XR7 Cisco8000 백서를 통한 BGP RPKI 이해

목차

소개

이 문서에서는 Cisco IOS® XR 플랫폼의 BGP(Border Gateway Protocol) RPKI(Resource Public Key Infrastructure) 기능에 대해 설명합니다.

배경 정보

서론

이 문서에서는 BGP RPKI 기능 및 라우터가 있는 BGP를 허위/악성 BGP 접두사 업데이트로부터 보호하는 방법에 대해 설명합니다.

범위

이 문서에서는 데모용으로 Cisco 8000 및 XR 7.3.1 릴리스를 사용합니다. 그러나 BGP RPKI는 플랫폼에 종속되지 않는 기능입니다. 이 문서에서 설명하는 개념은 적절한 CLI 변환을 통해 다른 Cisco 플랫폼(Cisco IOS, Cisco IOS-XE 사용)에 적용됩니다. 이 문서에서는 지역 인터넷 레지스트리에 ROA(Route Origin Authorization)를 추가하는 절차에 대해서는 다루지 않습니다.

사전 요구 사항

판독기는 BGP 프로토콜에 대한 지식이 필요합니다.

면책조항

이 문서에 사용된 IP(인터넷 프로토콜) 주소는 실제 주소가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력 및 그림은 이해를 돕기 위한 자료일 뿐입니다. 실제 IP 주소를 사용하는 것은 의도하지 않은 우연의 일치입니다.

잘못된 접두사 광고로 인한 BGP 문제

BGP는 인터넷 트래픽의 백본 역할을 합니다. 인터넷 코어의 가장 중요한 구성 요소이지만 인그레스 BGP 알림이 인증된 자동 시스템에서 시작되었는지 확인할 수 있는 기능이 없습니다.

BGP의 이러한 제한은 다양한 종류의 공격에 대한 쉬운 후보입니다. 한 가지 일반적인 공격을 '라우트 하이잭'이라고 합니다. 이 공격은 다음과 같은 목적으로 악용될 수 있습니다.

- 스팸 결과를 전송하기 위해 IP를 도용하면 IP가 거부되어 서비스가 거부됩니다.
- 비밀번호와 같은 민감한 정보를 얻기 위해 트래픽을 감시합니다.
- 관리자의 잘못된 구성으로 인한 중단
- 서비스 거부를 위해 위조 서버를 가동하여 트래픽의 전달을 방지합니다.

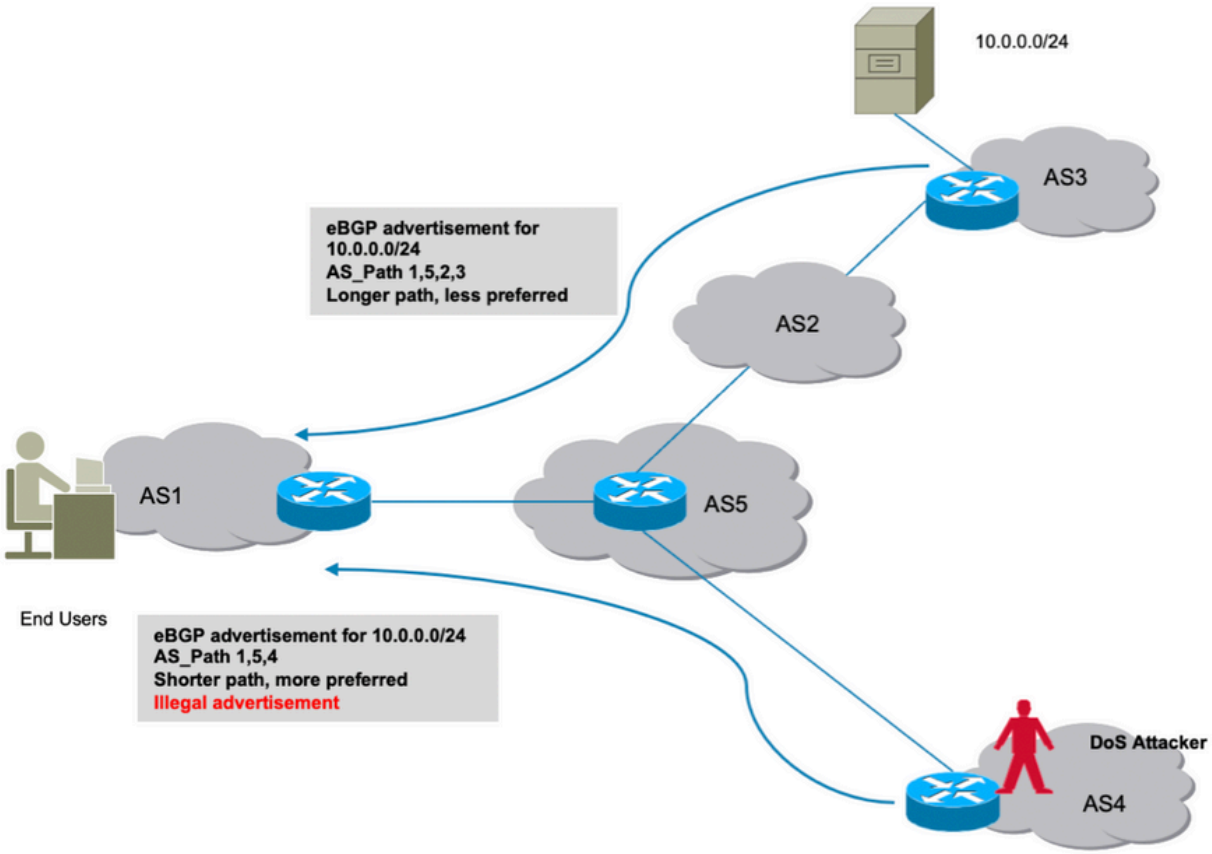
DoS(Denial of Service) 공격은 라우터, 스위치, 서버 등에 대한 정상적인 트래픽을 방해하려는 악의적인 시도입니다. 다양한 DoS 공격이 있으며 여기서는 몇 가지 공격에 대해 설명합니다.

