Whitepaper: BGP RPKI mit XR7 Cisco8000

Inhalt

Einleitung
Hintergrundinformationen
Vorwort
Umfang
Voraussetzungen
Haftungsausschluss
BGP-Probleme aufgrund von schlechter Präfix-Ankündigung
Route Hijacking
Beeinträchtigung der Systemleistung
Hijacking mit Sub-Präfix
RPKI
Validator
BGP-RPKI-Demonstration
Topologie
Konfigurieren
BGP-RPKI-Sitzung
ROA-Downloads auf Router
Überprüfung
Aktivieren von Origin-as-Validität
Präfix-Gültigkeitsstatus
1. 203.0.113.0/24 - Gültig
2. 203.0.113.1/24 - Ungültig
3. 192.168.122.1/32 Nicht gefunden
Ungültiges Präfix zulassen
Manuelle ROA-Konfiguration auf Router
Validierungsstatus für Route Policy und Präfix
Weitergabe von Präfixvalidierungsinformationen über die erweiterte Community
Empfehlungen für die BGP RPKI-Implementierung
Best Practices für die ROA-Erstellung
Leistungsauswirkung von RPKI auf XR-BGP-Routern
Auswirkung der ROA-Aktualisierung auf die CPU mit Routen-Richtlinie
Minimierung der durch ROA-Update verursachten CPU-Auswirkungen
BGP-RPKI-Speicherbedarf
Szenario 1. Drei auf Router konfigurierte RPKI-Server
Szenario 2. Auf Router konfigurierte einzelne RPKI-Server

Einleitung

In diesem Dokument wird die Border Gateway Protocol (BGP) Resource Public Key Infrastructure (RPKI)-Funktion auf der Cisco IOS® XR-Plattform beschrieben.

Hintergrundinformationen

Vorwort

In diesem Dokument wird die BGP-RPKI-Funktion und der Schutz des BGP mit Routern vor falschen/bösartigen BGP-Präfix-Updates beschrieben.

Umfang

In diesem Dokument wird zu Demonstrationszwecken Cisco 8000 mit XR 7.3.1 verwendet. BGP RPKI ist jedoch eine plattformunabhängige Funktion. Die in diesem Dokument behandelten Konzepte gelten für andere Cisco Plattformen (mit Cisco IOS, Cisco IOS-XE usw.) mit entsprechenden äquivalenten CLI-Konvertierungen. In diesem Dokument wird nicht auf das Verfahren eingegangen, Route Origin Authorizations (ROAs) in regionale Internet-Register aufzunehmen.

Voraussetzungen

Der Leser benötigt Kenntnisse über das BGP-Protokoll.

Haftungsausschluss

Bei den in diesem Dokument verwendeten IP-Adressen handelt es sich nicht um tatsächlich existierende Adressen. Alle im Dokument enthaltenen Beispiele, Befehlsausgaben und Abbildungen dienen lediglich der Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

BGP-Probleme aufgrund von schlechter Präfix-Ankündigung

Das BGP fungiert als Backbone des Internetdatenverkehrs. Obwohl es sich hierbei um die wichtigste Komponente des Internet-Core handelt, kann nicht überprüft werden, ob die BGP-Eingangsankündigung von einem autorisierten autonomen System stammt.

Diese Einschränkung von BGP macht es zu einem einfachen Kandidaten für verschiedene Arten von Angriffen. Ein häufiger Angriff wird als "Route Hijack" bezeichnet. Dieser Angriff kann genutzt werden, um:

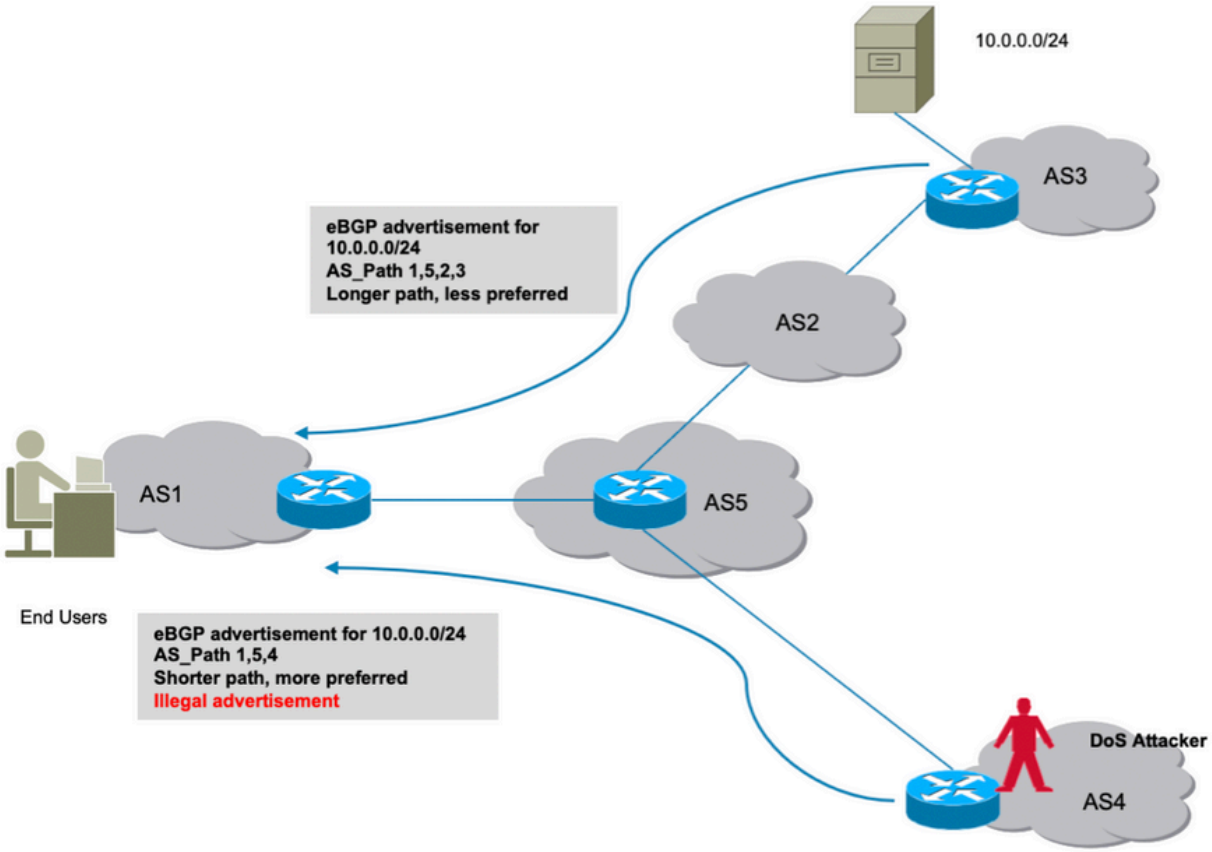
- Diebstahl von IPs, um Spam-Ergebnisse in IP zu senden, wird abgelehnt und damit Denial-of-Service.
- Datenverkehr ausspionieren, um vertrauliche Informationen wie Kennwörter zu erhalten.
- Störungen aufgrund falscher Konfigurationen durch den Administrator.
- Durch die Aktivierung gefälschter Server wird die Bereitstellung von Datenverkehr durch Denial-of-Service verhindert.

