lacnic 45

25 - 28 MAYO / CIUDAD DE PANAMÁ, PANAMÁ

Incidente BGP AS28001 - AS142395

Secuestros de rutas en BGP - *El extraño caso del PDF falso*

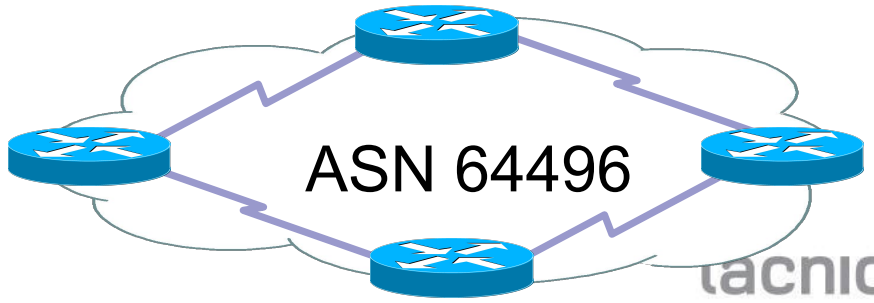
Sistema Autónomo

Sistema Autónomo (RFC 1771): conjunto de routers bajo una misma administración técnica, que usan un protocolo de ruteo interno (IGP) y métricas para rutear paquetes dentro de él, y que usan un protocolo de ruteo externo (EGP) para rutear paquetes fuera de él.

Desde afuera el AS es visto como una entidad única.

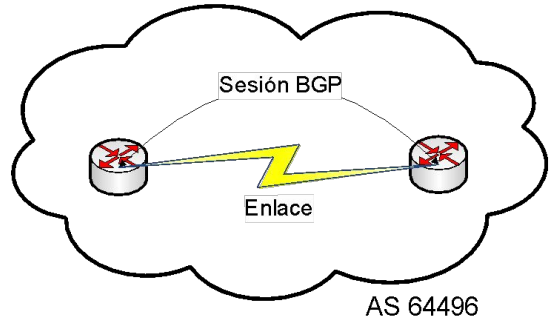
Cada AS tiene un identificador: ASN (Autonomous System Number).

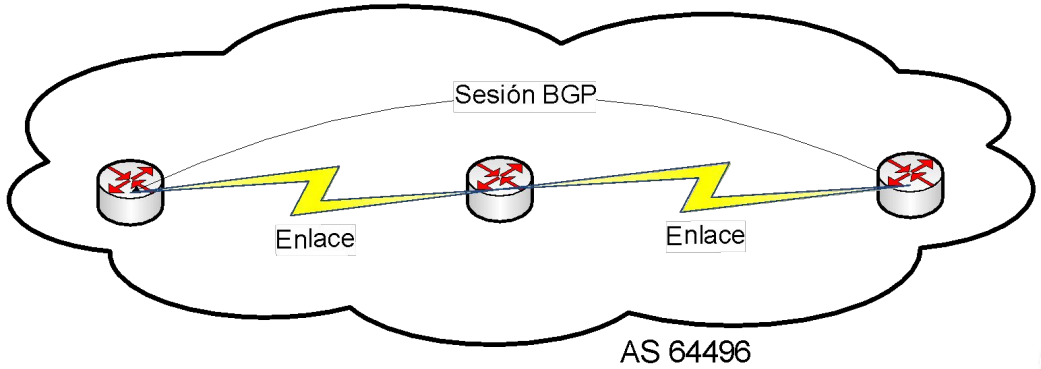
Tiene su propia política de ruteo.



¿Cómo trabaja BGP? Conceptos

- Usa TCP como protocolo de transporte
- Routers Neighbors (o peers)
  - BGP establece entre cada par de routers una conexión TCP, mediante la cual intercambian información de ruteo BGP
- BGP oculta la complejidad interna al resto de Internet





¿Como trabaja BGP? Conceptos

Aprende y enseña rutas

- Para que un router sepa hacia donde encaminar un paquete, alguien tiene que decirle por donde hacerlo (aprende).
- De la misma manera, si queremos que alguien llegue a nuestras redes tenemos que “comunicar” que las tenemos (anuncia).

Para BGP el ruteo interno es un dato de la realidad. Asume que hay otra función (*protocolo de enrutamiento interno, IGP*) en la red que se encarga de generar las rutas internas.

