A Profile for Mapping Origin Authorizations (MOAs)

Chongfeng Xie	China Telecom
Guozhen Dong	China Telecom
Xing Li	CERNET Center/Tsinghua University
Geoff Huston	APNIC
Di Ma	ZDNS

sidrops@IETF 123， July 2025

Overview

- This is about a new digitally signed object of RPKI, it is used for the verification of the address mapping announcement in multi-domain IPv6-only underlay network.

- It was adopted by SIDROPS WG October 2024 , the current version is -02.

Scenario

- For IPv4 service delivery in IPv6-only network(proposed in [*draft-ietf-v6ops-framework-md-ipv6only-underlay*]), IPv6 mapping prefixes are configured at the PE to identify the location of each IPv4 network. So IPv6 mapping prefix is considered as the **mapping origin** of given IPv4 address block.

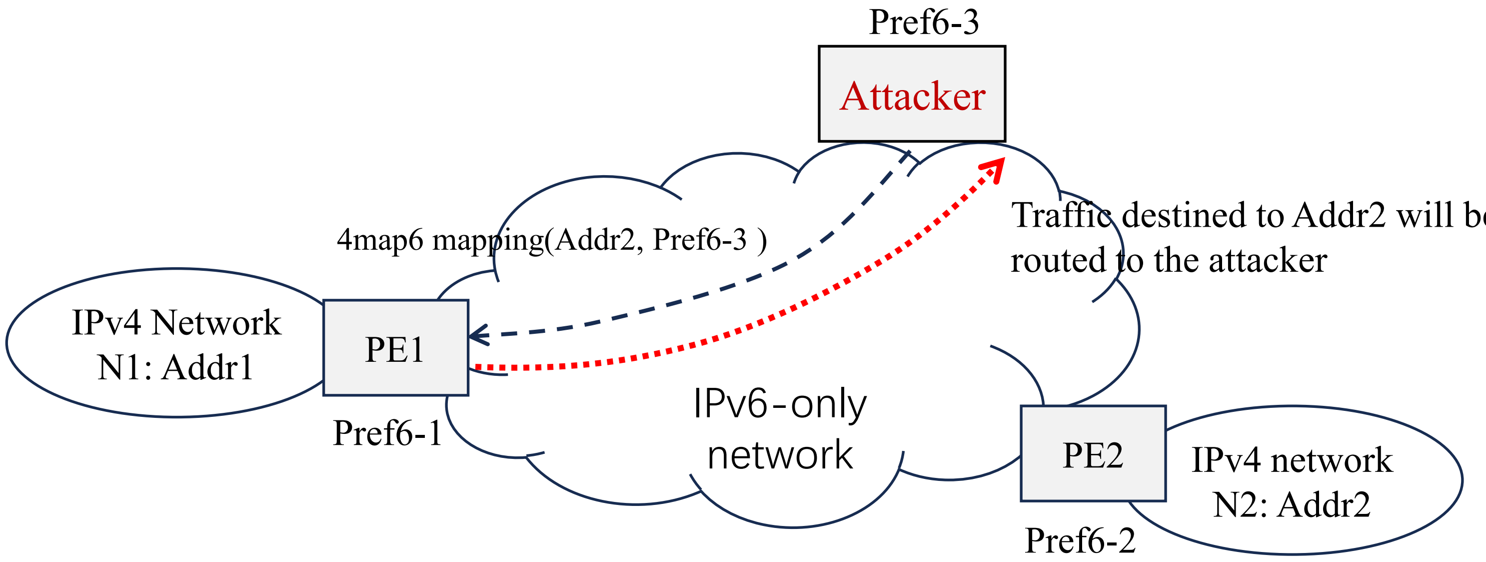
IPv4 address block
IPv6 mapping prefix

```
IPv4 A1          +--------+        +-+      +--------+        IPv4 A2
 +--------+     /   AS1    \     /AS2\    /   AS3    \      +--------+
|  IPv4   |    |+--++  +--+| |  |+--+ |  | +--+  +-+-+ |    |  IPv4    |
| network 1|---||PE1|--|P1 |-|--||P2|-|--|-|P3|--|PE2|-|---| network 2|
 +--------+    |+---+  +--+| |  |+--+ |  | +--+  +---+ |    +--------+
                \__________/     \___/    \__________/
```

- [*draft-ietf-idr-mpbgp-extension-4map6*] defines MP-BGP extension, i.e. 4map6, for announcing the mapping relation from egress PE to ingress PE.