Denial-of-Service-Angriffe (gemeinhin als DoS bekannt) sind ein böswilliger Versuch, den normalen Datenverkehr zu einem Router, Switch, Server usw. zu unterbrechen. Es gibt verschiedene DoS-Angriffe, von denen hier nur wenige behandelt werden.

Route Hijacking

Betrachten wir das hier gezeigte Szenario. Autonomous System 3 (AS3) sendet eine zulässige BGP-Benachrichtigung für das Präfix 10.0.0.0/24. Das BGP-Design sieht keine Einschränkung vor, die einen Angreifer daran hindern würde, dasselbe Präfix an das Internet weiterzugeben.

Wie gezeigt, kündigt der Angreifer in AS4 dasselbe Präfix 10.0.0.0/24 an. Der BGP-Algorithmus für den besten Pfad bevorzugt einen Pfad mit dem kürzeren AS_Path. AS_Path 1,5,4 gewinnt über AS 1,5,2,3 über einen längeren Pfad. Aus diesem Grund wird der Datenverkehr von den Clients nun an die Umgebung des Angreifers umgeleitet und kann als Blackholing ausgeführt werden, was zu einer Diensteverweigerung für Endkunden führt.

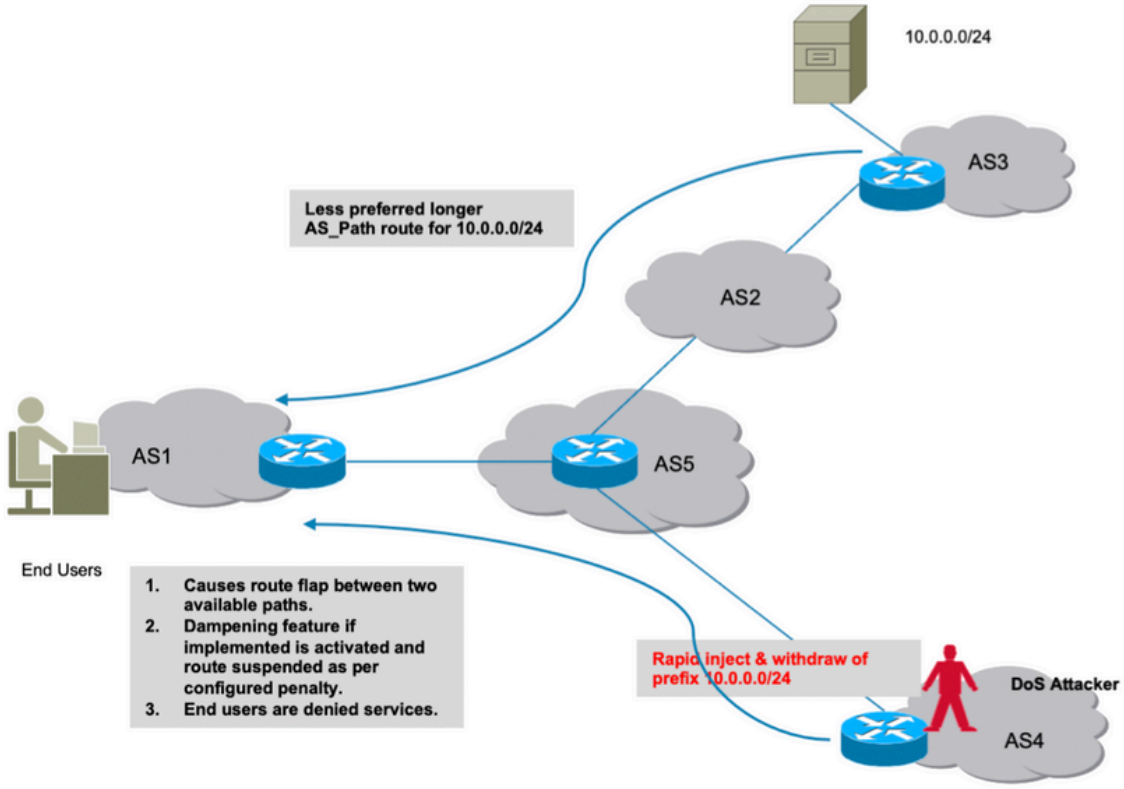


Route Hijack

Beeinträchtigung der Systemleistung

In diesem Abschnitt wird eine andere Möglichkeit beschrieben, Services abzulehnen. Wenn die BGP-Routen-Dampening-Funktion von Cisco konfiguriert ist, könnte sie ausgenutzt werden, wenn der Angreifer schnelle Routen-Flaps in das Netzwerk einführt, die eine konstante Abwanderung verursachen.