- BGP toma estas rutas y las comunica al resto de Internet.

¿Como trabaja BGP? Conceptos

Aprender una ruta:

Significa que voy a incorporar en mi tabla de BGP (*y eventualmente a mi tabla de enrutamiento)* alguna ruta que me están enseñando.

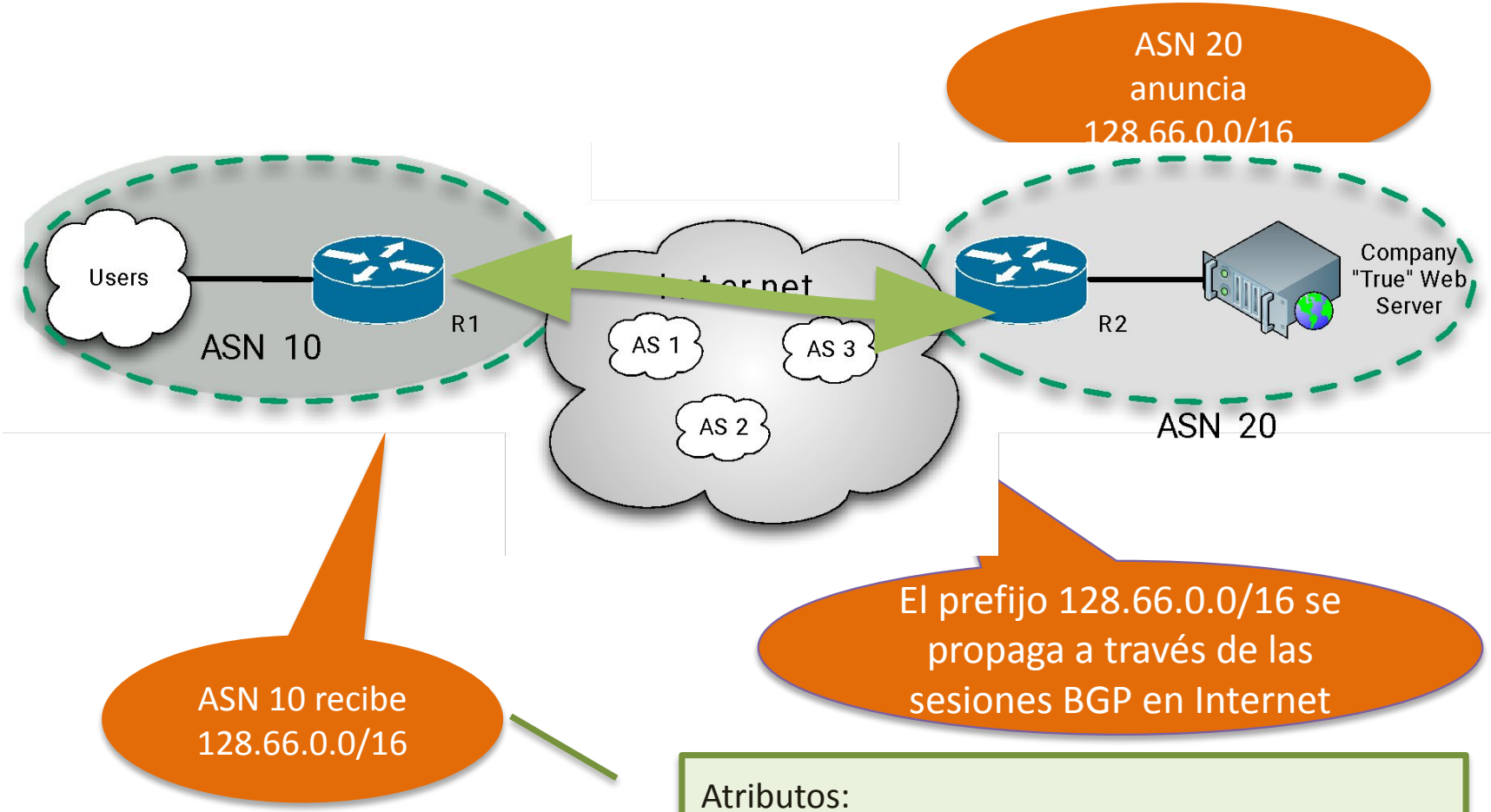
Anunciar una ruta:

Significa que le voy a decir a alguien que tengo una ruta para llegar a determinado destino. No basta con tener la ruta en mi tabla de BGP, la debo tener también en mi tabla de ruteo.

