Informe técnico sobre BGP RPKI With XR7 Cisco8000

Contenido

Introducción

Este documento describe la función de la Infraestructura de clave pública de recursos (RPKI) del Protocolo de gateway fronterizo (BGP) en la plataforma Cisco IOS® XR.

Antecedentes

Prefacio

Este documento explica la función BGP RPKI y cómo protege BGP con routers contra actualizaciones de prefijo BGP falsas/maliciosas.

Alcance

Este documento utiliza Cisco 8000 con XR versión 7.3.1 para demostración. Sin embargo, BGP RPKI es una función independiente de la plataforma; los conceptos descritos en este documento se aplican a otras plataformas de Cisco (con Cisco IOS, Cisco IOS-XE) con las conversiones de CLI equivalentes apropiadas. Este documento no cubre el procedimiento para agregar autorizaciones de origen de ruta (ROA) en los registros regionales de Internet.

Prerequisites

El lector necesita conocer el protocolo BGP.

Descargo

Las direcciones IP de este documento son ejemplos y no deben ser utilizadas en casos reales. Cualquiera de los ejemplos, resultados del comando Display y figuras incluidas en el documento son apenas de carácter ilustrativo. El uso de direcciones IP es de carácter ilustrativo, involuntario y fortuito.

Problemas de BGP debido a un anuncio de prefijo incorrecto

BGP actúa como la columna vertebral del tráfico de Internet. Aunque es el componente más importante del núcleo de Internet, carece de la capacidad de verificar si el anuncio BGP de ingreso se originó desde un sistema autónomo autorizado o no.

Esta limitación de BGP lo convierte en un candidato fácil para diversos tipos de ataques. Un ataque común se denomina "secuestro de ruta". Este ataque se puede utilizar para:

- Robar direcciones IP para enviar spam provoca que se rechace la dirección IP y, por tanto, se deniegue el servicio.
- Espiar el tráfico para obtener información confidencial como contraseñas.
- Interrupciones debidas a configuraciones incorrectas del administrador.
- Impida la entrega de tráfico mediante con hasta servidores falsos garantiza la denegación de servicio.

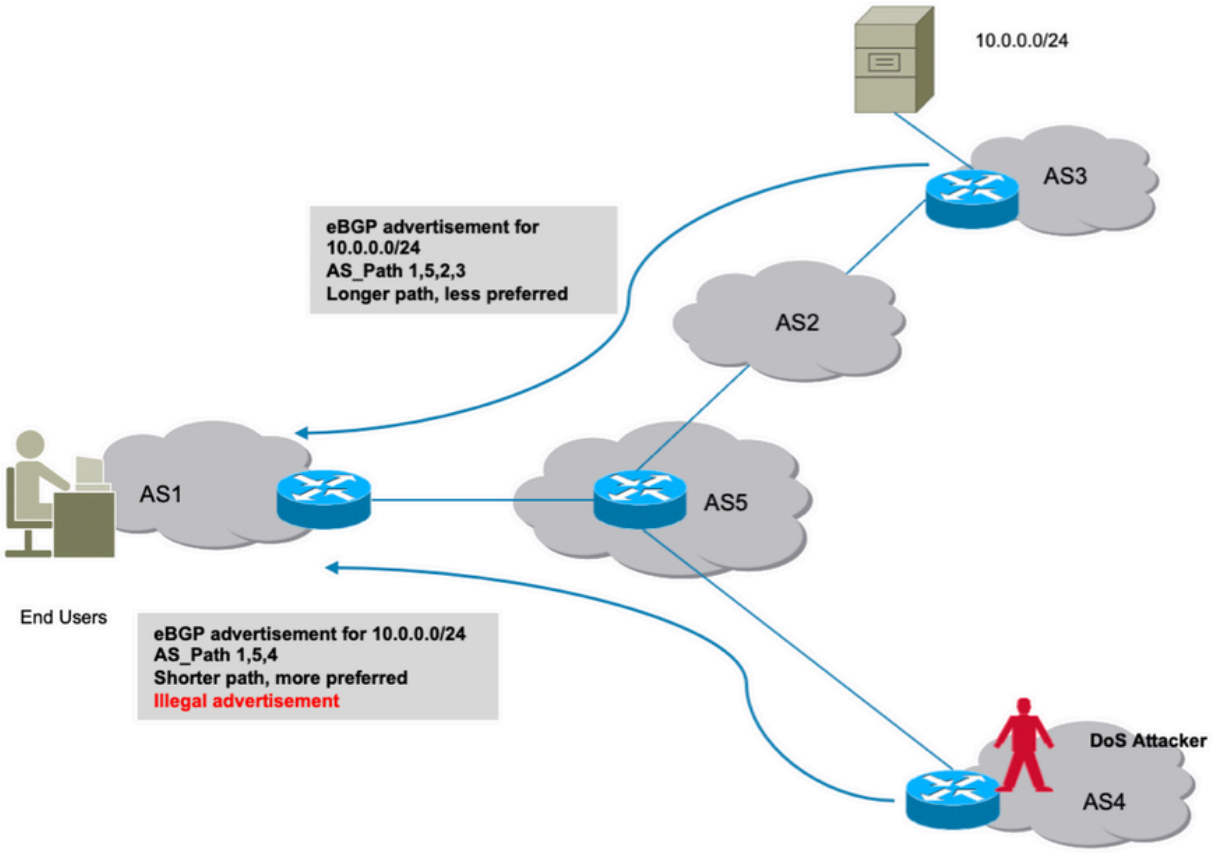
El ataque de denegación de servicio (conocido comúnmente como DoS) es un intento malintencionado de interrumpir el tráfico normal a un router, switch, servidor, etc. Hay una

variedad de ataques de DoS y pocos se discuten aquí.