경로 하이재킹

여기에 나와 있는 시나리오를 고려해 보십시오. AS3(Autonomous System 3)은 접두사 10.0.0.0/24에 대한 법적 BGP 광고를 전송합니다. BGP의 설계상, BGP에는 공격자가 동일한 접두사를 인터넷에 광고하는 것을 막을 수 있는 것이 없습니다.

그림과 같이 AS4의 공격자는 동일한 접두사 10.0.0.0/24을 광고합니다. BGP 최적 경로 알고리즘은

AS_Path가 더 짧은 경로를 선호합니다. AS_Path 1,5,4는 AS 1,5,2,3을 통해 더 긴 경로를 이깁니다. 따라서 클라이언트에서 오는 트래픽은 이제 공격자의 환경으로 리디렉션되고 블랙홀링되어 최종 클라이언트에 대한 서비스 거부가 발생할 수 있습니다.

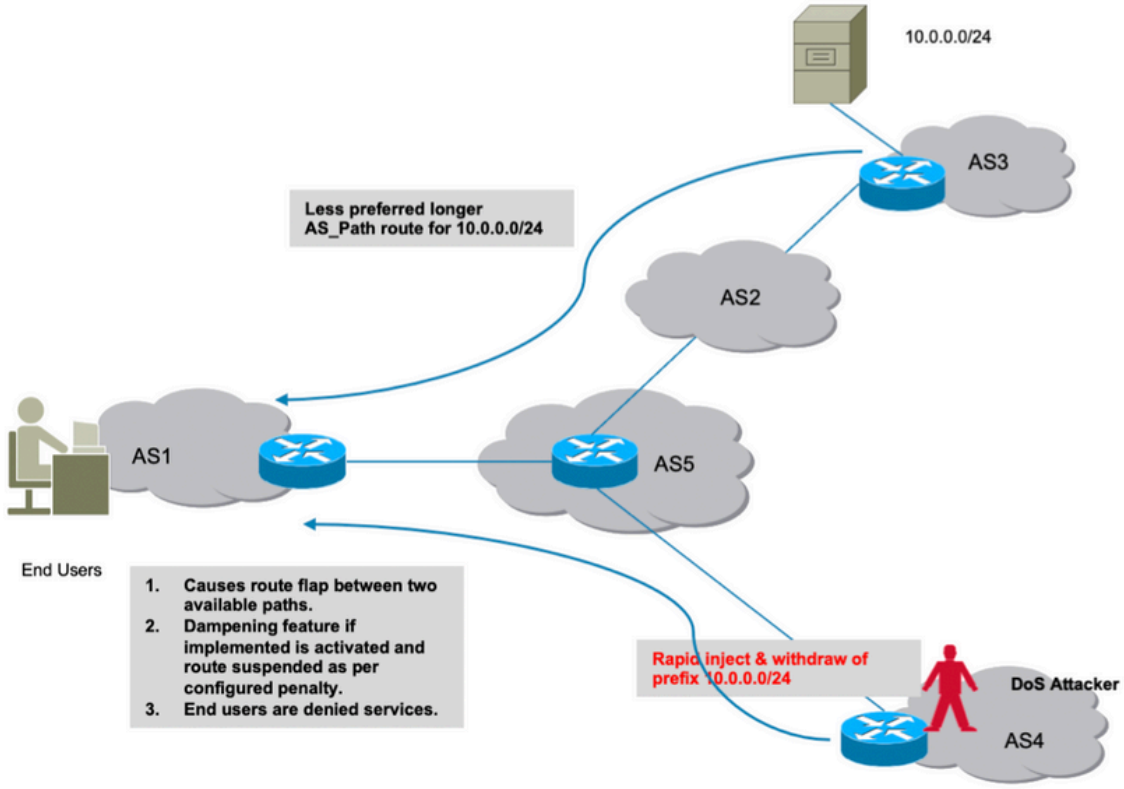


루트 하이잭

시스템 성능 저하

이 섹션에서는 서비스를 거부할 수 있는 또 다른 방법에 대해 설명합니다. Cisco의 BGP 경로 댐프닝 기능이 구성된 경우, 공격자가 네트워크에서 급격한 경로 플랩을 도입하여 지속적으로 흔들리는 경우 악용될 수 있습니다.