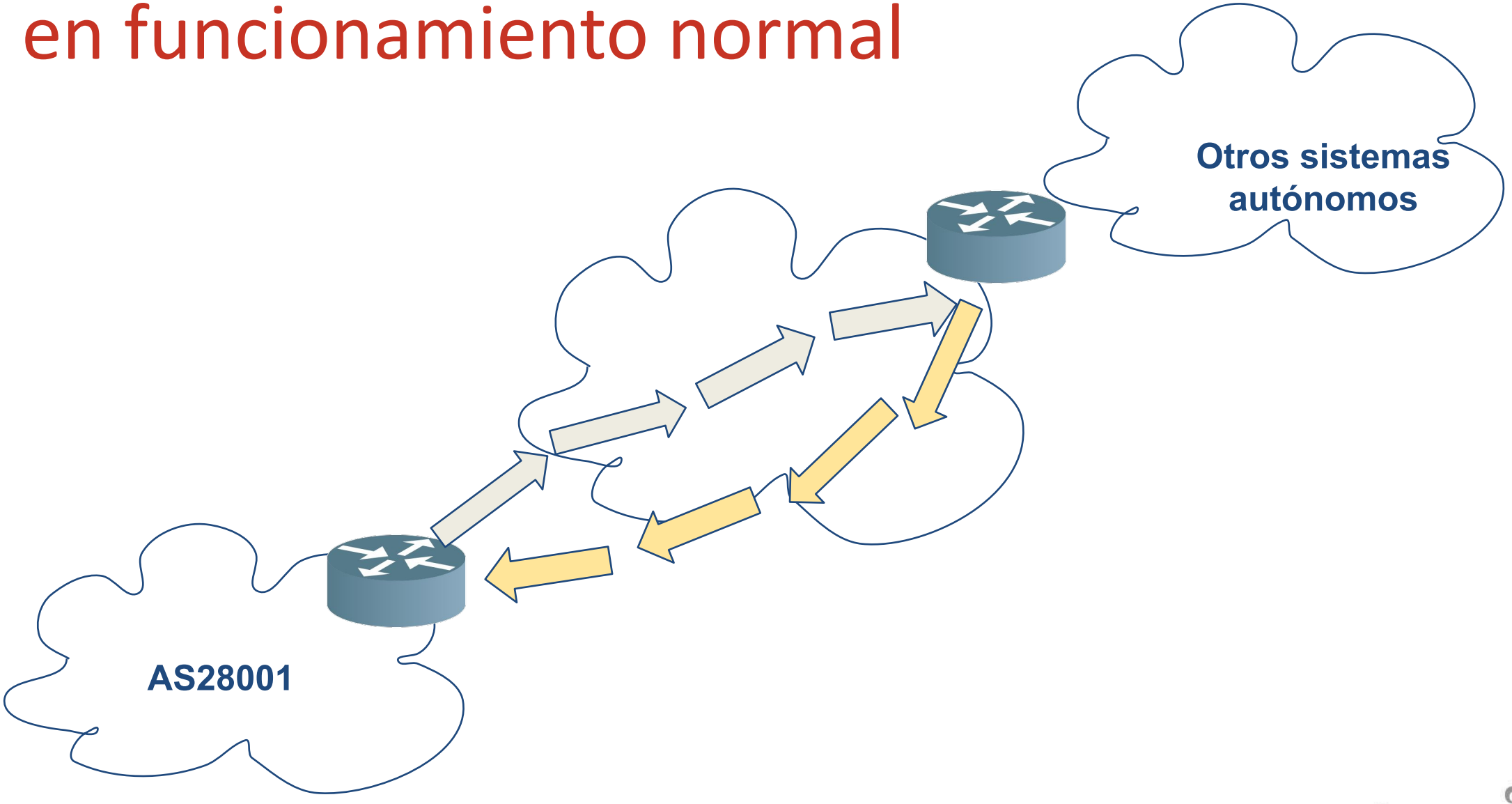
¿Como trabaja BGP? Conceptos

AS Path:

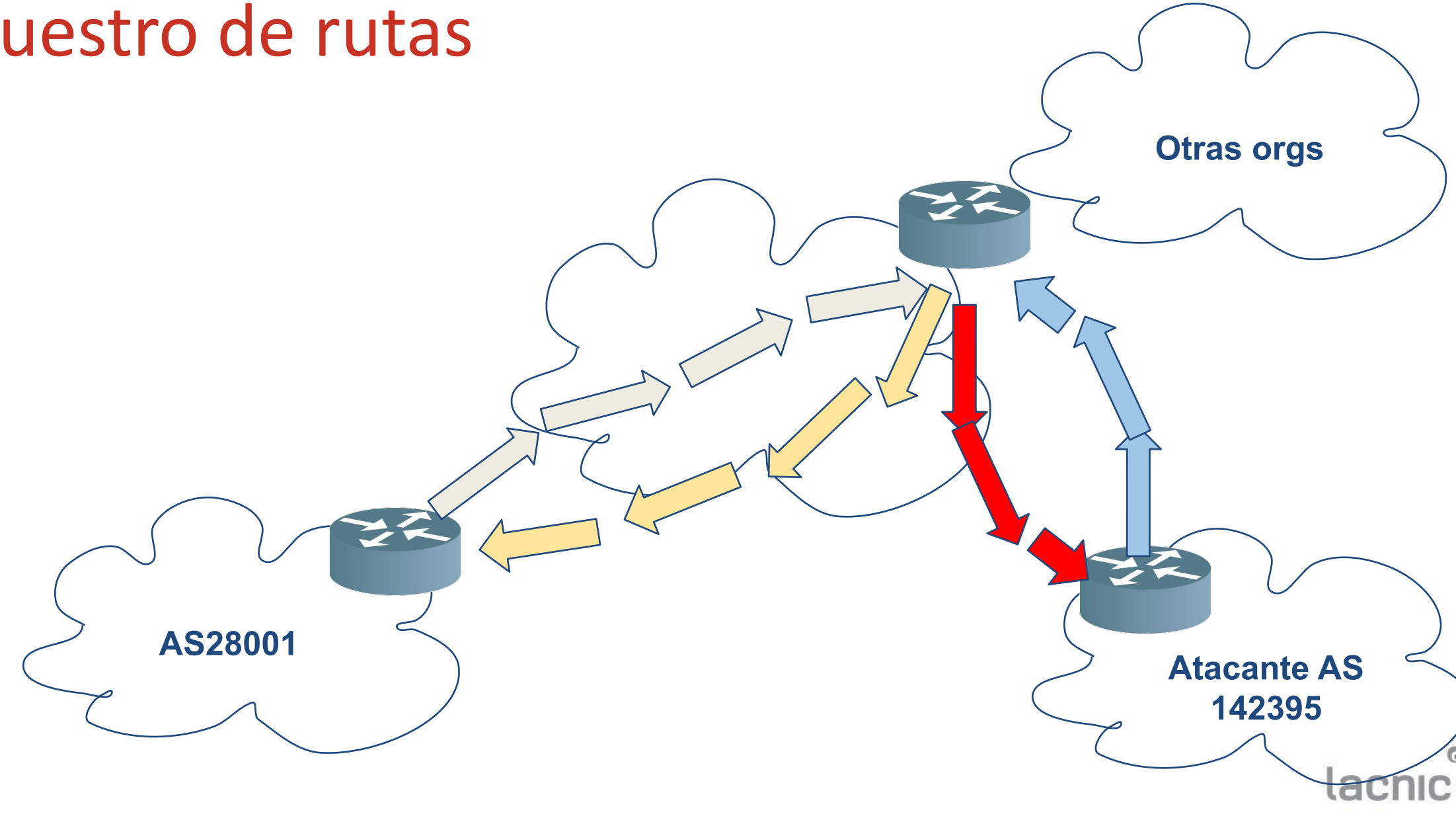
- El AS Path es un *atributo* de las rutas anunciadas que registra la lista de sistemas autonomos que un anuncio atraviesa