Durch die Dämpfung wird die zulässige Strecke bestraft, sodass sie für den tatsächlichen Verkehr nicht mehr verfügbar ist. Außerdem führen diese unethisch bedingten Flaps zu einer Belastung der Router-Ressourcen wie CPU, Arbeitsspeicher usw.

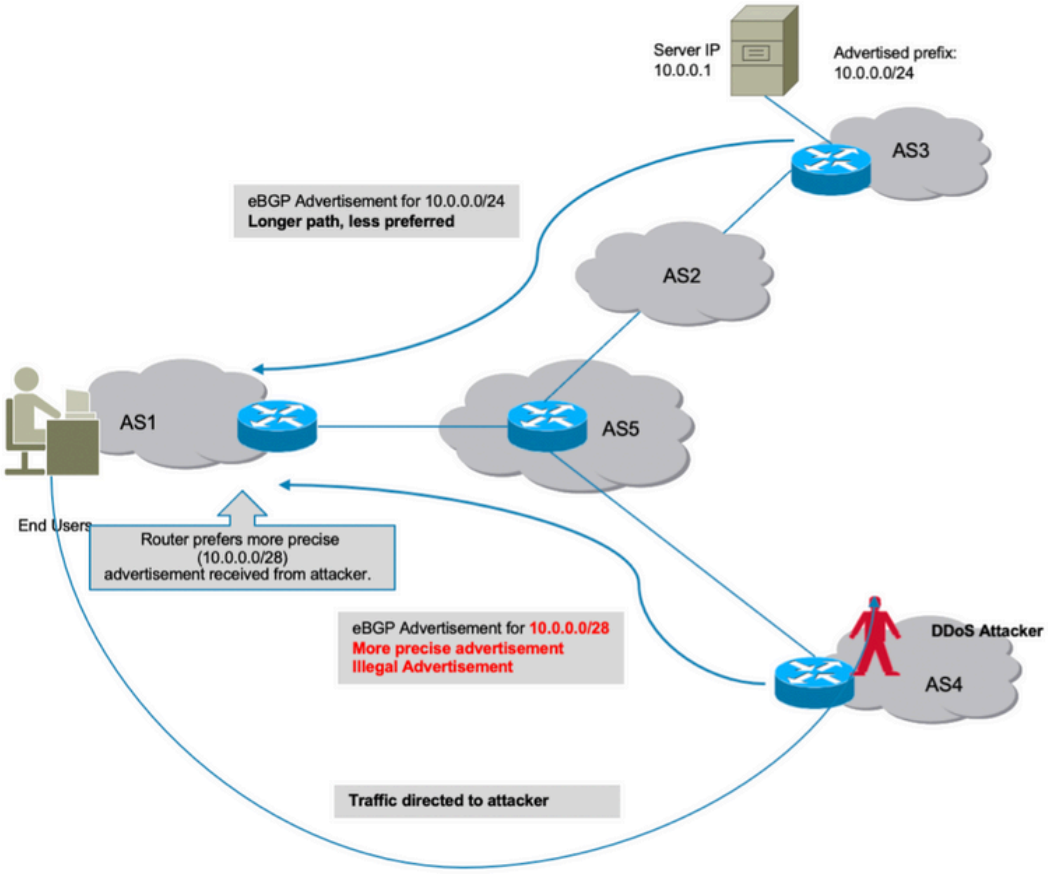


Streckendämpfung

Hijacking mit Sub-Präfix

Wie im vorherigen Abschnitt erläutert, kann ein Angreifer ein Präfix illegal generieren und eine Unterbrechung des Datenverkehrs verursachen. Leider ist eine Störung nicht der einzige Grund zur Sorge. Bei solchen Angriffen können die tatsächlichen Daten kompromittiert werden, indem ein Angreifer empfangene Daten für unethische Zwecke scannen kann.

Ebenso könnte die Entführung einer Route durch illegale Werbung für eine präzisere Route erfolgen. BGP bevorzugt Präfixe, die länger übereinstimmen, und dieses Verhalten kann falsch ausgenutzt werden, wie im Bild gezeigt.



Hijack mit Sub-Präfix

Alle hier behandelten Angriffe beruhen auf der Tatsache, dass das BGP nicht erkennen konnte, ob das Ursprungs-AS dieser böswillig angekündigten Präfixe gültig war. Um dieses Problem zu beheben, ist eine echte und vertrauenswürdige Datenquelle erforderlich, die der Router in seiner Datenbank speichern kann. Nach jedem Empfang einer neuen Benachrichtigung ist der Router nun in der Lage, die vom BGP-Peer empfangenen AS-Ursprungsinformationen des Präfix mit den lokalen Datenbankinformationen des Validators zu vergleichen.