Secuestro de rutas

Considere el escenario que se muestra aquí. El sistema autónomo 3 (AS3) envía un anuncio BGP legal para su prefijo 10.0.0.0/24. Según el diseño de BGP, nada en BGP impediría que un atacante anunciara el mismo prefijo en Internet.

Como se muestra, el atacante en AS4 anuncia el mismo prefijo 10.0.0.0/24. El algoritmo de mejor trayectoria BGP prefiere una trayectoria con AS_Path más corto. AS_Path 1,5,4 gana sobre el trayecto más largo vía AS 1,5,2,3. Por lo tanto, el tráfico de los clientes ahora se redirigirá al entorno del atacante y puede ser de agujeros negros, lo que se traduce en una denegación de servicio a los clientes finales.

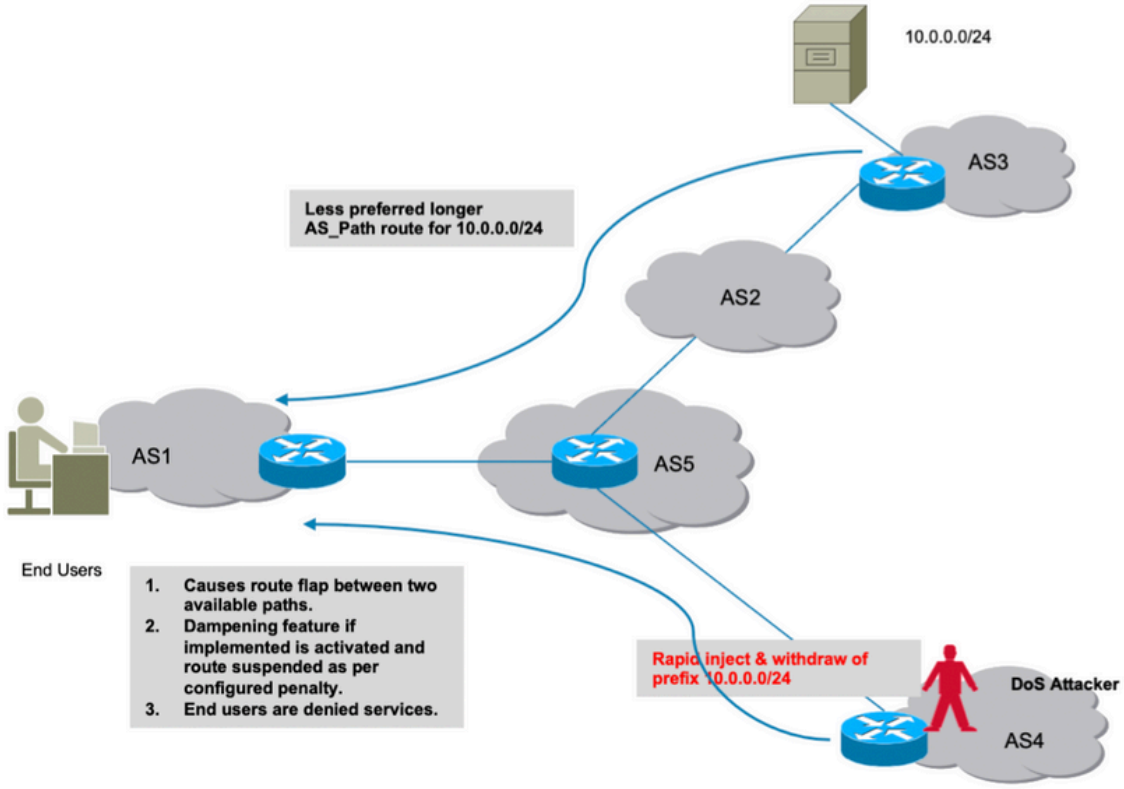


Secuestro de ruta

Degradar el rendimiento del sistema

Esta sección trata sobre otra forma en la que se pueden denegar servicios. Si se configura la función de amortiguación de rutas BGP de Cisco, podría aprovecharse si el atacante introduce inestabilidades de rutas rápidas en la red, lo que provoca una agitación constante.

La función dampening penalizará la ruta legítima y hará que no esté disponible para el tráfico real. Además, este tipo de inestabilidades inducidas de forma no ética causará tensión en los recursos del router, como la CPU, la memoria, etc.

