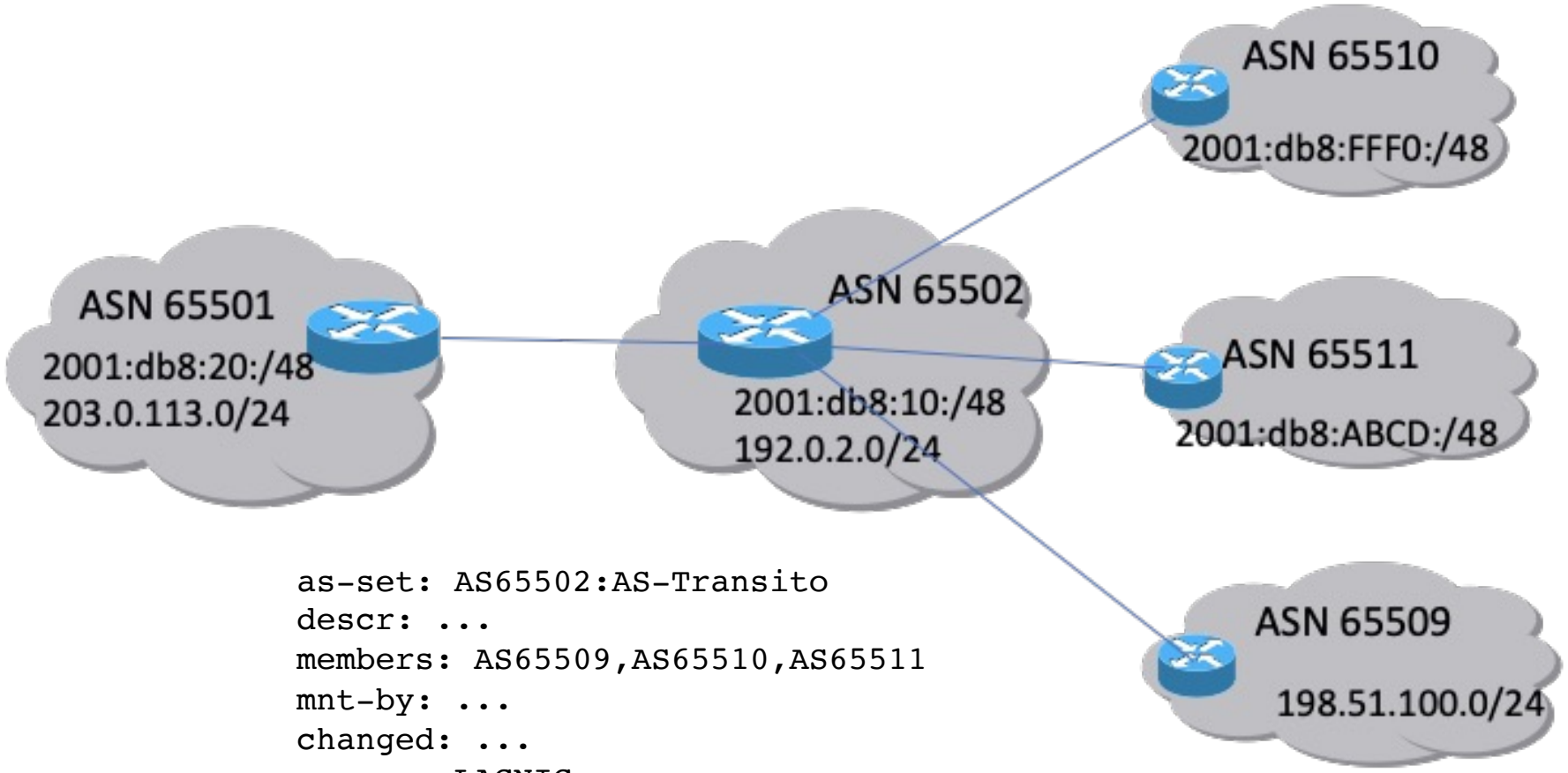
```
whois -h irr.lacnic.net '!oMNT-UY-NICO1-LACNIC'

route6:         2803:9910:8000::/34
descr:          LACNIC generated route6 for Ni Co
origin:         AS64135
remarks:        LACNIC generated route6 for Ni Co
remarks:        maxLength 48
mnt-by:         MNT-UY-NICO1-LACNIC
changed:        20220908
source:         LACNIC
remarks:        ****************************************************
remarks:        This object may have been modified
remarks:        For more information, please query whois.lacnic.net
remarks:        ****************************************************
last-modified:  2022-09-08T22:45:05Z

aut-num:        AS64136
descr:          LACNIC generated autnum for Ni Co
as-name:        AS64136
tech-c:         NIA14
remarks:        LACNIC generated autnum for UY-NICO1-LACNIC
mnt-by:         MNT-UY-NICO1-LACNIC
changed:        20220414
source:         LACNIC
remarks:        ****************************************************
remarks:        This object may have been modified
remarks:        For more information, please query whois.lacnic.net
remarks:        ****************************************************
last-modified:  2022-04-14T23:05:04Z
```