BGP en funcionamiento normal



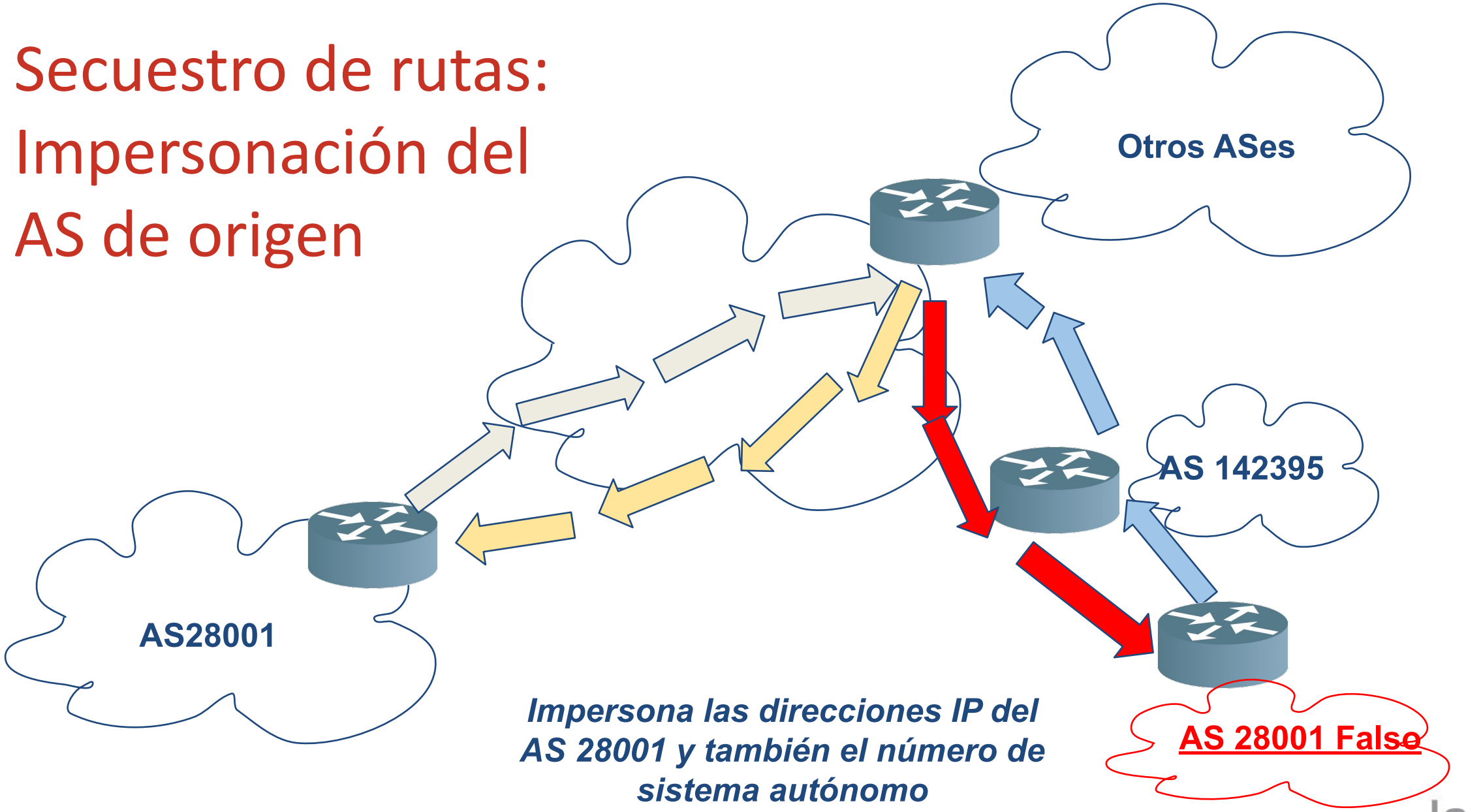
Secuestro de rutas



¿Que pasó entonces?

- Soporte LACNIC recibió quejas sobre la falta de entrega de mensajes de correo electrónico.
- Parte del espacio de direcciones asignado a LACNIC fue **secuestrado** por un AS (Sistema Autónomo) no autorizado.
- Fueron secuestrados no solos los prefijos que usamos en San Pablo, sino que también hubo una suplantación del AS de LACNIC.

Secuestro de rutas: Impersonación del AS de origen



Impersona las direcciones IP del AS 28001 y también el número de sistema autónomo

Observaciones

- La “impersonación” de direcciones IP puede ocurrir por error
  - *Es relativamente común*
- La “impersonación” de direcciones IP + la “impersonación” del **número de sistema autónomo no puede ocurrir por error**
  - Indica que el evento es dirigido hacia nosotros en este caso
    - Sabemos que este mismo AS de Indonesia también estuvo realizando este tipo de actividades contra otras organizaciones de nuestra región y de otras



¿Cuáles fueron los efectos?