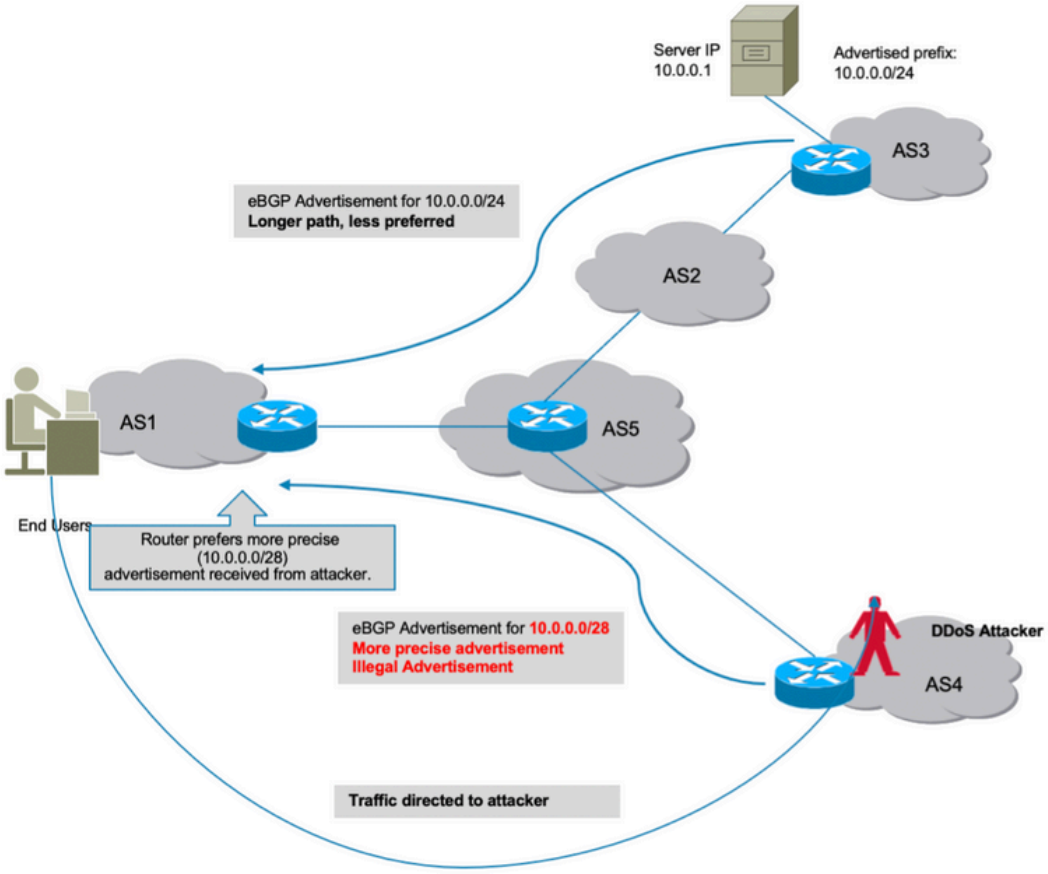


Dampening de ruta

Secuestro de subprefijo

Como se explicó en la sección anterior, cómo un atacante puede originar un prefijo ilegalmente y causar una interrupción del tráfico. Desafortunadamente, una interrupción no es la única causa de preocupación. En tales ataques, los datos reales pueden verse comprometidos en el hecho de que un atacante pueda escanear los datos recibidos para su uso no ético.

Del mismo modo, el secuestro de una ruta podría hacerse mediante la publicidad ilegal de una ruta más precisa. BGP prefiere prefijos que son una coincidencia más larga y este comportamiento puede ser explotado erróneamente como se muestra en la imagen.



Secuestro de subprefijo

Todos los ataques que se discuten se deben al hecho de que BGP no pudo identificar si el AS de origen de estos prefijos maliciosamente anunciados era válido o no. Para solucionar este problema, se necesita una fuente de datos "verdadera" y "fiable" que un router pueda mantener en su base de datos. Luego, cada vez que recibe un nuevo anuncio, el router ahora es capaz de verificar la información de origen AS del prefijo recibida del peer BGP con su información de base de datos local del validador.

Por lo tanto, el router es capaz de distinguir los anuncios buenos de los malos (ilegales) y la capacidad de evitar todos los ataques descritos anteriormente se agregan inherentemente en el router. BGP RPKI proporciona la fuente de confianza de información necesaria.

RPKI

RPKI hace uso de un repositorio que contiene ROAs. Un ROA contiene información sobre el prefijo y su número AS de BGP asociado. La autorización de origen de ruta es una instrucción firmada criptográficamente.

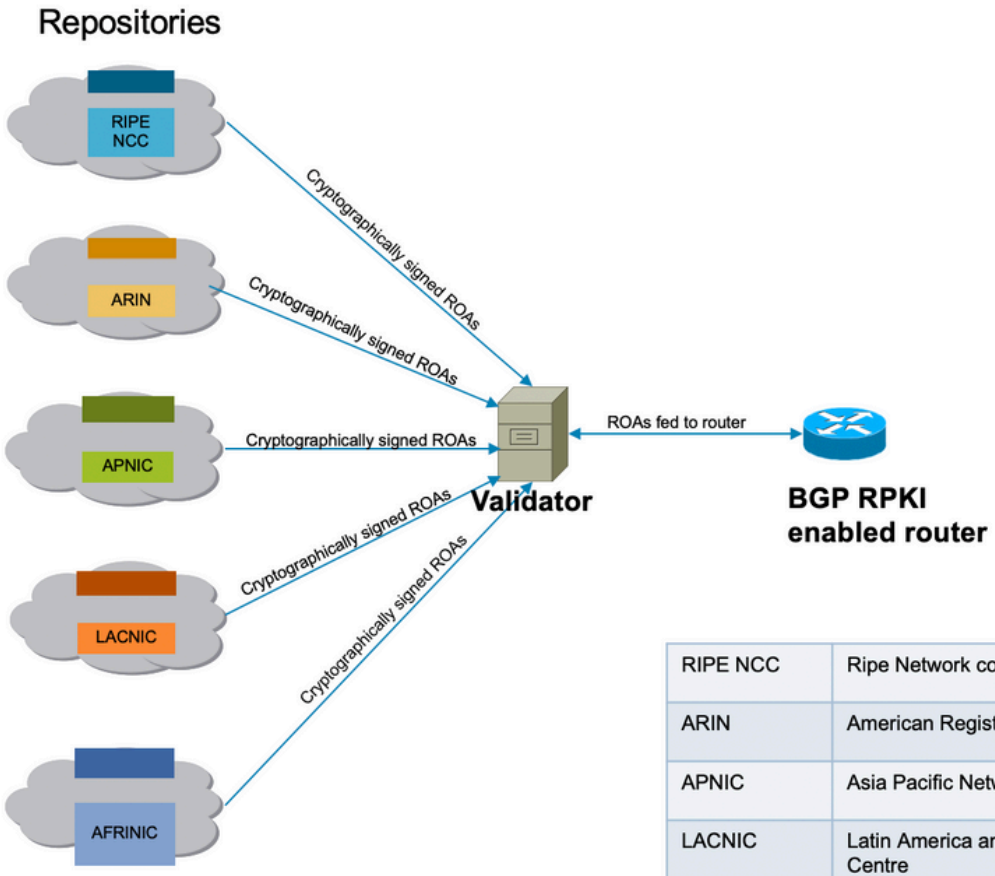
Los cinco registros regionales de Internet (RIR) son los depositarios de confianza de la RPKI. La Autoridad de números asignados de Internet (IANA) es la parte superior del árbol que distribuye los prefijos IP. Los RIR son los siguientes en la jerarquía. Asignan subprefijos a los registros locales de Internet (LIR) y a los grandes proveedores de servicios de Internet (ISP). Firman un certificado para estos prefijos. El siguiente nivel asigna subprefijos de esos y utiliza los certificados de arriba para firmar sus propios certificados para certificar sus propias asignaciones. Normalmente, utilizan sus propios puntos de publicación para alojar los certificados y los ROA.