Cómo usar la información

Ejemplo de tránsito




```
as-set: AS65502:AS-Transito
descr: ...
members: AS65509,AS65510,AS65511
mnt-by: ...
changed: ...
source: LACNIC
```

Creación de AS-SET en MILACNIC

Inicio / Organización / IP / ASN / **Editar AS-SET**

AS-SET

Aquí podrá generar un AS-SET con la información de sus ASNs. EL nombre del AS-SET va ha estar compuesto por al nombre del ASN + el tipo de uso + un texto libre a su elección, todos con el prefijo AS delante. Ej: AS-28000:AS-PEERS:AS-TEXTOLIBRE.

Nombre (identificador) AS64135:AS- LabRPKIpermitidos1

ASN Members

AS28000 ✖ AS28001 ✖ AS12654 ✖ AS196615 ✖

AS-SET Members Elija uno

Comentarios (Remarks Agregue cualquier información relacionada al AS-SET que crea necesario aclarar

ASNs permitidos para el Lab de RPKI (set No.1) ✖

Cancelar Guardar

Ni Co

AS64135

Creación de AS-SET en MILACNIC

AS64135

Nombre	ASN Members	AS-Set Members		
AS64135:AS-LabRPKIpermitidos1	AS28000, AS28001, AS12654, AS196615		Editar	Eliminar
AS64135:AS-LabRPKIprivadosTutores	AS65000, AS65001, AS65002, AS65003, AS65004, AS65005		Editar	Eliminar

Volver Agregar

Utilizando bgpq3/bgpq4 (https://github.com/bgp/bgpq4)

- En este caso, usamos el as-set:
- Prefijos IPv4

```
$ bgpq4 -h irr.lacnic.net -l clientes-as65502 AS65502:AS-Transito
no ip prefix-list clientes-as65502
ip prefix-list clientes-as65502 permit 198.51.100.0/24
```

- Prefijos IPv6

```
$ bgpq4 -h irr.lacnic.net -6 -l clientes-as65502 AS65502:AS-Transito
no ipv6 prefix-list clientes-as65502
ipv6 prefix-list clientes-as65502 permit 2001:db8:FFF0:/48
ipv6 prefix-list clientes-as65502 permit 2001:db8:ABCD:/48
```

Utilizando bgpq3/bgpq4 (https://github.com/bgp/bgpq4)

- Otra opción: permitir un conjuto de ASN usando filtro por as-path

```
whois -h irr.lacnic.net AS64135:AS-LABRPKIPERMITIDOS1

as-set:   AS64135:AS-LabRPKIpermitidos1

descr:    Ni Co

members:  AS28000,AS28001,AS12654,AS196615

remarks:  ASNs permitidos para el Lab de RPKI (set No.1)

mnt-by:   MNT-UY-NICO1-LACNIC
```

```
$ bgpq4 -h irr.lacnic.net -f 65000 -l asn-permitidos AS64135:AS-LABRPKIPERMITIDOS1

no ip as-path access-list asn-permitidos

ip as-path access-list asn-permitidos
    permit ^65000(_[0-9]+)*_(12654|28000|28001|196615)$
```