- El espacio de LACNIC fue secuestrado intermitentemente:
  - 9 de julio de 2025 a las 19:47 (GMT-3) por 20 minutos.
  - 10 de julio de 2025 a las 20:34 (GMT-3) por 15 minutos.
  - 12 de julio de 2025 a las 10:13 (GMT-3) por 5 minutos.
  - No ocurrieron más eventos.
- Durante estas ventanas de tiempo el resto de Internet (incluyendo la red de LACNIC en Montevideo) tuvo dificultades para acceder a los servicios de LACNIC en San Pablo

Motivaciones

¿Porque alguien haría esto? Es difícil saberlo con exactitud, algunas razones podrían incluir:

- Actividad exploratoria
  - Entender la postura de seguridad de LACNIC
- Intento de capturar cuentas de MiLACNIC
  - Tratar de forzar recuperaciones de clave y capturar el correo con un enlace para cambiar la clave
- Denegación de servicio
  - Impedir el acceso normal a los servicios, generalmente con fines extorsivos
- Robo de información con fines extorsivos directos o para venta en la *dark web*

La investigación

- El AS que daba tránsito al “falso” 28001, el 142935, pertenece a una organización basada en Indonesia.
- Nos pusimos en contacto con el equipo de APNIC, en particular con su equipo de seguridad y con miembros del equipo de APNIC que tienen vinculación con la comunidad de Internet de Indonesia
- Sanjaya (APNIC) llevó el tema a un organismo apropiado (APJII) en Indonesia y solicitó se realizara una investigación.

Los resultados de la investigación

Esto se pone cinematográfico.

¿Como se establecen los acuerdos de peering y tránsito en BGP?

- Dos organizaciones (A y B digamos) expresan su intención :
  - A va a anunciarle a B una cierta lista de rutas desde un cierto número de ASN
  - B acepta propagarlas al resto de Internet
- Requisitos de verificación
  - B debe estar *segura* de que A tiene derecho tanto tanto a usar el ASN como a anunciar las rutas que expresó en el acuerdo

Verificación de datos

¿Cómo se verifican los datos que están expresados en el acuerdo de sesión BGP?

- LoA : Letter of Authorization
- Verificaciones de los datos expresados en la LoA en:
  - WHOIS
  - IRRs (RADB, RIPE, LACNIC)

Letters of Authorization

Es así de precario como se ve:

- Un PDF firmado con una firma escaneada (a veces ni eso)
- Un listado de prefijos y eventualmente un número de ASN que va a ser utilizado

Es obligación de quien presta el servicio el verificar que estos datos son reales

lacnic

Montevideo, 4 de abril de 2018

Carta de Autorización para el anuncio y tránsito de prefijos

A quien corresponda:

LACNIC – El Registro Regional de Direcciones IP para Latinoamérica y el Caribe (UY-LACN-LACNIC), ASN 28002, le otorga a UFINET PANAMA S.A. – AS 52468 el permiso para hacer tránsito, en nuestro nombre, de los siguientes prefijos:

Origin ASN: 28002

IPv4: 45.6.248.0/21
200.0.86.0/23

IPv6: 2001:13c7:7003::/48

Atentamente,



Carlos Martínez
CTO - LACNIC

Resultados de la investigaci´

Alguien en Indonesia, usando un PDF falso y engaños varios consiguió que un ISP internacional le aceptara anunciar prefijos de LACNIC usando el sistema autónomo de LACNIC.

El engaño también incluía a un ISP de Indonesia (AS142395) que en realidad también resultó ser una víctima del incidente.



Montevideo, 4 de abril de 2018

Carta de Autorización para el anuncio y tránsito d… …os

A quien corresponda:

LACNIC – El Registro Regional d… …mérica y el Caribe (UY-LACN-LACNIC… PANAMA S.A. – AS 524… …tro nombre, de los sigui…

Origin ASN:

IPv4: 45.6.24… 200.0.86.…

IPv6: 2001:13c7:7…

Atentamente,

Carlos Martínez
CTO - LACNIC

Pero pero espera un poquito: ¿Y RPKI?

