Material de descarga - Módulo 5
Conceptos de RPKI

Introducción:

Bienvenidos al quinto módulo del curso “Fundamentos de BGP e introducción a RPKI” de LACNIC. A lo largo de los 4 temas que comprenden este módulo se podrá aprender acerca de la confiabilidad del ruteo, a qué se le llama secuestro de rutas, cuáles son las medidas de protección que se pueden tomar y qué implica la certificación de recursos.

TEMA 1 - La confiabilidad sobre la información de ruteo en Internet

Desde los comienzos del curso se ha dejado claro que BGP es el protocolo que se utiliza en Internet para la comunicación entre los Sistemas Autónomos, permitiendo que la información de ruteo pueda fluir entre ellos.

Se ha visto cómo trabaja BGP, cómo se configura para que anuncie y/o aprenda rutas, lo cual permitirá que se alcancen los destinos, y se ha visto también que para hacer más controlado el proceso de pasaje de rutas es aconsejable tomar medidas con la implementación de filtros, o sea, políticas.

No obstante, es importante aclarar que Internet ha funcionado desde siempre gracias a una gran cadena de confianza que se establece entre los operadores de las redes para que el ruteo pueda llevarse a cabo lo mejor posible.

Dicho de otra manera, la confianza en Internet radica en que cada organización anuncie sólo sus propios prefijos, o los prefijos de las organizaciones a las que le da tránsito. Sin embargo, eso no está garantizado en BGP, sino que se basa en el buen trabajo que hagan los operadores de las diferentes redes.

Este trabajo confiable de los operadores de redes se puede complementar con diferentes medidas, algunas de ellas serán descritas a continuación.

Para intentar hacer más confiable la información que se recibe de los *neighbors*, una organización puede tomar medidas como ser: valerse de algún *IRR* para recibir y anunciar rutas (se podrá ver información de cómo

funciona un IRR en irr.net), proteger a los dispositivos *routers* para que no puedan ser accedidos en forma indebida, implementar la autenticación entre *peers*, entre otras medidas.

Otra medida que complementa y ayuda al trabajo de los operadores de redes es la implementación de filtros basados en el RFC1918, el cual describe a las redes que son de usos privados y/o reservados, y que no deben ser anunciados a Internet, como por ejemplo las redes de uso sólo en LAN, las redes para *multicast*, los bloques para documentación, entre otras. Se recomienda consultar este RFC en la URL: https://tools.ietf.org/html/rfc1918

La aplicación de estas medidas por parte de cada una de las organizaciones ayuda a que Internet funcione de una manera confiable.
¿Y por qué esto resulta tan importante?

Como se ha visto en los contenidos de este curso, cuando se reciben rutas, se está afectando al tráfico saliente de la organización. En forma análoga, cuando se anuncian rutas, se logra afectar el tráfico entrante. Entonces, con esto se deduce que, si las rutas que se reciben son incorrectas, los *routers* estarán encaminando los paquetes en forma errónea basados en la información que han recibido. ¿Y qué sucede si las rutas que se anuncian a otros sistemas autónomos no pertenecen a quien las anuncia? Entonces el tráfico que no es para la organización que anuncia, será atraído hacia ésta.

Cuando ocurre este proceso, en el cual algún dispositivo en el *routing* de Internet anuncia un prefijo que no le corresponde anunciar por no estar autorizado a hacerlo, ya sea porque no es propio o porque no es parte de los sistemas autónomos a los que le da tránsito, se produce lo que se denomina “Secuestro de rutas”, o “*route hijacking*”, y en el próximo tema se tratará este concepto en detalle.

Tema 2 - Secuestro de rutas

Tal como se definió en el tema anterior, se le llama “Secuestro de ruta” a la acción de anunciar a Internet prefijos cuando no se está autorizado a hacerlo.