Cada certificado enumera los puntos de publicación de los certificados secundarios que firma. Por lo tanto, RPKI forma un árbol de certificados que refleja el árbol de asignaciones de direcciones IP. Los validadores de RPKI propiedad de las partes que confían sondean todos los puntos de publicación para encontrar certificados y ROA actualizados (y CRL y manifiestos). Comienzan en los delimitadores de confianza y siguen los vínculos a los puntos de publicación de los certificados secundarios.

Los informes anuales de actividad se introducen en el repositorio mediante informes sobre resultados, pero lo mismo puede hacerse a través de otros registros (nacionales o locales). Esta responsabilidad también puede delegarse a los PSI con la supervisión y verificación adecuadas por parte de los RIR.

En este momento, hay cinco repositorios ROA mantenidos por RIPE NCE, ARIN, APNIC, LACNIC y AFRINIC.

Un validador presente en la red se comunica con estos repositorios y descarga una base de datos ROA de confianza para crear su caché. Se trata de una copia conjunta de la RPKI, que se obtiene/actualiza periódicamente, directa o indirectamente, de la RPKI global. A continuación, el validador envía esta información a los routers permitiéndoles comparar los anuncios BGP entrantes con la tabla RPKI para tomar una decisión segura.



RIPE NCC	Ripe Network coordination center
ARIN	American Registry for Internet Numbers
APNIC	Asia Pacific Network Information Centre
LACNIC	Latin America and Caribbean Network Information Centre
AFRINIC	African Network Information Centre

conectividad de infraestructura RPKI

Validador

Esta demostración utiliza el validador RIPE. El validador se comunicará con el router mediante el

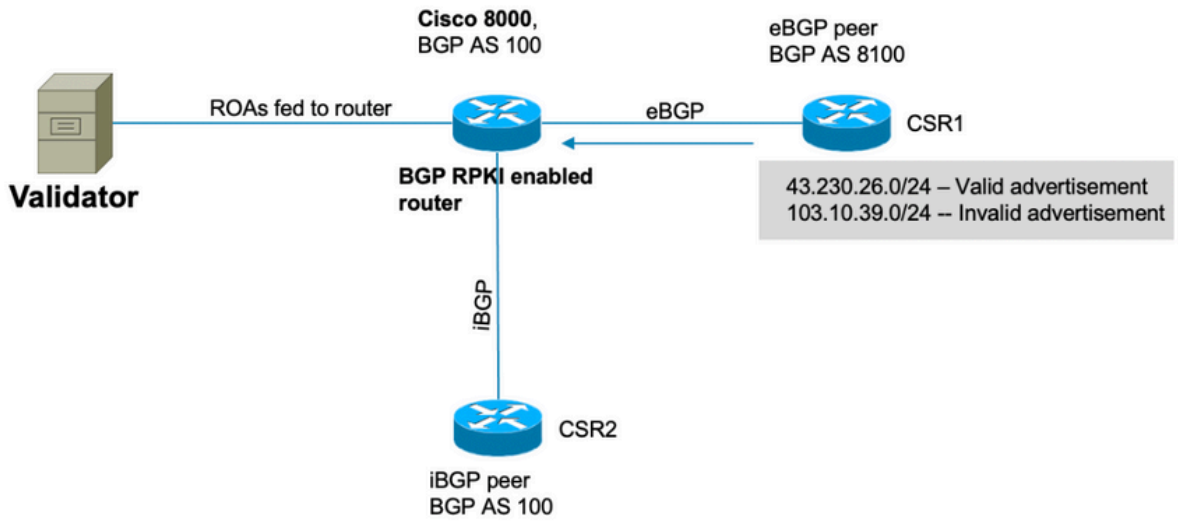
establecimiento de una sesión TCP. En esta demostración, el validador escucha en su IP 192.168.122.120 y en el puerto 3323.

```
routinator server --rtr 192.168.122.120:3323 --refresh=900
```

IANA ha especificado el puerto 3323 para esta comunicación. El temporizador de actualización define el intervalo de tiempo tras el cual el repositorio local se sincronizará y actualizará para mantenerse actualizado.

Demostración de BGP RPKI

Topología



Topología

> **Nota**: Esta demostración utiliza números y prefijos AS públicos aleatorios simplemente para explicar la mecánica BGP RPKI. Las IP públicas se utilizan debido a la RPKI principalmente para la protección de prefijos públicos y todas las ROA creadas en los RIR son prefijos públicos. Por último, ninguna de las acciones, configuraciones, etc. descritas en este documento afecta a estas IP públicas y AS de ninguna manera.