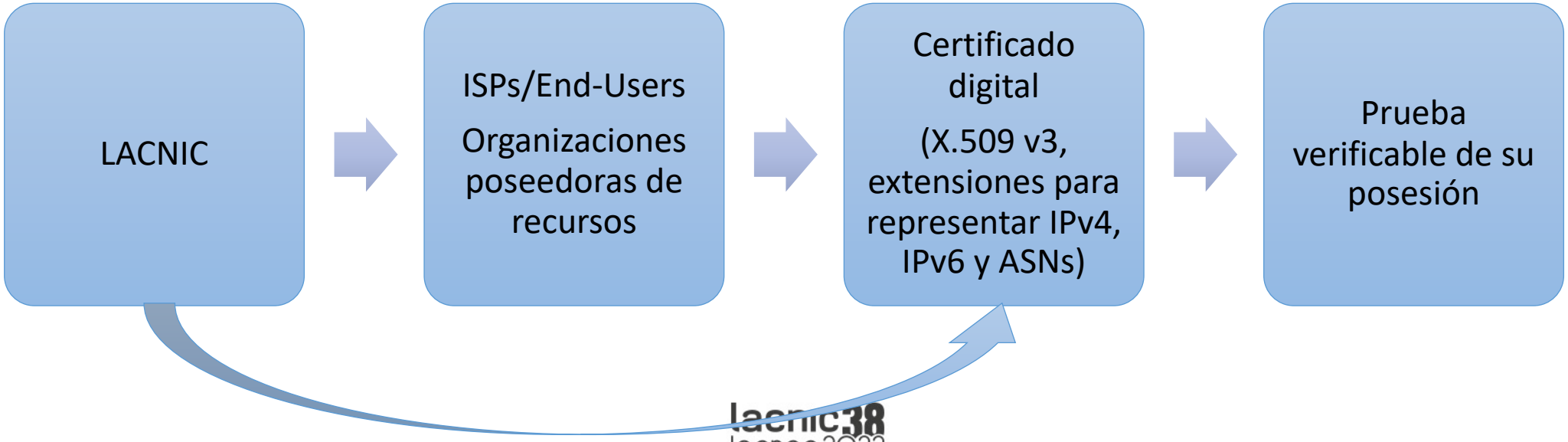
Referencias

- IRR de LACNIC: https://labs.lacnic.net/Uso-de-IRR-LACNIC/
- Peering, IRR y AS-SET: https://www.labs.lacnic.net/Peering-IRR/
- Bgpq4: https://github.com/bgp/bgpq4
- IRRd v4: https://irrd4.readthedocs.io/en/master/users/queries.html

- Documentación Mi LACNIC:
  - General: https://lacnic.zendesk.com/hc/es/categories/360002625214-Internet-Routing-Registry
  - RPKI: https://lacnic.zendesk.com/hc/es/sections/206490008-RPKI
  - IRR: https://lacnic.zendesk.com/hc/es/categories/203940327-Soporte-Mi-LACNIC

RPKI

- Define una infraestructura de clave pública especializada para ser aplicada al enrutamiento
  - En particular, para BGP



¿Qué compone la solución RPKI?