So ist der Router in der Lage, die gute Werbung von der schlechten (illegale) Werbung zu unterscheiden und die Fähigkeit, alle Angriffe zu vermeiden, die zuvor diskutiert wurden, werden automatisch auf dem Router hinzugefügt. BGP-RPKI stellt die erforderliche vertrauenswürdige Informationsquelle dar.

RPKI

RPKI nutzt ein Repository, das ROAs enthält. Ein ROA enthält Informationen über das Präfix und die zugehörige BGP-AS-Nummer. Route Origination Authorization ist eine kryptographisch signierte Anweisung.

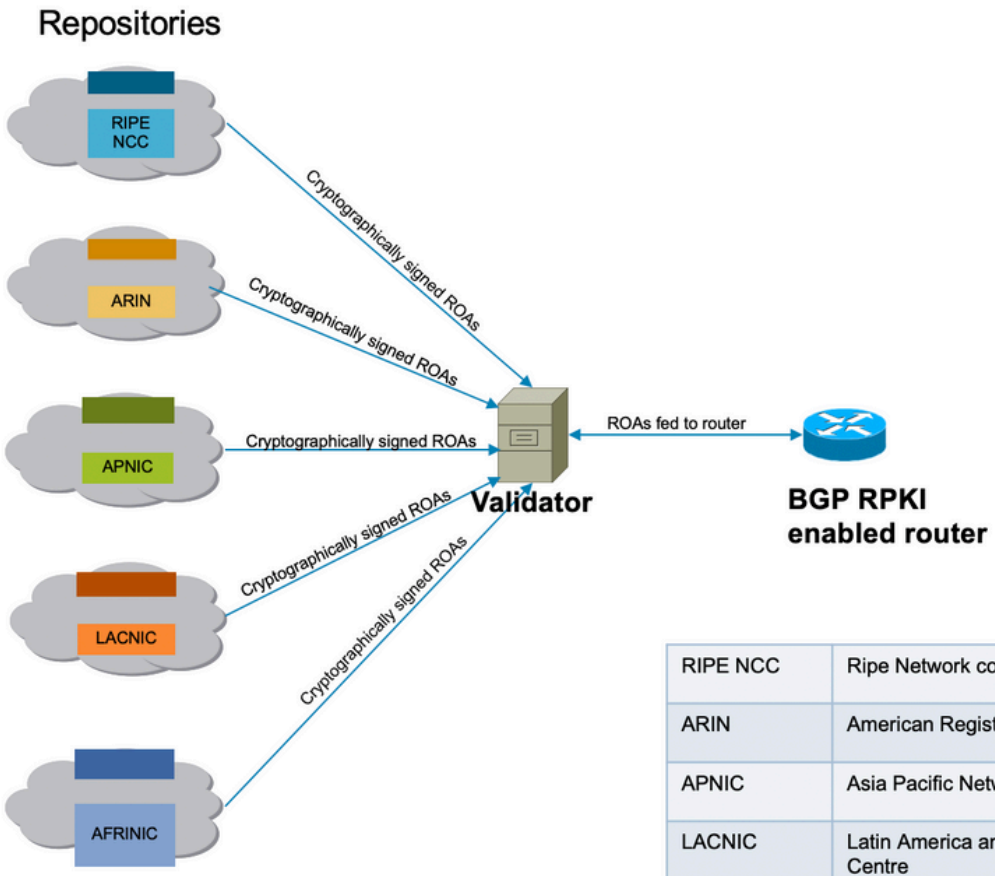
Die 5 regionalen Internet-Register (RIRs) sind die Vertrauensanker der RPKI. Die Internet Assigned Numbers Authority (IANA) ist die oberste Stelle im Baum, der die IP-Präfixe zugewiesen werden. Die RIRs folgen der Hierarchie. Sie weisen untergeordnete Präfixe lokalen Internetregistern (LIRs) und großen Internet Service Providern (ISPs) zu. Sie unterzeichnen ein Zertifikat für diese Präfixe. Die nächste Ebene weist diesen Teilpräfixen zu und verwendet die Zertifikate von oben, um ihre eigenen Zertifikate zu signieren, um ihre eigenen Zuweisungen zu

zertifizieren. In der Regel verwenden sie ihre eigenen Veröffentlichungspunkte, um die Zertifikate und ROAs zu hosten. Jedes Zertifikat listet die Veröffentlichungspunkte der untergeordneten Zertifikate auf, die es signiert. Daher bildet die RPKI einen Zertifikatsbaum, der den Baum der IP-Adresszuweisungen widerspiegelt. Die RPKI-Validierer der vertrauenden Parteien fragen alle Veröffentlichungspunkte ab, um aktualisierte Zertifikate und ROAs (sowie CRLs und Manifeste) zu finden. Sie beginnen an den Vertrauensankern und folgen den Links zu den Veröffentlichungspunkten der untergeordneten Zertifikate.

ROAs werden über RIRs in das Repository eingegeben, dies kann jedoch auch über andere (nationale oder lokale) Register erfolgen. Diese Verantwortung kann auch an die ISPs delegiert werden, wobei eine ordnungsgemäße Überwachung und Überprüfung durch die RIRs erfolgt.

Derzeit gibt es fünf ROA-Repositorys, die von RIPE NCE, ARIN, APNIC, LACNIC und AFRINIC unterhalten werden.