Configurar

```
router bgp 100

bgp router-id 10.1.1.1

rpki server 192.168.122.120

transport tcp port 3323
```

```
 refresh-time 900



address-family ipv4 unicast
 !
 neighbor 10.0.12.2
 remote-as 8100
 address-family ipv4 unicast
  route-policy Pass in
  route-policy Pass out
 !
 !
 neighbor 10.0.13.3
 remote-as 100
 address-family ipv4 unicast
 !
 !
// 'Pass' is a permit all route-policy.
```

Sesión BGP RPKI

El router establece una sesión TCP con un validador (IP: 192.168.122.120, puerto 3323) para descargar la memoria caché ROA a la memoria del router.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server 192.168.122.120
Wed Jan 20 22:54:15.763 UTC

RPKI Cache-Server 192.168.122.120
 Transport: TCP port 3323
 Bind source: (not configured)
 Connect state: ESTAB
 Conn attempts: 1
 Total byte RX: 4428792
 Total byte TX: 1400
 Last reset
```

```
   Timest: Jan 20 05:59:58 (16:54:17 ago)

   Reason: protocol error
```

Descargas de ROA en el router

El validador envía la información de ROA al router. Esta memoria caché se actualiza a intervalos periódicos para minimizar la posibilidad de que el router contenga información obsoleta. En esta demostración, se ha configurado un tiempo de actualización de 900 segundos. Como se muestra aquí, el router Cisco 8000 ha descargado 172632 ROA IPv4 y 28350 ROA IPv6 del validador.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Wed Jan 20 23:01:59.432 UTC


Hostname/Address        Transport       State           Time                ROAs (IPv4/IPv6)

192.168.122.120         TCP:3323        ESTAB           17:00:21        172632/28350

RP/0/RP0/CPU0:Cisco8000#show bgp rpki table ipv4

Wed Jan 20 23:09:26.899 UTC

>>>Snipped output<<<

 Network               Maxlen      Origin-AS         Server

 10.0.0.0/24            24              13335             192.168.122.120

 10.0.4.0/22            22              38803             192.168.122.120

 10.0.4.0/24            24              38803             192.168.122.120

 10.0.5.0/24            24              38803             192.168.122.120

 10.0.6.0/24            24              38803             192.168.122.120

 10.0.7.0/24            24              38803             192.168.122.120

 10.1.1.0/24            24              13335             192.168.122.120

 10.1.4.0/22            22              4134              192.168.122.120

 10.1.16.0/20           20              4134              192.168.122.120

 10.2.9.0/24            24              4134              192.168.122.120

 10.2.10.0/24           24              4134              192.168.122.120

 10.2.11.0/24           24              4134              192.168.122.120

 10.2.12.0/22           22              4134              192.168.122.120

 10.3.0.0/16            16              4134              192.168.122.120

 10.6.0.0/22            24              9583              192.168.122.120
```

Verificación

Esta sección demuestra cómo BGP RPKI está en acción y cómo evita que el router emita anuncios incorrectos/ilegales.

Habilitación de la Validez Origin-As

De forma predeterminada, el router obtiene los ROA del validador, pero no comienza a usarlos hasta que se configura para ello. Como resultado, estos prefijos se marcan como "D" o se desactivan.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Wed Jan 20 23:27:37.268 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 30

BGP main routing table version 30

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs


Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

D*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

D*> 203.0.113.1/24     10.0.12.2                0             0 8100 ?

D*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Para habilitar el router para la verificación de validez como origen, active este comando para la familia de direcciones correspondiente.

```
router bgp 100

 address-family ipv4 unicast
```

```
 bgp origin-as validation enable

 !
```

Cuando activa este comando, hace que el router escanee los prefijos presentes en su tabla BGP contra la información ROA recibida del validador y uno de los tres estados se asigna a los prefijos .

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 00:04:58.136 UTC

Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

V*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

I*  203.0.113.1/24     10.0.12.2                0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Para permitir que el router utilice la información de estado de validación de prefijo mientras realiza el cálculo de la mejor trayectoria, se necesita este comando. Esta opción no está habilitada de forma predeterminada, ya que le ofrece la opción de no utilizar la información de validez para el cálculo de la mejor ruta, pero le permite utilizarla en las políticas de ruta que se describen más adelante en este documento.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

Estados de validez de prefijo

Hay tres estados en los que se puede encontrar un prefijo.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 00:04:58.136 UTC



Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

V*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

I*  203.0.113.1/24     10.0.12.2                0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

- No válido: indica que el prefijo cumple cualquiera de estas dos condiciones: 1. Coincide con una o más **Autorizaciones de Origen de Ruta** (ROA), pero no hay coincidencia de ROA donde el AS de origen coincide con el AS de origen en AS-PATH. 2. Coincide con uno o más ROA en la longitud mínima especificada en el ROA, pero para todos los ROA en los que coincide con la longitud mínima, es más largo que la longitud máxima especificada. El AS de origen no importa para la condición #2.
- Válido - Indica que el prefijo y el par AS se encuentran en la tabla de memoria caché RPKI.
- No encontrado: indica que el prefijo no se encuentra entre los prefijos válidos o no válidos.

Esta sección trata cada prefijo y su estado en detalle.