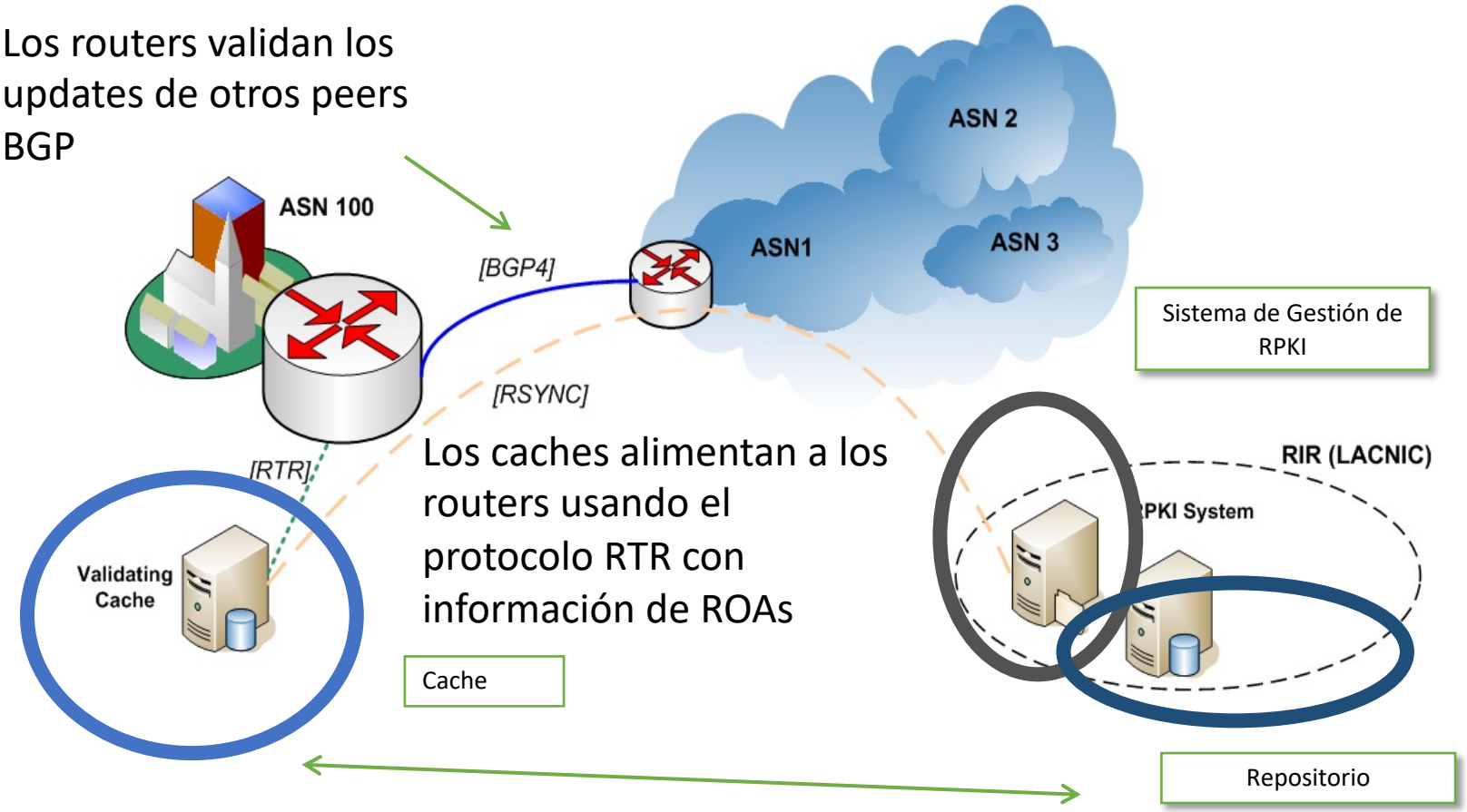
- **ROA**: Objetos firmados digitalmente para soportar seguridad del enrutamiento
  - Equivalentes a route o route6 objects de un IRR
  - Los ISPs u organizaciones pueden ***definir y certificar los anuncios de rutas que autorizan*** realizar
  - Los **ROAs** permiten definir el AS de origen para nuestros prefijos
  - **Firmados** con la clave privada del certificado
  - Toda la información es copiada en un **repositorio públicamente accesible**

- Un **mecanismo de validación** de prefijos
  - Validación de origen

Validación de Origen

RPKI en acción

Los routers validan los updates de otros peers BGP



Los caches alimentan a los routers usando el protocolo RTR con información de ROAs

Los caches traen y validan criptográficamente los certificados y ROAs de los repositorios

Validación de Origen

- Una vez que los routers reciben la información de los caches, tendrán una tabla con:

Prefix	Length	Max length	Origin-AS
200.0.112.0	22	24	65501

- Con esto es posible asignar un ***estado de validez*** a cada UPDATE de BGP
- El estado de validez puede ser:
  - Válido: El AS de origen y el Largo Máximo coinciden con la información del ROA
  - Inválido: La información del ROA no coincide
  - No encontrado: No hay un ROA para el prefijo dado