댐프닝 기능은 합법적인 경로에 페널티를 부과하고 실제 트래픽에 사용할 수 없게 만듭니다. 또한 이러한 종류의 비윤리적으로 유발된 플랩은 CPU, 메모리 등과 같은 라우터의 리소스에 부담을 줍니다.

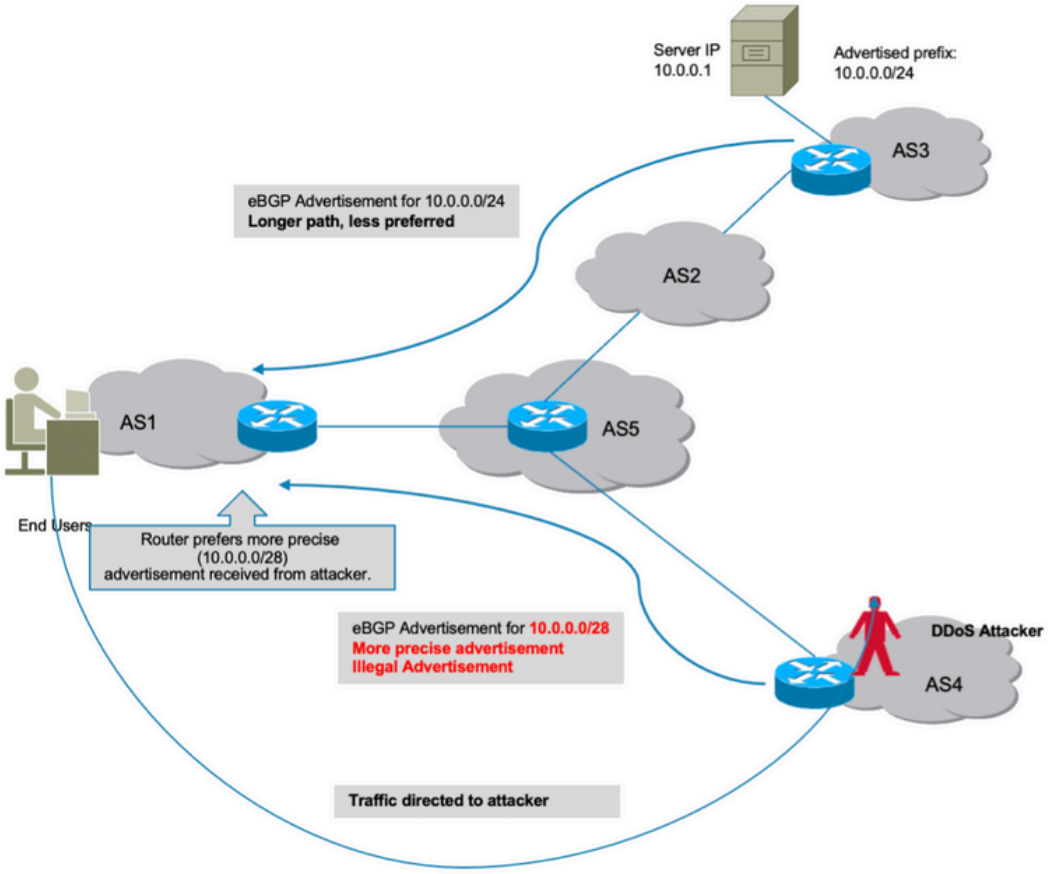


경로 댐프닝

하위 접두사 하이재킹

이전 섹션에서 설명한 것처럼, 공격자가 접두사를 불법적으로 생성하여 트래픽 중단을 일으킬 수 있는 방법은 무엇입니까? 안타깝게도, 혼란만이 우려의 원인이 아닙니다. 이러한 공격에서는 공격자가 수신된 데이터를 스캔하여 비윤리적인 용도로 사용할 수 있는 실제 데이터가 손상될 수 있습니다.

마찬가지로, 노선의 하이재킹은 보다 정확한 노선을 불법적으로 광고함으로써 이루어질 수 있다. BGP는 더 긴 일치 접두사를 선호하며 이 동작은 이미지에 표시된 것처럼 잘못 악용될 수 있습니다.



하위 접두사 하이잭

논의되는 모든 공격은 BGP가 악의적으로 광고된 접두사의 원본 AS가 유효한지 여부를 식별할 수 없었기 때문에 발생합니다. 이를 해결하려면 라우터가 데이터베이스에 보관할 수 있는 '실제' 및 '신뢰할 수 있는' 데이터 소스가 필요합니다. 그런 다음 새 광고가 수신될 때마다 라우터는 이제 BGP 피어에서 수신한 접두사의 AS 원점 정보를 검증기의 로컬 데이터베이스 정보와 상호 검증할 수 있게 됩니다.

따라서 라우터는 좋은 광고와 나쁜(불법) 광고를 구별할 수 있으며, 이전에 논의한 모든 공격을 방지하는 기능이 기본적으로 라우터에 추가됩니다. BGP RPKI는 신뢰할 수 있는 필수 정보 소스를 제공합니다.