1. 203.0.113.0/24 - Válido

El peer eBGP en AS 8100 originó esta ruta y se anunció al nodo Cisco 8000. Dado que el AS de origen (8100) coincide con el AS de origen en ROA (recibido del validador), este prefijo se marca como válido y se instala en la tabla de routing del router.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki table | in "203.0.113.0|Max"

Thu Jan 21 00:21:26.026 UTC

 Network               Maxlen          Origin-AS         Server

 203.0.113.0/24              24       8100              192.168.122.120
```

La ruta se instala en la tabla BGP.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.0/24

Thu Jan 21 05:30:13.858 UTC

BGP routing table entry for 203.0.113.0/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                31          31

Last Modified: Jan 21 00:03:33.344 for 05:26:40

Paths: (1 available, best #1)

 Not advertised to any peer

 Path #1: Received by speaker 0
```

```
 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best

     Received Path ID 0, Local Path ID 1, version 31

     Origin-AS validity: valid
```

Dado que este es el mejor prefijo BGP y también es válido por RPKI, se instala correctamente en la tabla de ruteo.

```
RP/0/RP0/CPU0:Cisco8000#show route 203.0.113.0/24

Thu Jan 21 00:29:43.667 UTC



Routing entry for 203.0.113.0/24

 Known via "bgp 100", distance 20, metric 0

 Tag 8100, type external

 Installed Jan 21 00:03:33.731 for 00:26:10

 Routing Descriptor Blocks

   10.0.12.2, from 10.0.12.2, BGP external

     Route metric is 0

 No advertising protos.
```

2. 203.0.113.1/24 - No válido

Este prefijo no es válido porque hay un conflicto en la información de AS de origen contenida en ROA y la información de origen-as recibida a través del mensaje BGP del peer eBGP. 203.0.113.1/24 se recibe vía BGP con origen AS 8100.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity invalid

Thu Jan 21 00:34:38.171 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 33

BGP main routing table version 33
```

```
BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs


Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop            Metric LocPrf Weight Path

*  203.0.113.1/24     10.0.12.2                0             0 8100 ?
```

Sin embargo, el ROA recibido del validador muestra que este prefijo pertenece a AS 10021.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki table 203.0.113.1/24 max 24

Thu Jan 21 00:37:05.615 UTC


RPKI ROA entry for 203.0.113.1/24-24

 Origin-AS: 10021 from 192.168.122.120

Version: 124211
```

Dado que la información de origen de AS en el anuncio de BGP recibido (AS 8100) no coincide con el origen de AS real recibido en ROA (AS 10021), el prefijo se marca como no válido y no se instala en la tabla de ruteo.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24

Thu Jan 21 05:37:26.714 UTC

BGP routing table entry for 203.0.113.1/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 32          32

Last Modified: Jan 21 00:03:33.344 for 05:33:53

Paths: (1 available, no best path)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external
```

```
     Received Path ID 0, Local Path ID 0, version 0

     Origin-AS validity: invalid
```

3. 192.168.122.1/32 No se encontró

Este es un prefijo privado y no está presente en la memoria caché ROA. BGP declaró este prefijo como "No encontrado".

```
RP/0/RP0/CPU0:Cisco8000#show bgp 192.168.122.1/32

Thu Jan 21 05:44:39.861 UTC

BGP routing table entry for 192.168.122.1/32

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 33          33

Last Modified: Jan 21 00:03:33.344 for 05:41:06

Paths: (1 available, best #1)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best

     Received Path ID 0, Local Path ID 1, version 33

     Origin-AS validity: not-found
```

Dado que RPKI aún se adopta, los prefijos 'no encontrados' se instalan en la tabla de ruteo. De lo contrario, BGP ignorará estos prefijos legítimos que no están registrados en la base de datos RPKI.

Permitir prefijo no válido

Aunque no se recomienda, el software proporciona un botón para permitir que los prefijos no válidos participen en el algoritmo de cálculo de la mejor trayectoria.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as allow invalid

 !
```

Con esta configuración, el router no considera los prefijos no válidos para el cálculo de la mejor trayectoria mientras que esto está marcado como "no válido". Este resultado muestra ‘203.0.113.1/24’ marcado como la mejor trayectoria.

```
RP/0/RP0/CPU0:Cisco8000#show bgp

Thu Jan 21 06:21:34.294 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 34

BGP main routing table version 34

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs



Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop            Metric LocPrf Weight Path

*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

*> 203.0.113.1/24     10.0.12.2                0             0 8100 ?

*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Como se muestra en esta salida, el prefijo se marca como el mejor a pesar de que se mantiene inválido.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24

Thu Jan 21 06:23:26.994 UTC

BGP routing table entry for 203.0.113.1/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 34          34

Last Modified: Jan 21 06:05:31.344 for 00:17:55

Paths: (1 available, best #1)
```

```
 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best

     Received Path ID 0, Local Path ID 1, version 34

     Origin-AS validity: invalid
```

Cabe señalar que un router sigue tratando el prefijo no válido como la última opción y siempre prefiere un prefijo válido sobre un prefijo no válido si está disponible.

Configuración manual de ROA en el router

Si por alguna razón, un ROA para un prefijo determinado aún no se crea, recibe o se retrasa, se podría configurar un ROA manual en el router. Por ejemplo, el prefijo "192.168.122.1/32" se marca como "No encontrado", como se muestra aquí.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 06:36:31.041 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 34

BGP main routing table version 34

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs



Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path
```

```
V*> 203.0.113.0/24     10.0.12.2               0             0 8100 ?

I*> 203.0.113.1/24     10.0.12.2               0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2               0             0 8100 ?
```

Se puede configurar un ROA manual como se muestra aquí. Este comando asocia el prefijo '192.168.122.1/32' con AS 8100.