Este anuncio “indebido” puede ser intencional o por error en la operación. Existen varios ejemplos sobres este tipo de incidentes que han ocurrido en lo últimos años y que merecen la pena repasar.

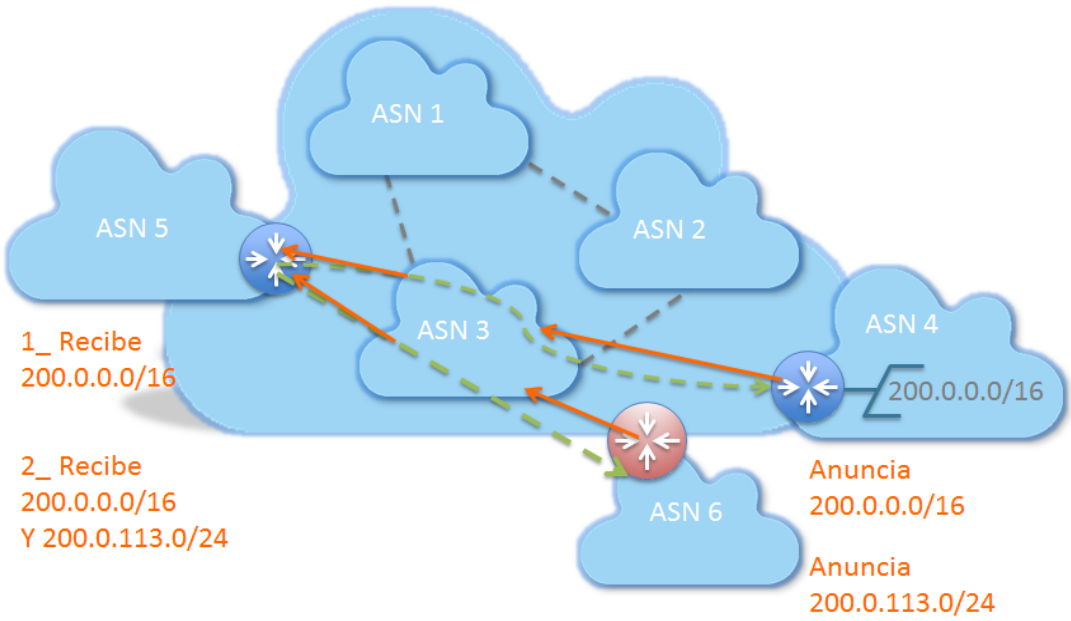
Los casos más conocidos de este tipo de incidentes son los siguientes:

- El ocurrido entre Pakistan Telecom y YouTube, en el año 2008.
- El de China Telecom, del año 2010.
- El de Google en Europa del Este, que afectó a varios ASs en el año 2010.
- Muchos más casos, incluso en nuestra región, que están incrementándose en los últimos años.

Información sobre estos incidentes puede ser encontrada fácilmente en Internet, por ejemplo en: http://www.youtube.com/watch?v=IzLPKuAOe50 y http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study pero más allá de los detalles, todos estos incidentes fueron provocados por errores en la operación, los cuales no duraron más que minutos hasta ser solucionados, pero que afectaron a decenas de miles de usuarios.

Veamos en detalle cómo es que se desarrolla un secuestro de rutas a través de un ejemplo.

Supongamos que tenemos el siguiente esquema de conexión de ASs en Internet, y el ASN4 es una organización dueña del prefijo de red 200.0.0.0/16. Este ASN4 anunciará a Internet el prefijo mencionado (según flechas naranjas):



El ASN5 recibirá el anuncio del ASN4 y sabrá por donde encaminar los paquetes que deben llegar a él (línea punteada verde)

Un ASN6 comienza a anunciar a Internet el prefijo 200.0.113.0/24, que claramente no le pertenece pues ya se ha visto que es propiedad del ASN4. No obstante, al hacerlo, veamos qué recibe el ASN5 que vimos anteriormente: recibe dos prefijos para el 200.0.113.0, pero uno más específico, que es el /24, por lo que el ASN5 redirigirá el tráfico para alcanzar a la red 200.0.113.0/24 a través del ASN6. Y así como hace el ASN5, lo harán todos los sistemas autónomos que reciban este prefijo más específico.

