Lumen now offers Resource Public Key Infrastructure (RPKI) on our global AS3356 Internet Core

1/26/2021

What is RPKI?

Resource Public Key Infrastructure **(**RPKI) is a framework intended to secure internet routing infrastructure and prevent route hijacking and other routing inconsistencies associated with Border Gateway Protocol (BGP). RPKI provides a way to connect IP prefixes to a trust anchor. Using RPKI, legitimate holders of IP prefixes can control the operation of Internet routing protocols to prevent route hijacking and other attacks.

Authorization at the Regional Internet Registry (RIR) level allows IP space holders to create Route Origin Authorizations (ROAs) enabling IP Address holders to specify which ASNs are authorized to originate their IP prefixes. Using cryptographically verifiable statements, RPKI helps to ensure that Internet IP Address resource holders are certifiably linked to those resources.

Why is Resource Certification necessary?

The Internet infrastructure was built based on mutual trust between service providers to ensure advertised routes are safe, accurate and will not be maliciously altered. Although that model proved sufficient in the earlier days for Internet development, it has become increasingly vulnerable to configuration mistakes or abuse and attack by malicious actors looking to redirect routes to achieve criminal objectives. This is called BGP Hijacking or IP Hijacking.

Resource Certification enables IP holders to specify which Autonomous Systems (ASNs) are authorized to originate their IP prefixes in BGP announcements. IP Service providers can use RPKI to validate IP route announcements at peering points to help ensure valid announcements are permitted and invalid announcements are dropped.

How does RPKI work?

Owners of IP address space can publish a ROA with an RIR which specifies the originating ASN and IP prefix length permitted. RPKI then attempts to validate these by checking the originating ASN and the prefix length against the ROA. This is also known as BGP Route Origin Validation (ROV).

Lumen uses RPKI route-validation on all BGP sessions for both customers and peers. Lumen's RPKI validation servers download all the ROAs, examines them, and then sends the tables to routers which are then able to determine the validity of an IP prefix. IP Prefixes are tagged with one of three labels after checking the ROA.

"Valid" – IP Prefix has positive match against ROA. IP Prefix permitted.
"Invalid" – IP Prefix does not match ROA (whether by invalid prefix length or invalid origin ASN). IP Prefix dropped.
"Unknown" – IP Prefix is not in ROA. IP Prefix permitted.

When will RPKI be enabled on the Lumen AS3356 Internet Core?

RPKI is already configured on the AS3356 Internet Core, however Lumen is implementing a phased grace-period approach.

- Phase 1 – Enable "mark-only" on all peers (current)
- Phase 2 – Enable "mark-only" on all customers (January 2021)
- Phase 3 – Enable "drop" on invalids for all peers (March 2021)
- Phase 4 – Enable "drop" on invalids for all customers (March 2021)

(Above dates subject to change)

During the grace period, customers may use the Lumen Looking Glass - https://lookingglass.centurylink.com to validate how their IP Prefixes are being marked in the Lumen network:

```
community "rpki-valid" members "3356:901"
community "rpki-invalid" members "3356:902″
community "rpki-unknown" members "3356:903"
```

***NOTE:** "3356:902"for "rpki-invalid" will only be visible in the looking glass during the "mark-only" phase. Once Lumen begins dropping "invalids", this community would no longer be visible in the looking glass. Following the grace period, if you suspect your prefix is being dropped due to an "invalid" tag, you could use the looking glass to see if there is a "3356:901" or "3356:903" community tag for the prefix in question. If not, then likely the prefix is tagged as "invalid" and being dropped.

How can customers establish ROAs?

For IP space owned by a customer, ROAs must be established with any one of the 5 RIR (Regional Internet Registries):

- ARIN (North America) – https://www.arin.com
- RIPE (Europe) – https://www.ripe.net
- APNIC (Asia Pacific) – https://www.apnic.com
- AFRINIC (Africa) – https://www.afrinic.net
- LACNIC – (Latin America and Caribbean Nations) – https://www.lacnic.net

For IP space owned by Lumen and loaned to customers, ROAs must be established by Lumen on behalf of the customer. Requests to have Lumen establish ROAs for customers can be made by emailing ipadmin@centurylink.com. In the email body, please provide authorized prefix and max length, originating ASN, and a valid circuit ID.