```
router bgp 100

 rpki route 192.168.122.1/32 max 32 origin 8100
```

Con esta configuración, el estado del prefijo cambia de 'N' a 'V'.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 06:36:34.151 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 35

BGP main routing table version 35

BGP NSR Initial initsync version 2 (Reached)



Status codes: s suppressed, d damped, h history, * valid, > best

              i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

   Network            Next Hop            Metric LocPrf Weight Path

V*> 203.0.113.0/24     10.0.12.2               0             0 8100 ?

I*> 203.0.113.1/24     10.0.12.2               0             0 8100 ?

V*> 192.168.122.1/32   10.0.12.2               0             0 8100 ?
```

Estado de validación de políticas de ruta y prefijos

El resultado del estado del prefijo se puede utilizar para crear políticas de ruta. Estos estados se pueden utilizar en una sentencia match y se pueden realizar las acciones deseadas por el administrador. Este ejemplo hace coincidir todos los prefijos con un estado no válido y establece un valor de peso de 12345 para ellos.

```
route-policy Invalid
 if validation-state is invalid then
   set weight 12345
 endif
end-policy
!



router bgp 100
 remote-as 8100
 address-family ipv4 unicast
  route-policy Invalid in
 !
 !
!
```

Este resultado muestra un peso aplicado de prefijo no válido de 12345.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24
Thu Jan 21 06:57:33.816 UTC
BGP routing table entry for 203.0.113.1/24
Versions:
 Process           bRIB/RIB  SendTblVer
 Speaker                 38          38
Last Modified: Jan 21 06:54:04.344 for 00:03:29
Paths: (1 available, best #1)
 Not advertised to any peer
 Path #1: Received by speaker 0
 Not advertised to any peer
 8100
   10.0.12.2 from 10.0.12.2 (192.168.122.105)
     Origin incomplete, metric 0, localpref 100, weight 12345, valid, external, best, group-best
     Received Path ID 0, Local Path ID 1, version 38
     Origin-AS validity: invalid
```

Compartir información de validación de prefijos a través de una comunidad ampliada

Como router BGP también puede compartir el estado de validación de prefijo con otros routers (sin caché local del validador) a través de la comunidad ampliada BGP. Esto ahorra la sobrecarga de todos y cada uno de los routers de la red con una sesión con el validador y la descarga de todas las ROA.

Esto es posible gracias a la comunidad extendida BGP.

Este comando permite que el router comparta la información de 'validación de prefijo' con los peers iBGP.

```
router bgp 100

 address-family ipv4 unicast

 bgp origin-as validation signal ibgp
```

Una vez que el router Cisco 8000 se configura como se muestra, las actualizaciones de BGP a los peers incluyen información de validación de prefijos. En este caso, el router iBGP vecino es un router IOS-XE.

```
csr2#show ip bgp 203.0.113.1/24

BGP routing table entry for 203.0.113.1/24, version 14

Paths: (1 available, best #1, table default)

 Not advertised to any peer

 Refresh Epoch 1

 8100

   10.0.12.2 from 10.0.13.1 (10.1.1.1)

     Origin IGP, metric 0, localpref 100, valid, internal, best

     Extended Community: 0x4300:0:2

     rx pathid: 0, tx pathid: 0x0

     Updated on Jan 21 2021 18:16:56 UTC
```

Esta asignación de comunidad ampliada se puede entender con el uso de 0x4300 0x0000 (4 bytes que indican el estado).

Los cuatro bytes que indican el estado se tratan como un entero sin signo de 32 bits que tiene uno de los valores:

- 0 - Válido
- 1 - No encontrado
- 2 - No válido

La comunidad del prefijo 203.0.113.1/24 es 0x4300:0:2, que se asigna al prefijo "no válido". De esta manera, el router csr2 a pesar de no tener su propia memoria caché local, aún puede tomar

decisiones basadas en el estado de validación de prefijo.

El estado de validación de prefijo ahora se puede utilizar para coincidir en un route-map o en el algoritmo de mejor trayectoria BGP.

Recomendaciones para la Implementación de BGP RPKI

Buenas prácticas para la creación de ROA

Estas son algunas recomendaciones basadas en redes inalcanzables observadas en RPKI-Observatorio. El Observatorio de la RPKI analiza múltiples aspectos del panorama de la RPKI desplegada.

- Si se crea un ROA para cualquier prefijo, se recomienda anunciar ese prefijo en BGP. En ausencia de ella, otra persona puede anunciarla simplemente fingiendo ser un ASN contenido en ese ROA y utilizar el prefijo.
- Si se crea ROA con una longitud máxima mayor que la longitud del prefijo, entonces es equivalente a crear ROA para todos los prefijos posibles bajo el prefijo original hasta la longitud máxima. Se recomienda encarecidamente anunciar todos esos prefijos en BGP.
- Si se crea un ROA para un prefijo y el propietario del prefijo anuncia un subprefijo del prefijo original, el ROA invalidará ese subprefijo. Un ROA para el subprefijo así como el maxlen del ROA original debe ser extendido para cubrir el subprefijo.
- Si una organización posee un prefijo, pero planea no anunciarlo en BGP, se debe crear un ROA para el prefijo para AS0. Esto invalidará cualquier anuncio de prefijo porque AS0 no puede aparecer en ninguna trayectoria de AS.
- Si hay varios ASN que originan el mismo prefijo, se deben crear los ROA para ese prefijo para cada ASN. Por lo tanto, si un router tiene varios ROA para el mismo prefijo, un anuncio de BGP que coincida con cualquiera de ellos será válido. Varios ROA para el mismo prefijo no entran en conflicto entre sí.
- Si "A" está originando un prefijo para su cliente "B" y crea un ROA para ese prefijo en nombre de "B", entonces "A" debe anteponer el ASN de "B" al anuncio o hacer que "B" origine el prefijo en sí.

Impacto en el rendimiento de RPKI en routers XR BGP

Efecto de la actualización de ROA en la CPU con política de rutas

Cuando se actualizan los ROA y si el router tiene una política de ruta de ingreso local para un vecino que contiene un "estado de validación es", entonces es importante volver a validar el estado de los prefijos en función de los nuevos ROA actualizados. Esto se logra mediante el envío por parte del router de una solicitud BGP REFRESH a su par.

Cuando los vecinos BGP reciben este mensaje como se muestra, los vecinos envían sus prefijos nuevamente y la política de ruta entrante puede revalidar los prefijos entrantes .