Ein Validator im Netzwerk kommuniziert mit diesen Repositories und lädt eine vertrauenswürdige ROA-Datenbank herunter, um den Cache zu erstellen. Hierbei handelt es sich um eine koaleszierte Kopie der RPKI, die regelmäßig direkt oder indirekt von der globalen RPKI abgerufen/aktualisiert wird. Validator leitet diese Informationen dann an die Router weiter, sodass diese die eingehenden BGP-Ankündigungen mit der RPKI-Tabelle vergleichen können, um eine sichere Entscheidung zu treffen.



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

RPKI-Infrastrukturkonnektivität

Validator

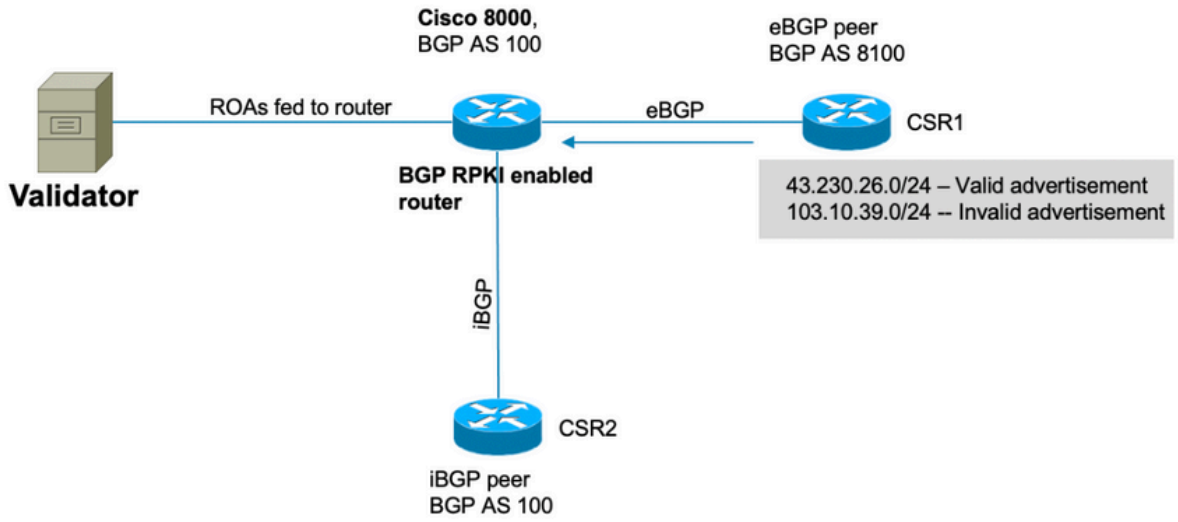
Bei dieser Demonstration wird der RIPE-Validator verwendet. Der Validator kommuniziert mit dem Router, indem er eine TCP-Sitzung herstellt. In dieser Demonstration lauscht das Validator unter seiner IP 192.168.122.120 und Port 3323.

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

IANA hat Port 3323 für diese Kommunikation angegeben. Der Aktualisierungszeitgeber definiert das Zeitintervall, nach dem das lokale Repository synchronisiert und aktualisiert wird, um aktualisiert zu bleiben.

BGP-RPKI-Demonstration

Topologie



Topologie

> **Hinweis**: Bei dieser Demonstration werden einfach zur Erläuterung der BGP RPKI-Mechanik zufällige öffentliche AS-Nummern und Präfixe verwendet. Öffentliche IPs werden verwendet, da RPKI primär für den Schutz öffentlicher Präfixe gedacht ist und alle auf RIRs erstellten ROAs öffentliche Präfixe sind. Schließlich hat keine der in diesem Dokument beschriebenen Aktionen, Konfigurationen usw. Auswirkungen auf diese öffentlichen IPs und AS.

Konfigurieren

```
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.
```

BGP-RPKI-Sitzung

Der Router richtet eine TCP-Sitzung mit einem Validator (IP: 192.168.122.120, Port 3323) ein, um den ROA-Cache in den Speicher des Routers herunterzuladen.

```
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
```

ROA-Downloads auf Router

Validator leitet die ROA-Informationen an den Router weiter. Dieser Cache wird in regelmäßigen Abständen aktualisiert, um die Möglichkeit zu minimieren, dass der Router veraltete Informationen enthält. In dieser Demonstration wurde eine Aktualisierungszeit von 900 Sekunden konfiguriert. Wie hier gezeigt, hat der Cisco Router der Serie 8000 vom Validator 172632 IPv4- und 28350 IPv6-ROAs heruntergeladen.

```
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
```

Überprüfung

Dieser Abschnitt zeigt, wie BGP RPKI in Aktion tritt und wie es den Router an falschen/illegalen Ankündigungen hindert.

Aktivieren von Origin-as-Validität

Standardmäßig ruft der Router ROAs vom Validator ab, verwendet sie jedoch erst, wenn er entsprechend konfiguriert wurde. Daher werden diese Präfixe als "D" markiert oder deaktiviert.

```
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 ?
```

Aktivieren Sie diesen Befehl für die betreffende Adressfamilie, um den Router für die Überprüfung der Ursprungsvalidität zu aktivieren.

```
router bgp 100
```

```
 address-family ipv4 unicast

 bgp origin-as validation enable

 !
```

Wenn Sie diesen Befehl aktivieren, veranlasst er den Router, die Präfixe in seiner BGP-Tabelle mit den ROA-Informationen abzugleichen, die er vom Validator erhalten hat, und einer der drei Zustände wird den Präfixen zugewiesen.

```
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 ?
```