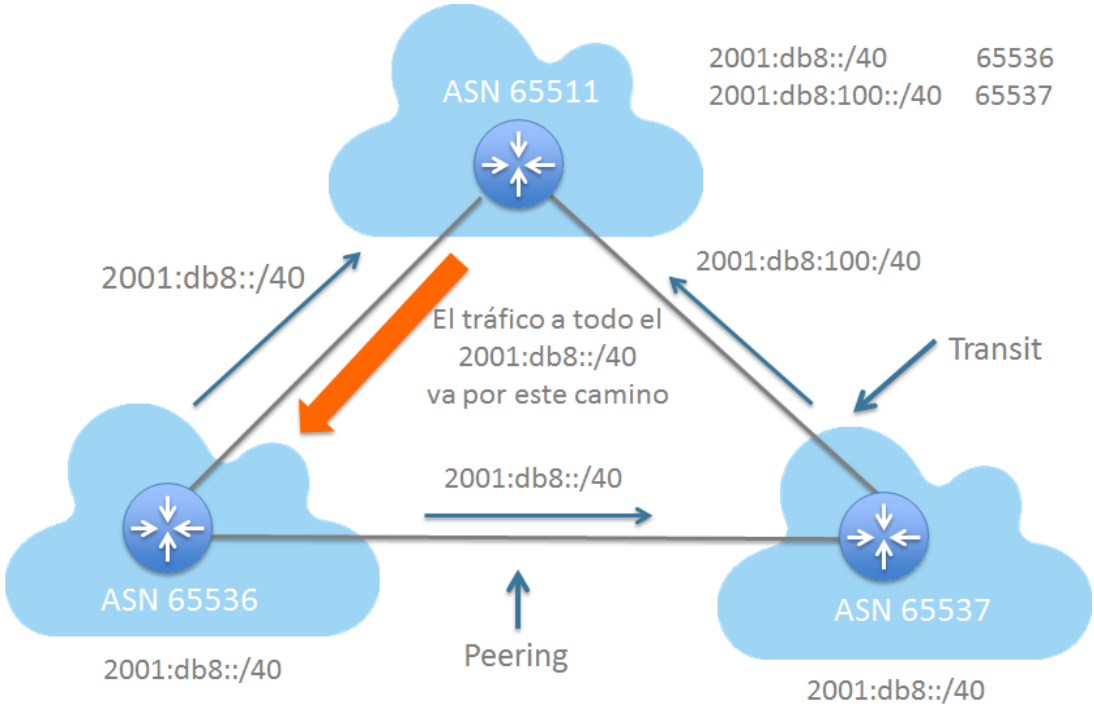
Se acaba de mostrar un ejemplo de cómo es que se lleva a cabo un secuestro de rutas. Notar que este ejemplo sirve tanto para los secuestros de rutas intencionales como para los que ocurren por un error de operación en la red. Sin embargo, lo que debe quedar claro es que en este tipo de eventos lo que sucede es que un AS anuncia un prefijo que no le pertenece.

Una situación distinta se produce cuando el camino se ve afectado no porque un AS anuncie un prefijo que no tiene, sino porque haga un “mal anuncio”, como podría ocurrir en un AS de tránsito.