RPKI

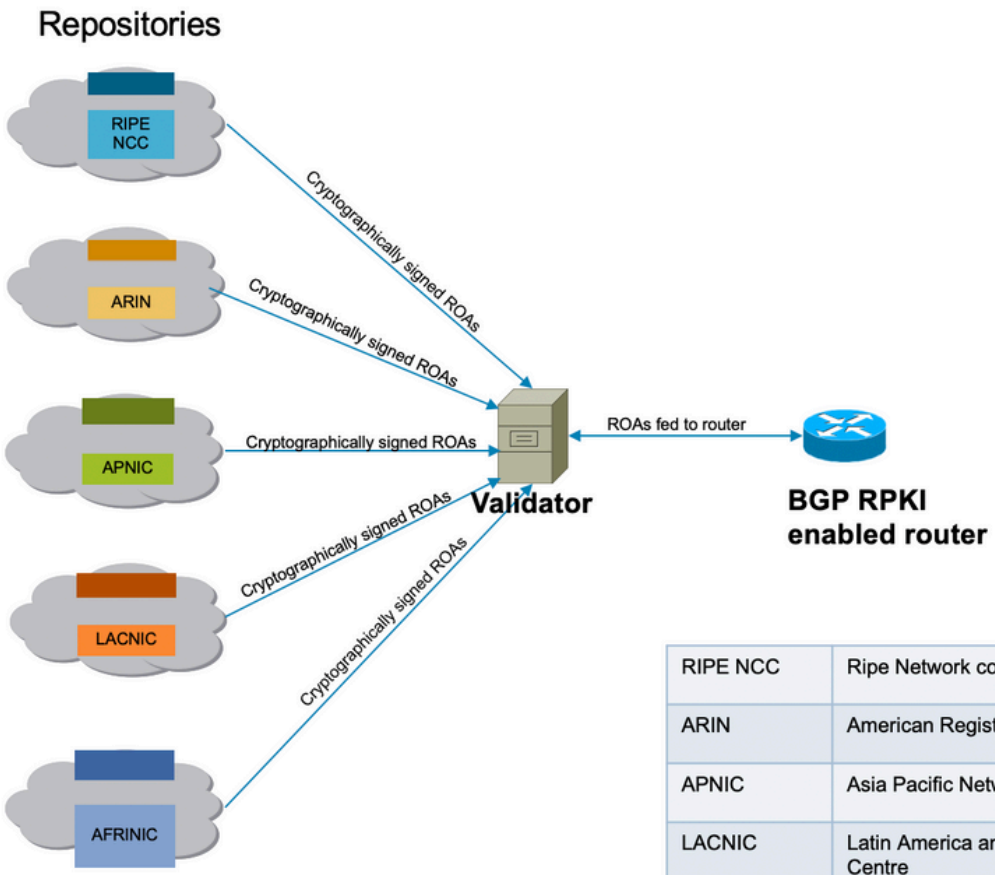
RPKI는 ROA가 포함된 리포지토리를 사용합니다. ROA에는 접두사 및 연결된 BGP AS 번호에 대한 정보가 포함됩니다. 경로 출처 인증은 암호로 서명된 문입니다.

5개의 지역 인터넷 레지스트리(RIR)는 RPKI의 트러스트 앵커입니다. IANA(Internet Assigned Numbers Authority)는 IP 접두사를 전달하는 트리의 상단입니다. RIR은 계층 구조의 다음입니다. 로컬 인터넷 레지스트리(LIR) 및 대형 인터넷 서비스 공급자(ISP)에 하위 접두사를 할당합니다. 이러한 접두사에 대한 인증서에 서명합니다. 다음 레벨에서는 하위 접두사를 할당하고 위의 인증서를 사용하여 자체 인증서를 서명하여 자체 할당을 인증합니다. 일반적으로 자체 게시 지점을 사용하여 인증서 및 ROA를 호스팅합니다. 각 인증서는 서명하는 하위 인증서의 게시 지점을 나열합니다. 따라서 RPKI는 IP 주소 할당 트리를 미러링하는 인증서 트리를 형성합니다. 신뢰 당사자가 소유한 RPKI 검증자는 모든 게시 지점을 폴링하여 업데이트된 인증서 및 ROA(및 CRL 및 매니페스트)를 찾습니다. 트러스트 앵커에서 시작하여 자식 인증서의 게시 지점으로 연결되는 링크를 따릅니다.

ROA는 RIR을 통해 저장소에 입력되지만, 다른 등록 기관(국가 또는 지역)을 통해서도 마찬가지입니다. 이러한 책임은 RIR에 의한 적절한 감독과 검증으로 ISP에 위임될 수도 있다.

현재 RIPE NCE, ARIN, APNIC, LACNIC 및 AFRINIC에 의해 유지되는 5개의 ROA 저장소가 있습니다.

네트워크에 있는 유효성 검사기는 이러한 저장소와 통신하고 신뢰할 수 있는 ROA 데이터베이스를 다운로드하여 캐시를 구축합니다. RPKI의 통합된 복사본이며 정기적으로 글로벌 RPKI에서 직접 또는 간접적으로 인출/새로 고칩니다. 그런 다음 검증기는 라우터에 이 정보를 전달하여 라우터가 수신 BGP 알림을 RPKI 테이블과 비교하여 안전하게 결정할 수 있도록 합니다.