RPKI en la práctica

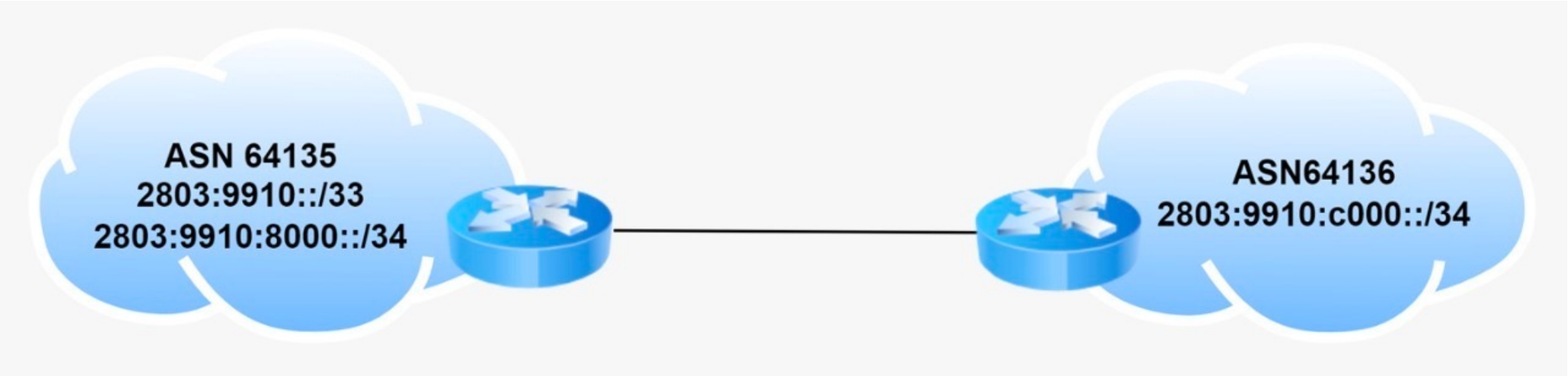
¿Cómo definir los ROA?

- Un ROA es semánticamente equivalente a un route(6) object:
  - **Asocia un prefijo a un ASN de origen**
  - Con esta información es posible hacer chequeo de un anuncio BGP
- Quienes tienen recursos IPv4, IPv6, ASN:
  - Pueden hacerlo desde el sistema de administración de recursos de LACNIC (MiLACNIC)
  - Se necesita para eso los datos de usuario y contraseña de administración de recursos
- Quienes no tienen recursos propios, dependerán del ISP
- Puede haber organizaciones con recursos IP pero no ASN
  - Deben crear los ROA permitiendo a cada ASN (upstream) anunciar los prefijos
  - La creación la realiza quien posee los recursos (diferente modelo que en el IRR en el que lo hace el que posee el ASN)

¿Qué tener en cuenta?

- Verificar cómo estamos realizando los anuncios
- Ejemplo: red 203.0.112.0/22
  - La estamos publicando sumarizada?
  - La estamos publicando desagregada?
    - En bloques de qué tamaño? /23? /24?
  - Con qué sistema autónomo se originan las publicaciones?
  - Siempre es el mismos ASN?
  - Los distintos bloques se anuncian siempre con un mismo ASN?
- Importante: los ROA que creamos deben respetar esta política
- De lo contrario, estaremos invalidando nuestras publicaciones

Ejemplo de peering



Validadores

Software disponible

- RIPE NCC's RPKI Validator 3
  - RIPE ha dejado de mantenerlo desde Julio 2021
  - Uno de los primeros validadores disponibles, muy utilizado, buena interfaz gráfica
- Cloudflare: OctoRPKI & GoRTR
  - Soporte para uso en CDNs, separación clara entre la validación y el protocolo RTR
- NLnetLabs: Routinator 3000
  - Una versión con soporte profesional, muy eficiente en términos de RAM y CPU
- RPKI-client
  - Implementación libre para facilitar la validación de origen de los anuncios BGP. Genera configuración para OpenBGPD o BIRD, pero también otros formatos como CSV o JSON para ser consumidos por otros programas
- LACNIC y NIC.MX: Validador FORT
  - Proyecto FORT incluye el validador y el Monitoreo FORT. El Validador está desarrollado en C y es muy eficiente, muy liviano para ejecutar en una VM