Damit der Router bei der Berechnung des besten Pfads Präfixvalidierungszustandsinformationen verwenden kann, ist dieser Befehl erforderlich. Diese Option ist nicht standardmäßig aktiviert, da Sie die Validitätsinformationen nicht für die Berechnung des besten Pfads verwenden können. Sie können sie jedoch weiterhin in Weiterleitungsrichtlinien verwenden, die weiter unten in diesem Dokument behandelt werden.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

Präfix-Gültigkeitsstatus

Es gibt drei Zustände, in denen ein Präfix gefunden werden kann.

```
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 ?
```

- Ungültig - gibt an, dass das Präfix eine der beiden Bedingungen erfüllt: 1. Er stimmt mit einer oder mehreren **Route Origin Authorizations (**ROAs) überein, aber es gibt keine ROA-Übereinstimmung, bei der die Original-AS mit der Original-AS auf dem AS-PATH übereinstimmt. 2. Er entspricht mindestens einer ROA mit der in der ROA angegebenen Mindestlänge, ist jedoch für alle ROA, bei denen er mit der Mindestlänge übereinstimmt, länger als die angegebene Höchstlänge. Die Herkunft AS ist für die Bedingung #2 unerheblich.
- Gültig - Zeigt an, dass das Präfix und das AS-Paar in der RPKI-Cachetabelle gefunden wurden.
- Nicht gefunden - gibt an, dass das Präfix nicht zu den gültigen oder ungültigen Präfixen gehört.

In diesem Abschnitt werden jedes Präfix und sein Status im Detail beschrieben.

1. 203.0.113.0/24 - Gültig

Der eBGP-Peer im AS 8100 hat diese Route erstellt und dem Cisco 8000-Knoten angekündigt. Da das Ursprungs-AS (8100) mit dem Ursprungs-AS in ROA (vom Validator empfangen) übereinstimmt, wird dieses Präfix als gültig markiert und in der Routing-Tabelle des Routers installiert.

```
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
```

Die Route wird in der BGP-Tabelle installiert.

```
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
```

Da es sich hierbei um das beste und auch pro RPKI gültige BGP-Präfix handelt, wird es erfolgreich in der Routing-Tabelle installiert.

```
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 - Ungültig

Dieses Präfix ist ungültig, da ein Konflikt zwischen den in der ROA enthaltenen AS-Ursprungsinformationen und den AS-Ursprungsinformationen besteht, die über die BGP-Nachricht vom eBGP-Peer empfangen wurden. 203.0.113.1/24 wird über BGP mit dem Ursprungs-AS 8100 empfangen.

```
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 ?
```

Die vom Validator erhaltene ROA zeigt jedoch, dass dieses Präfix zu AS 10021 gehört.

```
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
```

Da die AS-Ursprungsinformationen in der empfangenen BGP-Ankündigung (AS 8100) nicht mit dem tatsächlichen AS-Ursprung übereinstimmen, der in ROA (AS 10021) empfangen wurde, wird das Präfix als ungültig markiert und nicht in der Routing-Tabelle installiert.

```
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 Nicht gefunden

Hierbei handelt es sich um ein privates Präfix, das nicht im ROA-Cache vorhanden ist. BGP hat dieses Präfix als "Nicht gefunden" deklariert.

```
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
```

Da RPKI immer noch übernommen wird, werden nicht gefundene Präfixe in der Routing-Tabelle installiert. Andernfalls ignoriert BGP diese legitimen Präfixe, die nicht in der RPKI-Datenbank registriert sind.

Ungültiges Präfix zulassen

Obwohl dies nicht empfohlen wird, bietet die Software einen Regler, mit dem ungültige Präfixe am Algorithmus zur Berechnung des besten Pfads beteiligt werden können.

```
router bgp 100
 address-family ipv4 unicast
 bgp bestpath origin-as allow invalid
 !
```

Bei dieser Konfiguration berücksichtigt der Router ungültige Präfixe für die Berechnung des besten Pfads, während dies als "ungültig" markiert ist. Diese Ausgabe zeigt "203.0.113.1/24" als besten Pfad an.

```
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 ?
```

Wie in dieser Ausgabe gezeigt, wird das Präfix als am besten markiert, obwohl es ungültig bleibt.

```
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
```

Es ist zu beachten, dass ein Router immer noch ein ungültiges Präfix als letzte Option behandelt und immer ein gültiges Präfix einem ungültigen Präfix vorzieht, wenn es verfügbar ist.

Manuelle ROA-Konfiguration auf Router

Wenn aus irgendeinem Grund ein ROA für ein bestimmtes Präfix noch nicht erstellt wurde, empfangen wird oder verzögert wird, kann ein manueller ROA auf dem Router konfiguriert werden. Das Präfix "192.168.122.1/32" ist z. B. als "Nicht gefunden" markiert, wie hier gezeigt.

```
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 ?
```

Ein manueller ROA kann wie hier dargestellt konfiguriert werden. Mit diesem Befehl wird das Präfix "192.168.122.1/32" dem AS 8100 zugeordnet.

```
router bgp 100

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

Bei dieser Konfiguration ändert sich der Status des Präfix von "N" zu "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 ?
```

Validierungsstatus für Route Policy und Präfix

Das Ergebnis des Präfixstatus kann zum Erstellen von Weiterleitungsrichtlinien verwendet werden. Diese Zustände können in einer Match-Anweisung verwendet werden, und der Administrator kann die gewünschten Aktionen durchführen. In diesem Beispiel werden alle Präfixe mit einem ungültigen Status abgeglichen und ein Gewichtswert von 12345 für sie festgelegt.

```
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
 !
 !
!
```

Diese Ausgabe zeigt eine ungültige Präfixgewichtung von 12345 an.

```
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
```

Weitergabe von Präfixvalidierungsinformationen über die erweiterte Community

Da der BGP-Router den Präfix-Validierungsstatus auch mit anderen Routern (ohne lokalen Cache vom Validator) über die erweiterte BGP-Community teilen kann. Dies spart den Aufwand für jeden Router im Netzwerk, indem eine Sitzung mit dem Validator aufgebaut und alle ROAs heruntergeladen werden.