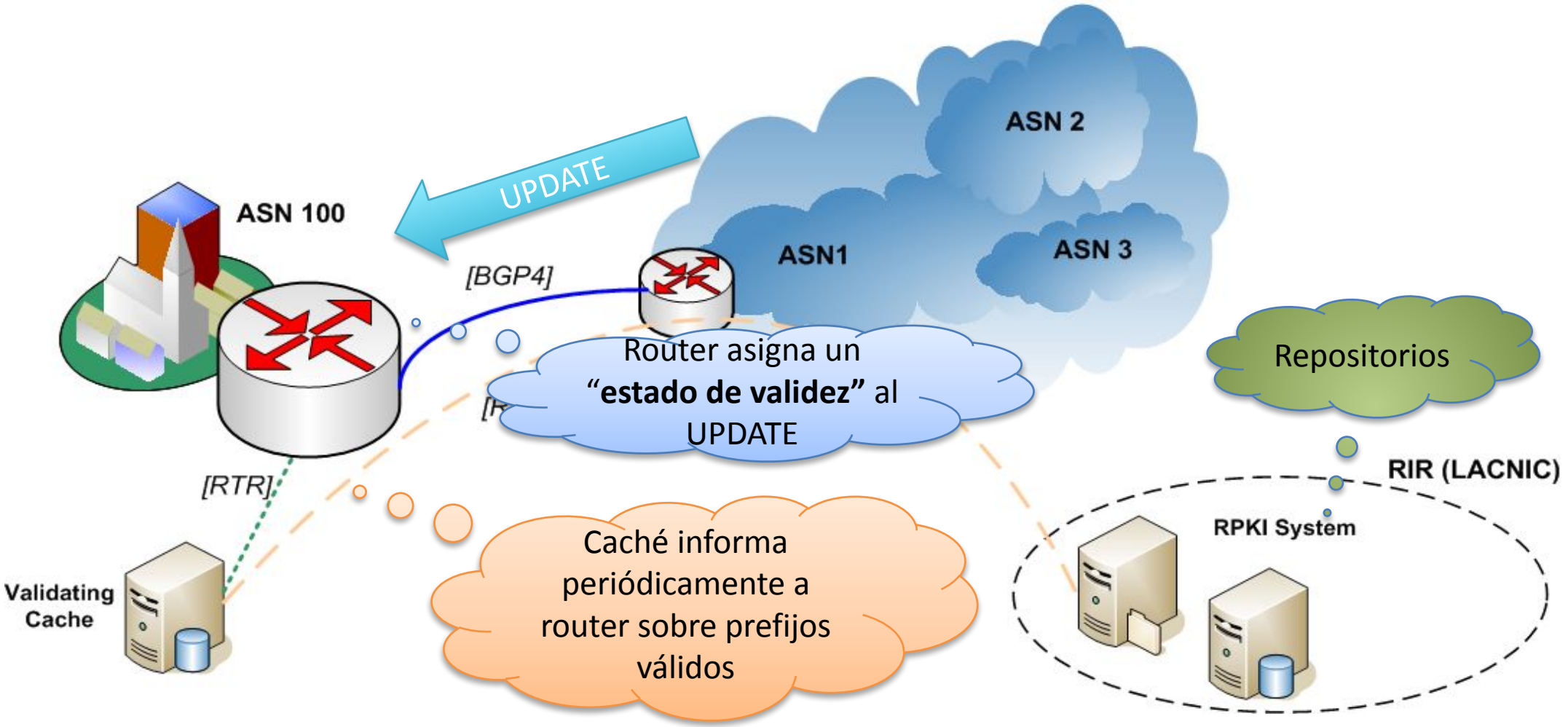
¿RPKI / ROA no era lo que justamente para proteger el enrutamiento de casos como este?

- RPKI/ROA protege el **origen de las rutas** entendido como el primer sistema autónomo que inyecta una ruta en Internet
- Los enrutadores pueden leer los ROAs y comparar el AS de origen autorizado con el AS de origen que ven en los mensajes de BGP

En este caso el atacante **también falsificó el AS de origen**, con lo que la protección de RPKI no resultó efectiva.

ASPA es una nueva funcionalidad de RPKI que justamente apunta a proteger Internet de este tipo de escenarios.

RPKI


ASN 100
UPDATE
[BGP4]
ASN 2
ASN1
ASN 3
Router asigna un "estado de validez" al UPDATE
Repositorios
RIR (LACNIC)
[RTR]
RPKI System
Validating Cache
Caché informa periódicamente a router sobre prefijos válidos

¡Gracias! ¡Ahora vamos con la 2a parte!