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 인프라 연결

유효성 검사기

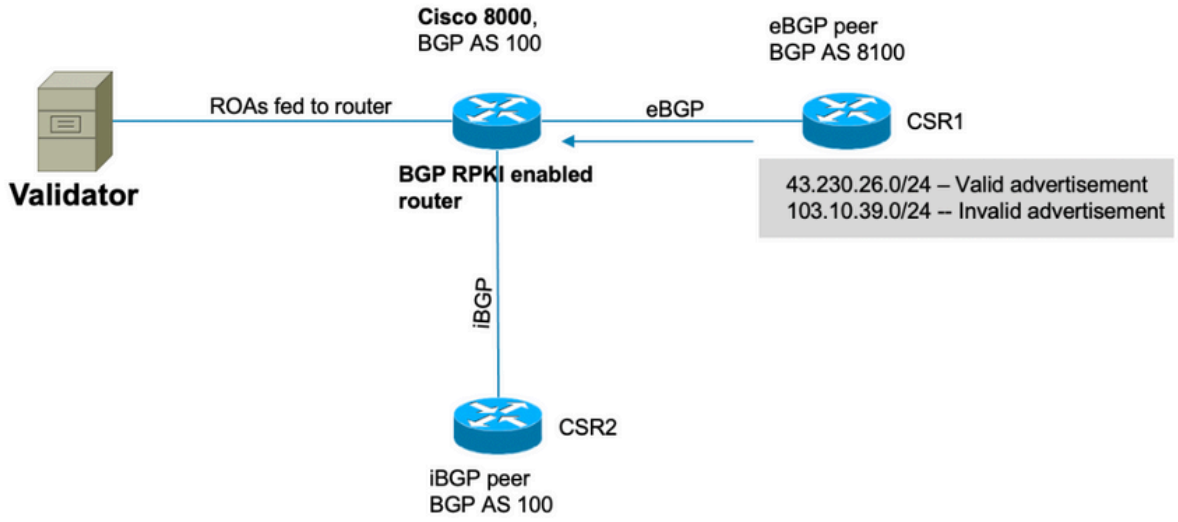
이 데모에서는 RIGHT 유효성 검사기를 사용합니다. 검증기는 TCP 세션을 설정하여 라우터와 통신합니다. 이 데모에서 검증기는 IP 192.168.122.120 및 포트 3323에서 수신 대기합니다.

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

IANA에서 이 통신에 대해 포트 3323을 지정했습니다. 새로 고침 타이머는 로컬 저장소가 동기화 및 업데이트되어 업데이트 상태를 유지하는 시간 간격을 정의합니다.

BGP RPKI 데모

토폴로지



토폴로지

> **참고**: 이 데모에서는 BGP RPKI 메커니즘을 설명하기 위해 무작위 공용 AS 번호 및 접두사를 사용합니다. RPKI로 인해 공용 IP가 사용되며, 이는 주로 공용 접두사 보호를 위한 것이며 RIR에 생성된 모든 ROA는 공용 접두사입니다. 마지막으로, 이 문서에 설명된 작업, 컨피그레이션 등은 어떤 식으로든 이러한 공용 IP 및 AS에 영향을 미치지 않습니다.

구성

```
 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 세션

라우터는 ROA 캐시를 라우터의 메모리에 다운로드하기 위해 검증기(IP: 192.168.122.120, 포트 3323)를 사용하여 TCP 세션을 설정합니다.

```
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
```

라우터에서 ROA 다운로드

검증기는 ROA 정보를 라우터에 전달합니다. 이 캐시는 라우터가 오래된 정보를 보유할 가능성을 최소화하기 위해 주기적으로 업데이트됩니다. 이 데모에서는 900초의 새로 고침 시간이 구성되었습니다. 여기에 표시된 것처럼 Cisco 8000 라우터는 172632 IPv4 및 28350 IPv6 ROA를 검증기에서 다운로드했습니다.

```
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
```

다음을 확인합니다.

이 섹션에서는 BGP RPKI의 작동 방식 및 라우터의 잘못된/불법 광고를 방지하는 방법을 설명합니다.

Origin-As 유효성 활성화

기본적으로 라우터는 검증기에서 ROA를 가져오지만 사용하도록 구성될 때까지 사용을 시작하지 않습니다. 그 결과, 이러한 접두사는 'D'로 표시되거나 비활성화됩니다.

```
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 ?
```

as-origin 유효성 검사를 위해 라우터를 활성화하려면 관련 주소 패밀리에 대해 이 명령을 활성화합니다.

```
router bgp 100

 address-family ipv4 unicast

 bgp origin-as validation enable

 !
```

이 명령을 활성화하면 라우터가 BGP 테이블에 있는 접두사를 유효성 검사기에서 받은 ROA 정보에 대해 검사하고 세 가지 상태 중 하나가 접두사에 할당됩니다.

```
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 ?
```

라우터가 최상의 경로 계산을 수행하면서 접두사 유효성 검사 상태 정보를 사용할 수 있도록 하려면 이 명령이 필요합니다. 이 옵션은 최상의 경로 계산을 위해 유효성 정보를 사용하지 않고 이 문서의 뒷부분에서 설명하는 경로 정책에서 사용할 수 있도록 하는 옵션을 제공하므로 기본적으로 활성화되지 않습니다.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

접두사 유효성 상태

접두사는에서 찾을 수 있는 세 가지 상태가 있습니다.