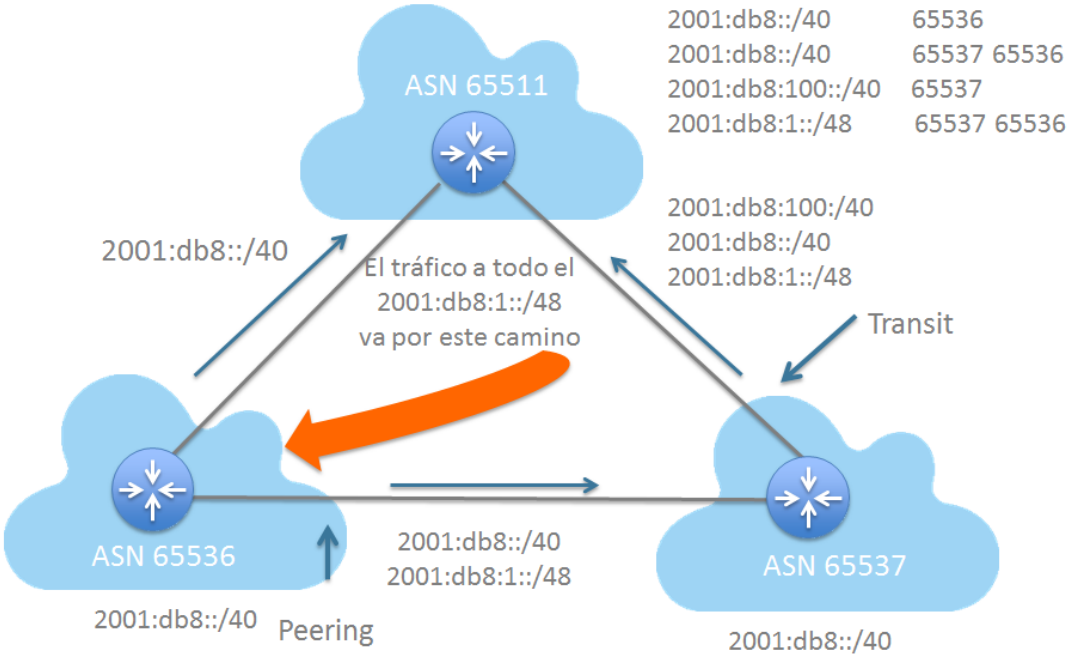
Muchas veces a estos eventos se le llama “***route leak***”, y aunque no hay un claro consenso sobre eso, es interesante que se vea el RFC7908 (https://datatracker.ietf.org/doc/rfc7908/), pues puede ayudar a ver las diferentes posturas respecto a la definición del término.

No obstante, se verá un ejemplo que, para que sea más claro se mostrará con direcciones IPv6.

En este primer ejemplo se ve cómo se comporta un ASs que no producen un *route leak*:



Ahora se verá cómo es el comportamiento de los ASs cuando sí se produce un *route leak*:



Se deberá notar que el ASN65537 no "mintió" al anunciar la ruta más específica, a diferencia de lo que ocurre en los casos de *route hijacking* que vimos. El ASN65537 recibe efectivamente el bloque que por error se le "escapa" al ASN65536, pero al darle tránsito a todo su prefijo /40, termina anunciando una ruta más específica.

Existen otras acciones que atentan contra el buen ruteo en Internet. Por ejemplo, aquellas que se manifiestan como ataques con el camino o *path*.
Una técnica para realizar este tipo de ataques es la de insertar en el mensaje UPDATE, no solo el propio AS sino más números de sistemas autónomos.

Otro tipo de ataque al camino consiste en originar una ruta para determinado prefijo, pero, hacerlo utilizando un ASN que no es el que corresponde que origine rutas para ese prefijo.

Tema 3 - Diferentes medidas de protección

Se comenzará a tratar el tema sobre las medidas que hay disponibles para ayudar a mitigar los problemas de ruteo causados por ataques o malas operaciones de redes. A esta tarea ayuda mucho tener en claro quiénes son

los que pueden utilizar los recursos sensibles de Internet como ser direcciones IPv4, direcciones IPv6 y números de sistemas autónomos.