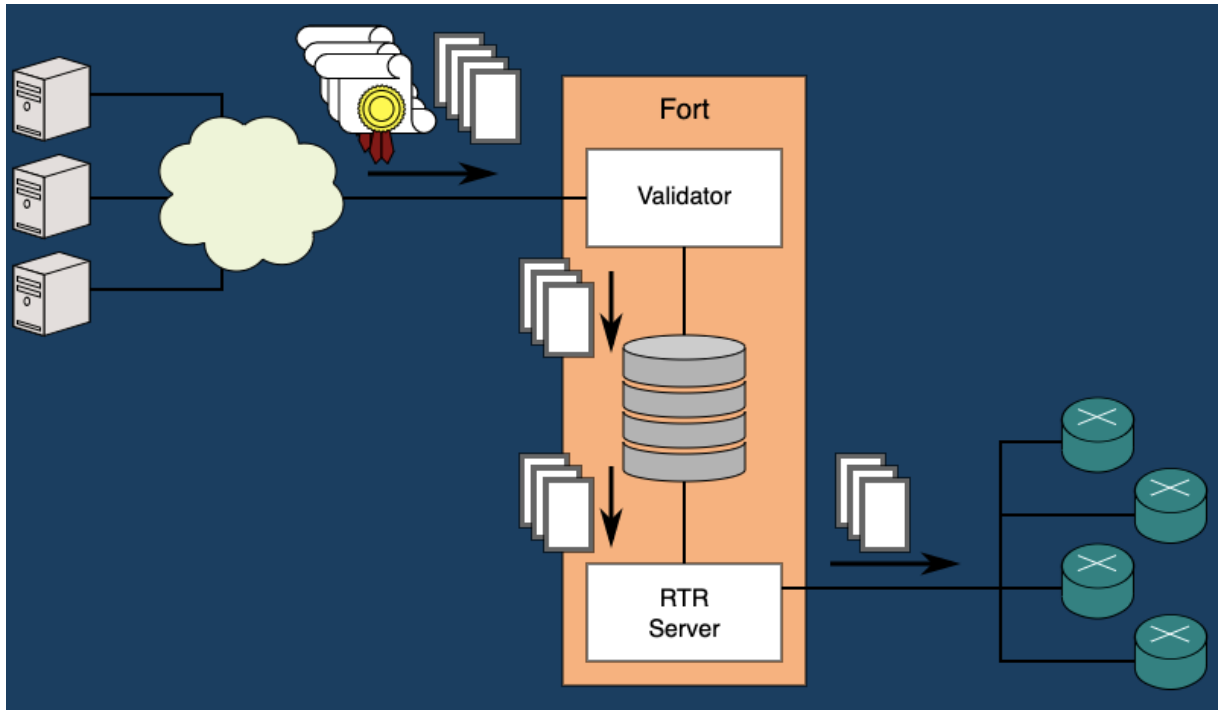
Validador FORT

El validador FORT es un validador RPKI de código abierto

- Es parte del Proyecto FORT, iniciativa conjunta entre **LACNIC** y **NIC.MX**
- Soporte para Linux y BSD
- Desarrollado en C

Documentación general: https://nicmx.github.io/FORT-validator/

Descargar el validador: https://github.com/NICMx/FORT-validator/releases



Herramientas útiles

- Mi LACNIC: https://milacnic.lacnic.net

- LACNIC Tools: https://tools.labs.lacnic.net/
  - Información de los repositorios de RPKI, consultas a RDAP, WHOIS y preguntas directas a servidores de nombres
- Inforedes: https://inforedes.labs.lacnic.net/
  - Información de recursos de numeración, ruteo, conectividad, DNS, RPKI
- Monitoreo FORT: https://monitor.fortproject.net/
  - Cobertura de ROAs, validez de los updates BGP, anomalías en la información de ruteo, etc

- RIPE RIS: https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris
- BGP HE.NET https://bgp.he.net