```
Jan 22 18:28:41.360: BGP: 10.0.12.1 rcv message type 5, length (excl. header) 4
```

```
Jan 22 18:28:41.360: BGP: 10.0.12.1 rcvd REFRESH_REQ for afi/safi: 1/1, refresh code is 0
```
El problema se amplifica cuando muchos vecinos se actualizan al mismo tiempo cada vez que se actualizan los ROA. Si la política de ruta entrante del vecino es compleja y requiere mucho procesamiento, los resultados de CPU altos durante unos minutos después de una actualización de ROA. Estos mensajes REFRESH no ocurren si la política de ruta entrante del vecino no contiene un comando "validation-state is".

Si se configura "soft-reconfiguration inbound always" para un vecino, no se enviarán mensajes BGP REFRESH, pero las mismas políticas de ruta se seguirán ejecutando a la misma velocidad y se puede esperar el mismo uso de CPU.

Se recomienda preferir el enfoque "bgp bestpath origin-as use validation" en lugar de configurar una política de ruta por las razones explicadas en 6.2.2 a continuación.

Minimizar el impacto en la CPU causado por la actualización de ROA

La mejor manera de evitar el problema explicado aquí es utilizar **bestpath origin-as use validation** sin **validation-state is** en la política.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```
Este comando mantiene una ruta recibida no válida en el router pero evita que se convierta en una mejor trayectoria. No se instalará ni se anunciará. Es tan bueno como dejarlo caer. Si con la siguiente actualización de ROA pasa a ser válida, no se requiere NINGUNA ACTUALIZACIÓN y pasará a ser elegible automáticamente para la mejor ruta sin necesidad de ejecutar ninguna política.

Si el usuario prefiere permitir prefijos "no válidos" y no utilizarlos, además de la **validez de uso de bestpath origin-as**, utilice la configuración **best path origin-as allow invalid**.

En este caso, cuando cambia un ROA, la mejor trayectoria se actualiza automáticamente sin requerir un mensaje REFRESH. Para anular la preferencia, una ruta significa que durante la selección de la ruta BGP la trayectoria RPKI inválida se considera menos preferible que cualquier otra trayectoria al mismo destino. Es similar a asignarle un peso o una preferencia local menor que 0.

El número de inválidos de la RPKI es relativamente pequeño y su mantenimiento en el cuadro no tiene un impacto significativo en los recursos.

> **Nota**: Para utilizar "bestpath origin-as use validation", todas las trayectorias de una ruta, incluidas las trayectorias IBGP, deben tener la validez RPKI correcta. Si no es así, se puede seguir utilizando la prueba del estado de validación en la política de rutas.

El router no valida las rutas IBGP en la base de datos ROA. Las rutas IBGP obtienen una validez RPKI de la comunidad ampliada RPKI. Si la ruta IBGP se recibe sin esta comunidad ampliada, su

estado de validación se establece en not-found.

Espacio de Memoria BGP RPKI

Cada ROA consume memoria para el índice y los datos. Si dos ROA son para el mismo prefijo IP, pero tienen max_len diferente o se reciben de servidores RPKI diferentes, comparten el mismo índice pero tienen datos separados. Los requisitos de memoria pueden variar porque la sobrecarga de memoria no es constante. Se recomienda un 10% de sobrepresupuesto. Las plataformas de 64 bits requieren más memoria para cada objeto de memoria que las plataformas de 32 bits. El uso de memoria IOS-XR en bytes para un objeto de índice y un objeto de datos está en la tabla. Algunos gastos generales constantes se incluyen en los números.

	Plataforma de 32 bits (bytes)	Plataforma de 64 bits (bytes)
Índice IPv4	74	111
índice IPv6	86	125
datos	34	53

Esta sección toma dos escenarios para explicar cómo los ROA consumen memoria.

Escenario 1. Tres servidores RPKI configurados en el router

Considere un router que utilice 3 servidores RPKI, cada uno de los cuales proporciona 200 000 ROA IPv4 y 20 000 ROA IPv6 en un procesador de routing de 64 bits que requerirá esta memoria:

20000 * (125 + 3*53) + 200000 * (111 + 3*53) bytes = 59,68 millones de bytes

Mientras se calculaba la memoria, el ROA para el mismo prefijo de tres validadores diferentes compartía el mismo valor de índice.

Situación hipotética 2. Servidores RPKI únicos configurados en el router

Memoria de proceso BGP sin ROA:

```
RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:19:57.945 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot
 Process

1069           2M        71M       132K        25M      7447M        50M        74M        bgp


RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:12:09.073 UTC

Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)
```

```
192.168.122.120     TCP:3323      NONE          00:00:25      N/A
```

Se observa que el proceso BGP consume 25 MB de memoria sin ningún ROA.

Memoria de proceso BGP con ROA:

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:23:46.769 UTC

Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)

192.168.122.120     TCP:3323      ESTAB         00:02:42      172796/28411

RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:24:14.659 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot     Process

1069          2M        99M       132K        53M      7447M        50M       102M       bgp
```

Se observa que el proceso BGP consume 25 MB de memoria sin ningún ROA.

Memoria de proceso BGP con ROA:

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:23:46.769 UTC

Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)

192.168.122.120     TCP:3323      ESTAB         00:02:42      172796/28411

RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:24:14.659 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot     Process

1069          2M        99M       132K        53M      7447M        50M       102M       bgp
```


El router Cisco 8000 ejecuta un sistema operativo de 64 bits. Recibió 172796 ROA IPv4 y 28411 ROA.

Memoria (bytes) = 172 796 x [111 (índice) + 53 (datos)] + 28411 x [125 (índice) + 53 (datos)].

Estos cálculos proporcionan ~27 MB, que es aproximadamente el incremento observado en la memoria del router.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).