Por ejemplo, ¿qué medidas podría tomar un ISP? Una de ellas sería indicarle a sus *upstream* u organizaciones con las que mantiene acuerdos de *peering*, cuáles son los bloques IP que se les va a anunciar, como una suerte de acuerdo previo que permita implementar filtros a medida. Esto puede hacerse de una manera informal, cuando los operadores se conocen, mediante un e-mail o un llamado telefónico. Pero cuando estas organizaciones se interconectan con otras y ya no hay tal posibilidad, ¿cómo verificar que los anuncios que se reciben de un *neighbor* son correctos?

Otra forma es que se dé a conocer entre los peers la base de datos de recursos de Internet que se utilizará para verificar la información de pertenencia de los recursos, tal como se mencionó en el tema anterior, y que puede hacerse a través del servicio de **Internet Routing Registry** o **IRR**. En estas bases de datos las organizaciones listan, no sólo los recursos que poseen, sino también la política de ruteo que implementan: cuáles son sus *peers*, qué anuncian a cada uno y qué se acepta recibir de ellos, entre otros datos. Con toda esta información se puede automatizar el filtrado y configuración de políticas de entrada en los routers. Una de las bases de datos IRR más conocidas es RADB; a su vez, los RIRs suelen implementar IRRs. Al día de hoy, LACNIC no cuenta con una base de datos de este tipo.

Además de esto, complementan la medida que, independientemente de la información suministrada por el *peer*, los operadores de redes utilicen información de los servicios de "***whois***" con el fin de verificar el derecho de uso del recurso.

No obstante, ninguna de estas fuentes provee información firmada, ni mecanismos que garanticen la autenticación de derecho de uso. Por tal motivo se dice que la integridad de Internet depende de la confianza entre quienes la operan, la confianza que se pueda generar entre los administradores de redes de todos los sistemas autónomos que componen la gran red de redes. Algunos operadores reemplazan esta ausencia de mecanismos de firma de la información por cartas escritas por parte de la organización, llamadas ***LoA***, firmadas de puño y letra. Esto puede ser fácilmente falsificado y no resulta de gran utilidad en la automatización.

No obstante, existe una propuesta de solución que poco a poco va ganando terreno entre las implementaciones de seguridad en redes, que se denomina **RPKI**.

Se verá entonces cuál la propuesta de solución de RPKI.

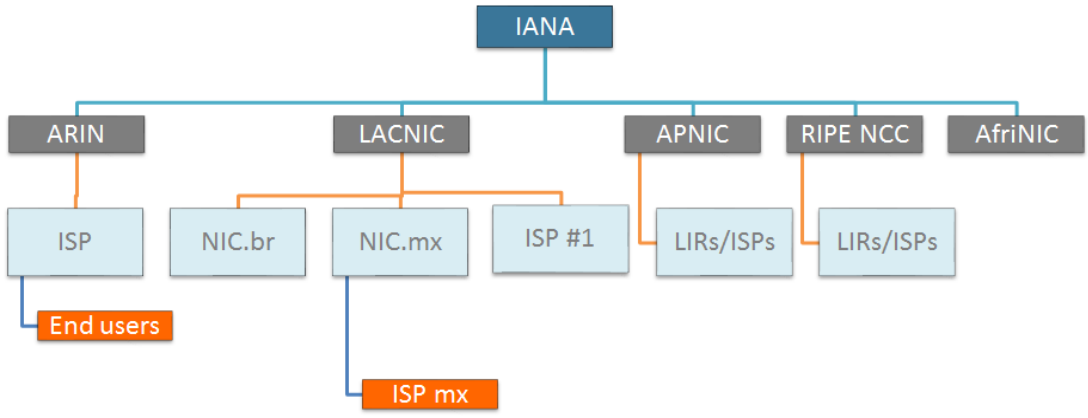
Tema 4 - Certificación de recursos

RPKI, por sus siglas en inglés de ***Resource Public Key Infraestructure***, propone un mecanismo para validar que el sistema autónomo que origina una ruta sea el que está autorizado a hacerlo. Implementando RPKI, los ejemplos que hemos visto sobre secuestros de ruta y *route leaks* podrían evitarse.
Importante: RPKI sólo previene problemas que devienen del origen de la ruta, no de otros ataques.