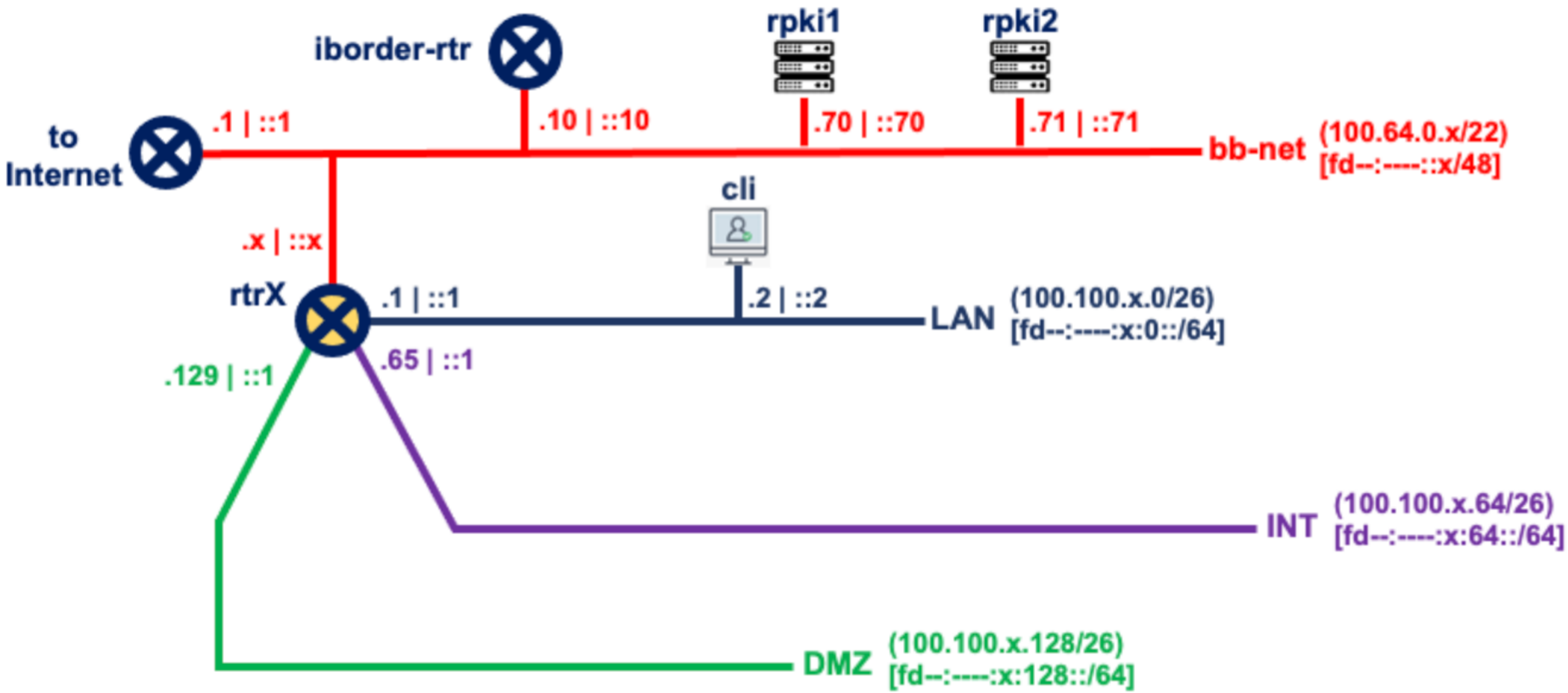
- Cursos de Campus de LACNIC: https://campus.lacnic.net (BGP y RPKI)
- Documentación RPKI: https://rpki.readthedocs.io/en/latest/

Herramientas útiles: BGPalerter y PacketVis

- Es importante monitorear el funcionamiento de RPKI
- A veces hacemos cambios en BGP y olvidamos actualizar RPKI (genera tráfico subóptimo o problemas de accesibilidad)
- Necesitamos poder automatizar la verificación de los ROAs
  - Si los ROAs vencen, si hay problemas en la cadena de validación, si hay problemas en el repositorio, etc
- BGPalerter
  - Es una herramienta open source
  - Hace monitoreo BGP y RPKI
  - GitHub: https://github.com/nttgin/BGPalerter
- https://packetvis.com
  - Es como BGPalerter, pero no necesita instalarlo!

¿Preguntas?