```
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 ?
```

- Invalid - 접두사가 다음 두 조건 중 하나를 충족함을 나타냅니다. 1. 하나 이상의 ROA(**Route Origin Authorization**)와 일치하지만, AS-PATH에서 원본 AS와 일치하는 ROA 일치는 없습니다 . 2 . ROA에 지정된 최소 길이의 하나 이상의 ROA와 일치하지만, 최소 길이와 일치하는 모든 ROA의 경우 지정된 최대 길이보다 깁니다. Origin AS는 조건 #2에 상관없습니다.
- Valid(유효) - RPKI 캐시 테이블에 접두사 및 AS 쌍이 있음을 나타냅니다.
- Not Found - 접두사가 유효하지 않거나 유효하지 않은 접두사에 없음을 나타냅니다.

이 섹션에서는 각 접두사와 접두사의 상태에 대해 자세히 설명합니다.

1. 203.0.113.0/24 - 유효

AS 8100의 eBGP 피어가 이 경로를 시작했으며 Cisco8000 노드에 알려졌습니다. Origin AS(8100)는 ROA(validator에서 수신)의 origin AS와 일치하므로 이 접두사는 유효한 것으로 표시되고 라우터의 라우팅 테이블에 설치됩니다.

```
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
```

경로가 BGP 테이블에 설치됩니다.

```
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
```

이는 최상의 BGP 접두사이며 RPKI당 유효하므로 라우팅 테이블에 성공적으로 설치됩니다.

```
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 - 잘못됨

ROA에 포함된 원본 AS 정보와 eBGP 피어에서 BGP 메시지를 통해 수신한 원본 AS 정보가 충돌하므로 이 접두사는 유효하지 않습니다. 203.0.113.1/24은 오리진 AS 8100의 BGP를 통해 수신됩니다.

```
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 ?
```

그러나 유효성 검사기에서 받은 ROA는 이 접두사가 AS에 속한다는 것을 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
```

수신된 BGP 알림(AS 8100)의 AS 발신지 정보가 ROA(AS 10021)에서 수신된 실제 AS 발신지와 일치하지 않으므로 접두사는 Invalid로 표시되고 라우팅 테이블에 설치되지 않습니다.

```
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. 192.168.122.1/32을 찾을 수 없음

이 접두사는 개인 접두사이며 ROA 캐시에 없습니다. BGP에서 이 접두사를 'Not found'로 선언했습니다.

```
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
```

RPKI가 계속 채택되므로 'not-found' 접두사가 라우팅 테이블에 설치됩니다. 그렇지 않으면 BGP가 RPKI 데이터베이스에 등록되지 않은 이러한 합법적인 접두사를 무시하게 됩니다.

잘못된 접두사 허용

권장되지 않지만, 소프트웨어는 잘못된 접두사가 최적 경로 계산 알고리즘에 참여할 수 있도록 노브를 제공합니다.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as allow invalid

 !
```

이 컨피그레이션에서는 라우터가 최상의 경로 계산을 위해 잘못된 접두사를 고려하는 반면, 이는 'invalid'로 표시됩니다. 이 출력에는 최상의 경로로 표시된 '203.0.113.1/24'이 표시됩니다.

```
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 ?
```

이 출력에 표시된 대로 접두사는 잘못된 상태로 유지되더라도 best로 표시됩니다.

```
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
```

라우터는 여전히 유효하지 않은 접두사를 마지막 옵션으로 취급하며, 사용 가능한 경우 항상 유효하지 않은 접두사보다 유효한 접두사를 선호합니다.

라우터의 수동 ROA 컨피그레이션

어떤 이유로 특정 접두사에 대한 ROA가 아직 생성되지 않았거나 수신되거나 지연되는 경우 라우터에서 수동 ROA를 구성할 수 있습니다. 예를 들어, 접두사 '192.168.122.1/32'는 여기에 표시된 대로 'Not Found'로 표시됩니다.

```
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 ?
```

여기에 표시된 대로 수동 ROA를 구성할 수 있습니다. 이 명령은 '192.168.122.1/32' 접두사를 AS 8100과 연결합니다.

```
router bgp 100

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

이러한 구성에 따라, 접두사의 상태가 'N'에서 'V'로 변경된다.

```
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 ?
```

경로 정책 및 접두사 유효성 검사 상태

접두사 상태 결과는 경로 정책을 생성하는 데 사용할 수 있습니다. 이러한 상태는 match 문에서 사용할 수 있으며 관리자가 원하는 작업을 수행할 수 있습니다. 이 예에서는 잘못된 상태의 모든 접두사를 일치시키고 접두사에 대한 가중치 값을 12345으로 설정합니다.

```
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

 !

 !

!
```

이 출력에는 잘못된 접두사 적용 가중치가 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
```

확장 커뮤니티를 통해 접두사 유효성 검사 정보 공유

BGP 라우터는 BGP 확장 커뮤니티를 통해 접두사 유효성 검사 상태를 다른 라우터(유효성 검사기의 로컬 캐시 없음)와 공유할 수도 있습니다. 이렇게 하면 검증기가 있고 모든 ROA를 다운로드하는 세션을 통해 네트워크에 있는 모든 라우터의 오버헤드가 절약됩니다.

이는 BGP 확장 커뮤니티에 의해 가능합니다.

이 명령을 사용하면 라우터가 'prefix-validation' 정보를 iBGP 피어와 공유할 수 있습니다.