Do customers need to order RPKI?

RPKI is enabled and active on the Lumen AS3356 global IP network for both peering and customer BGP sessions. As a result, there is no requirement or process to "order" RPKI – as it is already "on".

- Customers who have existing established ROAs will immediately receive BGP Route Origin Validation via RPKI from Lumen.
- Customers who establish new ROAs will receive BGP Route Origin Validation once the ROA is completed.
- Customers who do not have ROAs will not be impacted and BGP route announcements will operate as normal—(unless that route announcement is owned by another customer with a ROA only permitting their origin ASN).

RPKI is "on" and active in the Lumen AS3356 Internet Core and is not an option to turn off or deactivate. All external customer and peering sessions will be validated. We will not make exceptions and allow special un-verified sessions.

What is the impact to Lumen® DDoS Mitigation customers?

To redirect IP traffic to DDoS scrubbing centers, Lumen makes BGP route announcements for IP prefixes to be redirected. If these IP prefixes are registered via RPKI and Lumen does not have a Route Origin Authorization (ROA) to originate advertisements for the DDoS protected IP address space, then service providers that are enforcing RPKI will drop the route announcement. This means that some or all traffic, depending on which path the traffic takes from the originator to the protected infrastructure, will not be redirected to and mitigated by Lumen's DDoS Mitigation. For further information on RPKI and Lumen DDoS, please reference lumen.com/content/dam/lumen/help/globalview/frequently-asked-questions-about-rpki.pdf

Frequently asked questions

Q: Are ROA entry prefix lengths an "up to" format like normal BGP IRR filters?

A: No, ROA prefix lengths are exact matches to what is established in the ROA, e.g. if a customer establishes a ROA for a /22 and then proceeds to announce those via BGP in 4 separate /24 blocks, those would be labeled as "invalid" and subsequently dropped. Customers MUST get their ROA accurate and take into consideration any additional subnet advertisements they may want to announce -and if there are more specifics, account for those using the max length attribute or a separate specific ROA.

Q: If I do not establish a ROA will my IP Prefixes be impacted?

A: No. Lumen will only act on "invalid" tags against a ROA. If no ROA exists, IP prefixes will fall into the "unknown" category (3356:903) and will work as normal.

Q: Can Lumen fix customer ROAs if a mistake is made?

A: Only the owner of the IP prefix can fix a ROA in the event a mistake is made or a change is needed. If the IP block is owned by Lumen and loaned to the customer for use, then only Lumen would be able to change that ROA.

Q: Can a ROA list multiple origin ASNs for BGP Prefixes?

A: Yes, it is perfectly acceptable to have multiple ROA origination ASNs for same blocks, e.g. if a customer has a DDoS service and needs Lumen to announce a subnet, the customer will need to issue another ROA giving Lumen permission to also be an ORIGIN ASN for that specific IP block to be advertised.

Q: Will Lumen “whitelist” or “override” invalid IP Prefixes?

A: No, Lumen will not support white-listing or overriding of “invalid” IP Prefixes.

Q: How can I validate if my ROA is legitimate?

A: Any one of the 5 RIRs have resource links that will allow customers to view if their prefixes have legitimate ROAs. In particular RIPE and APNIC have useful ROA validators: https://rpki-validator.ripe.net/roas and https://rpki-validator.apnic.net/roas

Q: What makes an IP Prefix “invalid”?

A: An “invalid” prefix is due to one of two reasons. 1) Improper subnet mask. 2) Improper origin ASN.

Q: What is the risk of not having a ROA for my IP Prefixes?

A: Not establishing ROAs puts customers prefixes at risk to bad actors or hijacking of IP space.

Q: Where can I go for additional information on Lumen RPKI policies?

A: For additional information on Lumen RPKI, you can email rpkisupport@centurylink.com

* DISCLAIMER: This information is provided for informational purposes only. It is not intended to amend any contractual terms between Lumen and customer. Nothing in this document modifies any right or obligation under your agreement with Lumen, nor is anything contained herein intended to constitute a warranty. Lumen reserves the right to modify this guide from time to time.

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.