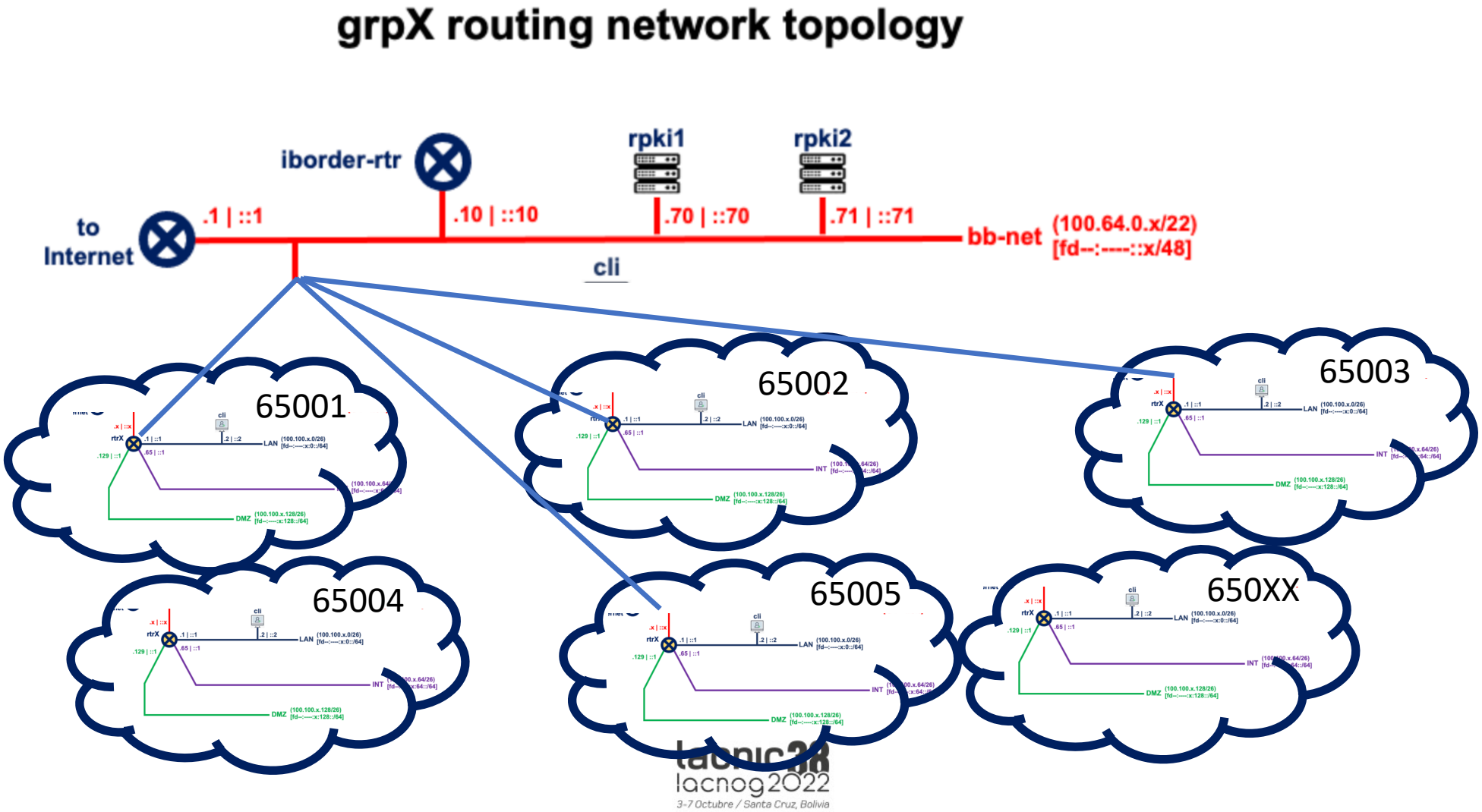
grpX routing network topology



Lab address space: (100.64.0.0/10)
[fd--:----::/32]

Click on selected device to access its terminal

Laboratorio



Registro para práctica

lacnic38
lacnog2022
3-7 Octubre / Santa Cruz, Bolivia

Muchas gracias!

lacnic lacnog Internet Society Capítulo Bolivia