```
router bgp 100

 address-family ipv4 unicast

 bgp origin-as validation signal ibgp
```

Cisco 8000 라우터가 그림과 같이 구성되면 피어에 대한 BGP 업데이트는 접두사 유효성 검사 정보를 포함합니다. 이 경우 네이버 iBGP 라우터는 IOS-XE 라우터입니다.

```
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
```

이 확장 커뮤니티 매핑은 0x4300 0x0000(상태를 나타내는 4바이트)을 사용하여 이해할 수 있습니다.

상태를 나타내는 4바이트는 값 중 하나를 갖는 32비트 부호 없는 정수로 처리됩니다.

- 0 - 유효
- 1 - 찾을 수 없음
- 2 - 유효하지 않음

접두사 203.0.113.1/24의 커뮤니티는 'Invalid' 접두사에 매핑되는 0x4300:0:2입니다. 이렇게 하면 자체 로컬 캐시가 없음에도 불구하고 csr2 라우터는 여전히 접두사 검증 상태를 기반으로 결정을 내릴 수 있습니다.

이제 경로 맵 또는 BGP 최적 경로 알고리즘에서 접두사 유효성 검사 상태를 일치시키는 데 사용할 수 있습니다.

BGP RPKI 구현을 위한 권장 사항

ROA 생성을 위한 모범 사례

다음은 RPKI- Observatory에서 관찰된 도달 불가 네트워크를 기반으로 한 몇 가지 권장 사항입니다. RPKI 전망대는 구축된 RPKI 환경의 여러 측면을 분석합니다.

- 접두사에 대해 ROA가 생성된 경우 BGP에서 해당 접두사를 알리는 것이 좋습니다. 그것이 없을 경우, 다른 누군가는 단순히 그 ROA에 포함된 ASN인 것처럼 가장하여 이를 발표하고 접두사를 사용할 수 있다.
- ROA가 접두사 길이보다 큰 maxlen으로 생성된 경우, 이는 maxlen까지 원본 접두사 아래에서 가능한 모든 접두사에 대한 ROA를 생성하는 것과 같습니다. BGP의 모든 접두사를 알리는 것이 좋습니다.
- 접두사에 대해 ROA가 생성되고 접두사 소유자가 원래 접두사의 하위 접두사를 알리면 ROA는 해당 하위 접두사를 무효화합니다. 서브-프리픽스에 대한 ROA 또는 원래 ROA의 최대값은 서브-프리픽스를 커버하도록 확장되어야 한다.
- 조직에서 접두사를 소유하고 있지만 BGP에서 이를 알리지 않을 계획인 경우 AS0의 접두사에 대한 ROA를 생성해야 합니다. AS0은 AS 경로에 나타날 수 없으므로 접두사 공지가 무효화됩니다.

- 동일한 접두사를 시작하는 ASN이 여러 개 있는 경우 각 ASN에 대해 해당 접두사에 대한 ROA를 생성해야 합니다. 따라서 라우터에 동일한 접두사에 대한 여러 ROA가 있는 경우 둘 중 하나와 일치하는 BGP 광고가 유효합니다. 동일한 접두사에 대한 여러 ROA는 서로 충돌하지 않습니다.
- 'A'가 고객 'B'에 대한 접두사를 생성하고 'B'를 대신하여 해당 접두사에 대한 ROA를 생성하는 경우, 'A'는 'B'의 ASN을 알림에 앞에 붙이거나 'B'가 접두사 자체를 시작하도록 해야 합니다.

XR BGP 라우터에 대한 RPKI의 성능 영향

Route-Policy를 사용하는 CPU에 대한 ROA 업데이트 효과

ROA가 업데이트되고 라우터에 "validation-state is"가 포함된 인접 디바이스에 대한 로컬 인그레스 경로 정책이 있는 경우, 업데이트된 새 ROA를 기반으로 접두사의 상태를 다시 검증하는 것이 중요합니다. 이는 라우터가 피어에 BGP REFRESH 요청을 전송함으로써 수행됩니다.

BGP 네이버가 표시된 대로 이 메시지를 수신하면 네이버가 접두사를 다시 보내고 인바운드 route-policy가 수신 접두사를 재검증할 수 있습니다.