Möglich wird dies durch die erweiterte BGP-Community.

Mit diesem Befehl kann der Router Informationen zur "Präfix-Validierung" für iBGP-Peers freigeben.

```
router bgp 100

 address-family ipv4 unicast

 bgp origin-as validation signal ibgp
```

Sobald der Cisco 8000-Router wie dargestellt konfiguriert ist, schließen BGP-Updates an Peers Informationen zur Präfixvalidierung ein. In diesem Fall ist der benachbarte iBGP-Router ein IOS-XE-Router.

```
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
```

Diese erweiterte Community-Zuordnung kann unter Verwendung von 0x4300 0x0000 (4 Byte für den Status) verstanden werden.

Die vier Bytes, die den Status angeben, werden als 32-Bit-Ganzzahl ohne Vorzeichen mit einem der folgenden Werte behandelt:

- 0 - Gültig
- 1 - Nicht gefunden
- 2 - Ungültig

Das Präfix 203.0.113.1/24 ist 0x4300:0:2, das dem Präfix "Invalid" zugeordnet ist. Auf diese Weise kann der csr2-Router, obwohl er keinen eigenen lokalen Cache hat, Entscheidungen basierend auf dem Präfix-Validierungsstatus treffen.

Der Präfixvalidierungsstatus kann jetzt für die Zuordnung in einer Routing-Map oder im BGP-Algorithmus für den besten Pfad verwendet werden.

Empfehlungen für die BGP RPKI-Implementierung

Best Practices für die ROA-Erstellung

Dies sind einige Empfehlungen, die auf nicht erreichbaren Netzwerken basieren, die am RPKI-Observatorium beobachtet wurden. Das RPKI Observatory analysiert verschiedene Aspekte der bereitgestellten RPKI-Landschaft.

- Wenn für ein Präfix eine ROA erstellt wird, wird empfohlen, dieses Präfix im BGP anzukündigen. Andernfalls kann ein anderer Benutzer den Vorgang ankündigen, indem er vorgibt, in diesem ROA enthaltene ASN zu sein, und das Präfix verwendet.
- Wenn der ROA mit einer maximalen Länge größer als die Präfixlänge erstellt wird, entspricht dies der Erstellung von ROAs für alle möglichen Präfixe unter dem ursprünglichen Präfix bis zur maximalen Länge. Es wird dringend empfohlen, alle diese Präfixe im BGP anzukündigen.
- Wenn eine ROA für ein Präfix erstellt wird und der Präfixbesitzer ein Subpräfix des ursprünglichen Präfixes ankündigt, wird dieses Subpräfix von der ROA ungültig gemacht. Eine ROA für das Sub-Präfix oder die maximale Anzahl der ursprünglichen ROA muss erweitert werden, um das Sub-Präfix abzudecken.
- Wenn eine Organisation über ein Präfix verfügt, dieses jedoch nicht im BGP ankündigen möchte, muss eine ROA für das Präfix für AS0 erstellt werden. Dadurch wird jede Ankündigung des Präfix ungültig, da AS0 in keinem AS-Pfad angezeigt werden kann.
- Wenn mehrere ASNs vom gleichen Präfix ausgehen, müssen ROAs für dieses Präfix für jedes ASN erstellt werden. Wenn ein Router über mehrere ROAs für dasselbe Präfix verfügt, ist daher eine BGP-Benachrichtigung gültig, die mit einem der ROAs übereinstimmt. Mehrere ROAs für dasselbe Präfix stehen nicht in Konflikt miteinander.
- Wenn "A" von einem Präfix für seinen Kunden "B" ausgeht und im Namen von "B" eine ROA für dieses Präfix erstellt, muss "A" der Ankündigung eine B-ASN voranstellen, oder das "B" muss den Präfix selbst ausgeben.

Leistungsauswirkung von RPKI auf XR-BGP-Routern

Auswirkung der ROA-Aktualisierung auf die CPU mit Routen-Richtlinie

Wenn ROAs aktualisiert werden und der Router über eine lokale Eingangs-Routenrichtlinie für einen Nachbarn verfügt, der den Status "validieren ist" aufweist, muss der Status von Präfixen basierend auf neuen aktualisierten ROAs erneut validiert werden. Dies wird erreicht, indem der

Router eine BGP-REFRESH-Anfrage an seinen Peer sendet.

Wenn BGP-Nachbarn diese Nachricht wie dargestellt empfangen, senden sie ihre Präfixe erneut, und die Richtlinie für eingehende Routen kann die eingehenden Präfixe erneut validieren.

```
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
```

Das Problem verschärft sich noch, wenn viele Nachbarn gleichzeitig neue ROAs installieren. Wenn die Richtlinien für eingehende Nachbar-Routen komplex sind und viel Verarbeitung erfordern, führt dies nach einer ROA-Aktualisierung für einige Minuten zu hohen CPU-Ergebnissen. Diese REFRESH-Meldungen treten nicht auf, wenn die eingehende Route-Policy des Nachbarn keinen Befehl "validation-state is" enthält.