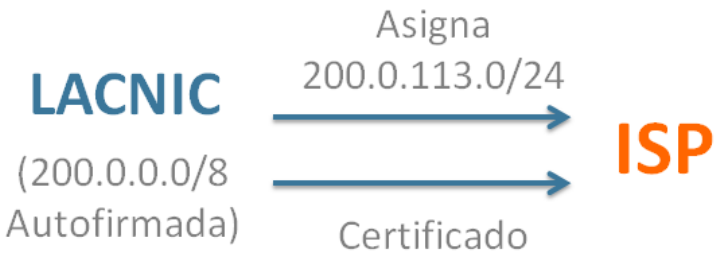
RPKI, tal como se mencionó, permite que se valide el derecho de una organización a utilizar un recurso como ser IPv4, IPv6 o ASN.

Básicamente lo que hace es combinar la jerarquía del modelo de RIRs con el uso de certificados digitales basados en el estándar X.509, los cuales tienen una extensión para soportar IPs y ASNs (para el caso, ver RFC 3779).
Punto importante a destacar: RPKI es un estándar de IETF, según los RFC 6480 - 6492.

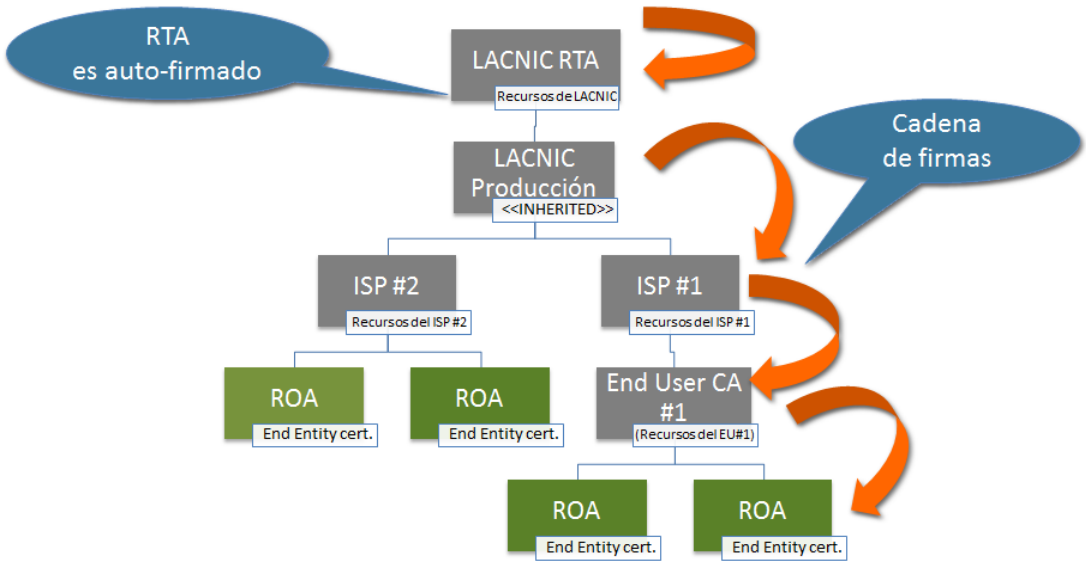
Hemos visto al comienzo del curso cómo es que los recursos de Internet se asignan desde IANA. Es importante tener en cuenta que entonces un RIR es una fuente autoritativa de información sobre el recurso y el usuario del mismo, de esta manera:



Esto permite generar una **PKI** sobre los recursos, donde la raíz de la cadena de confianza son los RIRs (por ejemplo como LACNIC en nuestra región) y mediante certificados digitales se construye una cadena de firmas hasta certificar los recursos de una organización. Por ejemplo: si un ISP tiene asignado el prefijo 200.0.113.0/24, podrá obtener un certificado de parte de LACNIC sobre dicho prefijo, que será firmado con la clave asociada al certificado 200.0.0.0/8 de LACNIC. A su vez, el 200.0.0.0/8 está firmado con la clave raíz (que es autofirmada):



Lo que se muestra ahora en la figura es la estructura de la RPKI de LACNIC:



Una vez que la organización tiene sus recursos firmados, podrá crear unos objetos llamados ROA (del inglés ***Route Origin Authorizations***), firmados digitalmente, que proveen una autorización explícita por parte del

poseedor de un prefijo permitiendo a un ASN originar rutas de ese rango.

En fin, usando certificados podemos crear objetos que identifiquen el origen de un prefijo.

Los ROAs contienen información sobre el AS de origen permitido para un conjunto de prefijos. Son firmados usando los certificados generados por RPKI, y luego los ROAs firmados son copiados al repositorio.

¿Qué información tienen o declaran esos ROAs? Básicamente un conjunto de prefijos, con su longitud y máximo permitido (/20 a /24 por ejemplo) y el ASN de origen de estos (también el período de validez del ROA).

Con esto, tenemos una fuente de información firmada digitalmente contra la cual podemos contrastar los UPDATEs que recibimos por BGP: si el ASN de origen de un prefijo en BGP coincide con un ROA generado por el poseedor de ese prefijo, entonces ese anuncio será correcto, o sea "válido". De lo contrario, será inválido. Puede suceder también que no exista un ROA que cubra ese prefijo, en ese caso tendremos un tercer estado que será incompleto o "not found" (este sería el caso de los prefijos de organizaciones que no han implementado RPKI).

Con todo lo mencionado, se está en condiciones de definir cómo está compuesta la solución de RPKI, y es de la siguiente manera:

- PKI (Public Key Infrastructure) de recursos, los cuales estarían integrados por las direcciones IP y ASN asignados, más los certificados de pertenencia otorgados por el RIR (y otra información de PKI).
- Objetos firmados digitalmente para soportar seguridad del enrutamiento, o sea los ROAs.
- Un repositorio distribuido que almacena los objetos PKI y los objetos de enrutamiento firmados. Este repositorio es público y puede ser copiado localmente por organizaciones que quieran utilizarlo (o sea, como si fuera un cache).

La solución obtiene su cierre cuando se lleva a cabo la “Validación”.

La validación es el proceso automatizado que llevan adelante los ISPs u organizaciones que quieren contrastar los anuncios de BGP, o sea los

UPDATE, contra la base de RPKI, o sea, los repositorios, y de esa forma verificar que los anuncios tienen una procedencia autorizada.

Durante el proceso de validación, los ISPs interesados utilizarán:

– Las propiedades del cifrado de clave pública (o sea, los certificados)

– Las propiedades de los prefijos.

En resumen, ¿qué debería hacer una organización que desea implementar RPKI para validar el origen de sus rutas?

En primer lugar, debería generar certificados digitales sobre sus recursos IPv4, IPv6 y ASN.

Luego generar los ROAs correspondientes a los anuncios de BGP que va a realizar. Esta acción es la que más cuidado merece, pues un ROA mal generado, que no contemple todos los prefijos podría invalidar a alguno de estos.

Una vez que la organización hizo estos dos pasos, ya cuenta con una certificación digital para los anuncios BGP sobre sus recursos.

Luego, las organizaciones que deseen utilizar la validación sobre los recursos de quien ya implementó RPKI podrá hacerlo, y con ello asegurarse la procedencia de las rutas, pero esto es un proceso independiente a la organización que firma sus propios recursos.

Hasta aquí se ha visto cómo es la solución de RPKI que permite la certificación de recursos. En el próximo módulo se verán recomendaciones y mejores prácticas en BGP.