```
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
```

ROA가 업데이트될 때마다 많은 인접 디바이스가 동시에 새로 고쳐지면 문제가 증폭됩니다. 네이버 인바운드 경로 정책이 복잡하고 많은 처리가 필요한 경우 ROA 업데이트 후 몇 분 동안 높은 CPU 결과가 발생합니다. 인접 디바이스 인바운드 route-policy에 "validation-state is" 명령이 포함되지 않은 경우 이러한 REFRESH 메시지가 발생하지 않습니다.

인접 디바이스에 대해 "soft-reconfiguration inbound always"가 구성된 경우 BGP REFRESH 메시지는 전송되지 않지만 동일한 경로 정책이 동일한 속도로 실행되며 동일한 CPU 사용량을 기대할 수 있습니다.

아래 6.2.2에 설명되어 있는 이유로 경로 정책 구성보다는 'bgp bestpath origin-as use validity' 접근 방식을 선호하는 것이 좋습니다.

ROA 업데이트로 인한 CPU 영향 최소화

여기서 설명하는 문제를 피하는 가장 좋은 방법은 정책에 **있는 검증 상태** 없이 **사용 타당성으로 가장 좋은 경로** 출처를 사용하는 것입니다.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

이 명령은 수신된 유효하지 않은 경로를 라우터에 유지하지만 최상의 경로가 되지 않도록 합니다. 설치되거나 더 이상 광고되지 않습니다. 떨어뜨리기만 하면 그만이다. 다음 ROA 업데이트로 인해 유효한 경우, REFRESH가 필요하지 않으며 정책 실행 없이 자동으로 최적 경로를 사용할 수 있게 됩니다.

사용자가 'invalid' 접두사를 허용하고 사용하지 않으려는 경우, **best path origin-as use validity** 외에도 **best path origin-as allow invalid 컨피그레이션**을 사용합니다.

이 경우 ROA가 변경되면 REFRESH 메시지 없이 최상의 경로가 자동으로 업데이트됩니다. 선호하지 않기 위해 경로는 BGP 경로 선택 과정에서 RPKI 유효하지 않은 경로가 동일한 대상에 대한 다른 경로보다 덜 선호되는 것으로 간주됨을 의미합니다. 가중치 또는 로컬 선호도를 0보다 작게 지정하는 것과 비슷합니다.

RPKI invalid 수가 상대적으로 적고 표에 보관해도 리소스에 큰 영향을 미치지 않습니다.

> **참고**: "bestpath origin-as use validity"를 사용하려면 IBGP 경로를 비롯한 경로의 모든 경로에 올바른 RPKI 유효성이 있어야 합니다. 그렇지 않은 경우 route-policy에서 validation-state 테스트를 계속 사용할 수 있습니다.

IBGP 경로는 라우터에서 ROA 데이터베이스에 대해 검증되지 않습니다. IBGP 경로는 RPKI 확장 커뮤니티에서 RPKI 유효성을 얻습니다. 이 확장 커뮤니티 없이 IBGP 경로를 수신하는 경우 해당 검증 상태가 not-found로 설정됩니다.

BGP RPKI 메모리 공간

각 ROA는 인덱스 및 데이터에 대한 메모리를 사용합니다. 두 ROA가 동일한 IP 접두사에 대한 것이지만 max_len이 다르거나 다른 RPKI 서버에서 받은 경우, 동일한 인덱스를 공유하지만 별도의 데이터가 있습니다. 메모리 오버헤드가 일정하지 않으므로 메모리 요구 사항이 달라질 수 있습니다. 10%의 초과 예산이 권장됩니다. 64비트 플랫폼은 32비트 플랫폼보다 각 메모리 개체에 더 많은 메모리가 필요합니다. 인덱스 객체 및 데이터 객체의 IOS-XR 메모리 사용량(바이트)이 테이블에 있습니다. 대부분 일정한 오버헤드가 그 수치에 포함된다.

	32비트 플랫폼(바이트)	64비트 플랫폼(바이트)
IPv4 인덱스	74	111
IPv6 인덱스	86	125
데이터	34	53

이 섹션에서는 ROA가 메모리를 사용하는 방법을 설명하는 두 가지 시나리오를 다룹니다.

시나리오 1. 라우터에 3개의 RPKI 서버 구성

64비트 라우트 프로세서에서 각각 200,000개의 IPv4 ROA 및 20,000개의 IPv6 ROA를 제공하는 3개의 RPKI 서버를 사용하는 라우터를 고려할 때 다음 메모리가 필요합니다.

20000 * (125 + 3*53) + 200000 * (111 + 3*53)바이트 = 5,968만 바이트

메모리를 계산하는 동안 서로 다른 3개의 유효성 검사기에서 동일한 접두사에 대한 ROA가 동일한 인덱스 값을 공유했습니다.

시나리오 2. 라우터에 구성된 단일 RPKI 서버

ROA 없는 BGP 프로세스 메모리:

```
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
```

BGP 프로세스에서 ROA 없이 25MB 메모리를 사용하는 것으로 나타났습니다.

ROA를 사용하는 BGP 프로세스 메모리:

```
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
```

BGP 프로세스에서 ROA 없이 25MB 메모리를 사용하는 것으로 나타났습니다.

ROA를 사용하는 BGP 프로세스 메모리:

```
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
```
Cisco 8000 라우터는 64비트 OS를 실행합니다. IPv4 ROA172796 ROA를 받고 ROA28411 받았습니다.

메모리(바이트) = 172,796 x [111(인덱스) + 53(데이터)] + 28411 x [125(인덱스) + 53(데이터)].

이러한 계산은 ~27MB를 제공하며, 이는 약 위 라우터의 메모리에서 확인된 증가분입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.