Wenn "Soft-Reconfiguration inbound always" (Soft-Rekonfiguration immer eingehend) für einen Nachbarn konfiguriert ist, werden keine BGP-REFRESH-Nachrichten gesendet, aber die gleichen Routing-Richtlinien werden weiterhin mit derselben Geschwindigkeit ausgeführt, und es kann mit derselben CPU-Auslastung gerechnet werden.

Es wird empfohlen, den Ansatz "bgp bestpath origine-as use valid" gegenüber der Konfiguration einer Routing-Richtlinie aus den in Abschnitt 6.2.2 unten erläuterten Gründen zu bevorzugen.

Minimierung der durch ROA-Update verursachten CPU-Auswirkungen

Die beste Möglichkeit, das hier erläuterte Problem zu vermeiden, besteht darin, **bestpath origine** zu verwenden**, da die Validierung** ohne **Validierungsstatus** in der Richtlinie **erfolgt**.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

Mit diesem Befehl wird eine empfangene ungültige Route auf dem Router beibehalten, aber verhindert, dass sie zu einem besten Pfad wird. Es wird nicht installiert oder weiterverbreitet. Es ist so gut wie fallen lassen. Wenn die ROA beim nächsten ROA-Update gültig wird, ist keine AKTUALISIERUNG erforderlich. Die Anwendung wird automatisch für den besten Pfad zugelassen, und es ist keine Richtlinienausführung erforderlich.

Wenn der Benutzer es vorzieht, "ungültige" Präfixe zuzulassen und diese nicht zu verwenden, dann verwenden Sie zusätzlich zur **bestmöglichen Pfadquelle als Verwendungsgültigkeit** die Konfiguration **bestmöglicher Pfadquelle als ungültig zulassen**.

In diesem Fall wird der beste Pfad automatisch aktualisiert, wenn sich die ROA ändert, ohne dass eine REFRESH-Meldung erforderlich ist. Um die Bevorzugung zu deaktivieren, bedeutet eine Route, dass während der Auswahl der BGP-Route der ungültige RPKI-Pfad als weniger bevorzugt angesehen wird als jeder andere Pfad zum gleichen Ziel. Es ist vergleichbar mit dem Zuweisen von Gewicht oder lokaler Präferenz unter 0.

Die Anzahl der RPKI-Invaliden ist relativ gering und bleibt in der Tabelle erhalten, was keine

nennenswerten Auswirkungen auf die Ressourcen hat.

> **Hinweis**: Um "bestpath origine-as use valid" zu verwenden, müssen alle Pfade einer Route, einschließlich der IBGP-Pfade, die richtige RPKI-Validität aufweisen. Ist dies nicht der Fall, kann weiterhin der Validierungsstatus in der Routenrichtlinie getestet werden.

IBGP-Routen werden vom Router nicht anhand der ROA-Datenbank validiert. IBGP-Routen erhalten eine RPKI-Gültigkeit von der erweiterten RPKI-Community. Wenn die IBGP-Route ohne diese erweiterte Community empfangen wird, wird ihr Validierungsstatus auf "nicht gefunden" gesetzt.

BGP-RPKI-Speicherbedarf

Jeder ROA belegt Arbeitsspeicher für den Index und die Daten. Wenn zwei ROAs für dasselbe IP-Präfix stehen, aber unterschiedliche max_len-Werte haben oder von verschiedenen RPKI-Servern empfangen werden, verwenden sie denselben Index, aber separate Daten. Die Speicheranforderungen können variieren, da der Arbeitsspeicher-Overhead nicht konstant ist. Es wird ein Überbudget von 10 % empfohlen. 64-Bit-Plattformen benötigen mehr Speicher für jedes Speicherobjekt als 32-Bit-Plattformen. Die IOS-XR-Speichernutzung in Byte für ein Indexobjekt und ein Datenobjekt ist in der Tabelle aufgeführt. Einige meist konstante Gemeinkosten sind in den Zahlen enthalten.

	32-Bit-Plattform (Byte)	64-Bit-Plattform (Byte)
IPv4-Index	74	111
IPv6-Index	86	125
Daten	34	53

In diesem Abschnitt werden zwei Szenarien erläutert, wie ROAs Speicher nutzen.

Szenario 1. Drei auf Router konfigurierte RPKI-Server

Stellen Sie sich einen Router vor, der 3 RPKI-Server verwendet, von denen jeder 200.000 IPv4-ROAs und 20.000 IPv6-ROAs auf einem 64-Bit-Routing-Prozessor benötigt:

20000 * (125 + 3*53) + 200000 * (111 + 3*53) Bytes = 59,68 Millionen Bytes

Bei der Berechnung des Speichers wurde der ROA für dasselbe Präfix von drei verschiedenen Validierungssteuerelementen mit demselben Indexwert verwendet.

Szenario 2. Auf Router konfigurierte einzelne RPKI-Server

BGP-Prozessspeicher ohne ROAs:

```
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
```

Der BGP-Prozess beansprucht 25 MB Speicher ohne ROAs.

BGP-Prozessspeicher mit 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
```

Der BGP-Prozess beansprucht 25 MB Speicher ohne ROAs.

BGP-Prozessspeicher mit 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
```

Auf dem Cisco 8000-Router wird ein 64-Bit-Betriebssystem ausgeführt. Es erhielt 172796 IPv4 ROA und 28411 ROA.

Speicher (Byte) = 172.796 x [111 (Index) + 53 (Daten)] + 28411 x [125 (Index) + 53 (Daten)].

Diese Berechnungen ergeben ~27 MB. Dies entspricht in etwa dem Inkrement, das oben im Speicher des Routers festgestellt wurde.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.