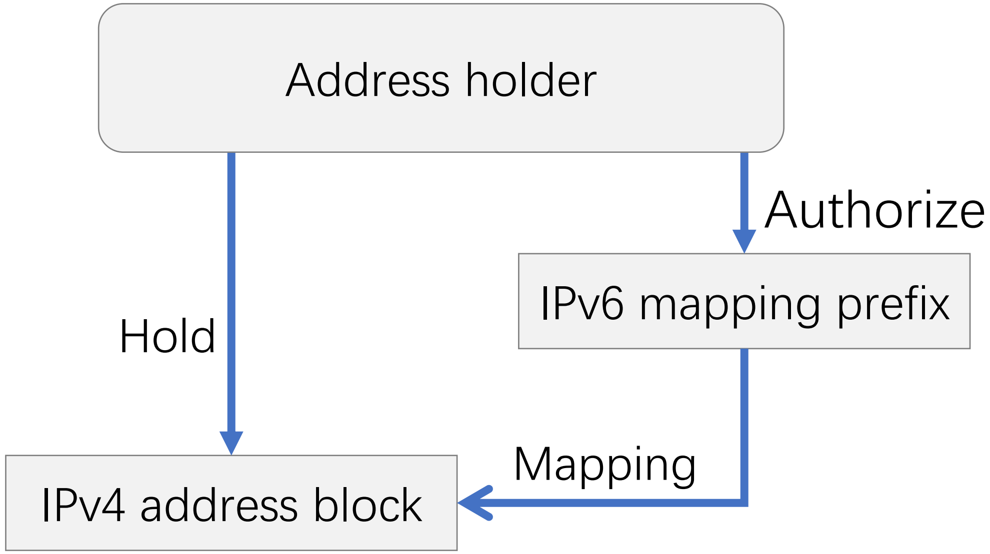
Problem statement

- The validity of transmitting IPv4 service data in IPv6-only underlay network relies on the authenticity of the mapping origin of the IPv4 address block.
- If an attacker maps an IPv4 address block using a fake IPv6 mapping prefix, IPv4 service data will be routed through the attacker-controlled route and reach to the wrong egress PE, resulting in a situation of IPv4 prefix hijacking.



Mapping Origin Authorization (MOA)

- This approach leverages RPKI architecture to verify the authenticity of the mapping origin of IPv4 address.
- MOA is a cryptographically signed binding between an IPv4 address block and its right IPv6 mapping prefix that is allowed to be declared in BGP announcement.
- With MOA, a legitimate holder of an IPv4 address block, e.g. an ISP, can authorize an IPv6 mapping prefix to map the IPv4 address block.



The MOA eContent

The content-type for a MOA is defined as MappingOriginAuthz and has the numerical value of x.x.xxx.xxxxx.x.x.x.x.xx.

ASN.1 format of MOA

```
MappingOriginAttestation ::= SEQUENCE {
   version [0] INTEGER DEFAULT 0,
   mappings SEQUENCE (SIZE(1..MAX)) OF MOAIPMapping }

MOAIPMapping ::= SEQUENCE {
   v6MappingPrefix IPv6MappingPrefix,
   v4Prefixs SEQUENCE (SIZE(1..MAX)) OF IPv4Prefix }

IPv6MappingPrefix ::= BIT STRING (SIZE (0..ub-IPv6))

IPv4Prefix ::= BIT STRING (SIZE (0..ub-IPv4))

ub-IPv6 INTEGER ::= 128
ub-IPv4 INTEGER ::= 32
```

MOA Validation

- Before a relying party uses a MOA to validate a mapping announcement, the relying party MUST perform all the validation checks specified in [RFC6488] as well as the additional MOA-specific validation step.

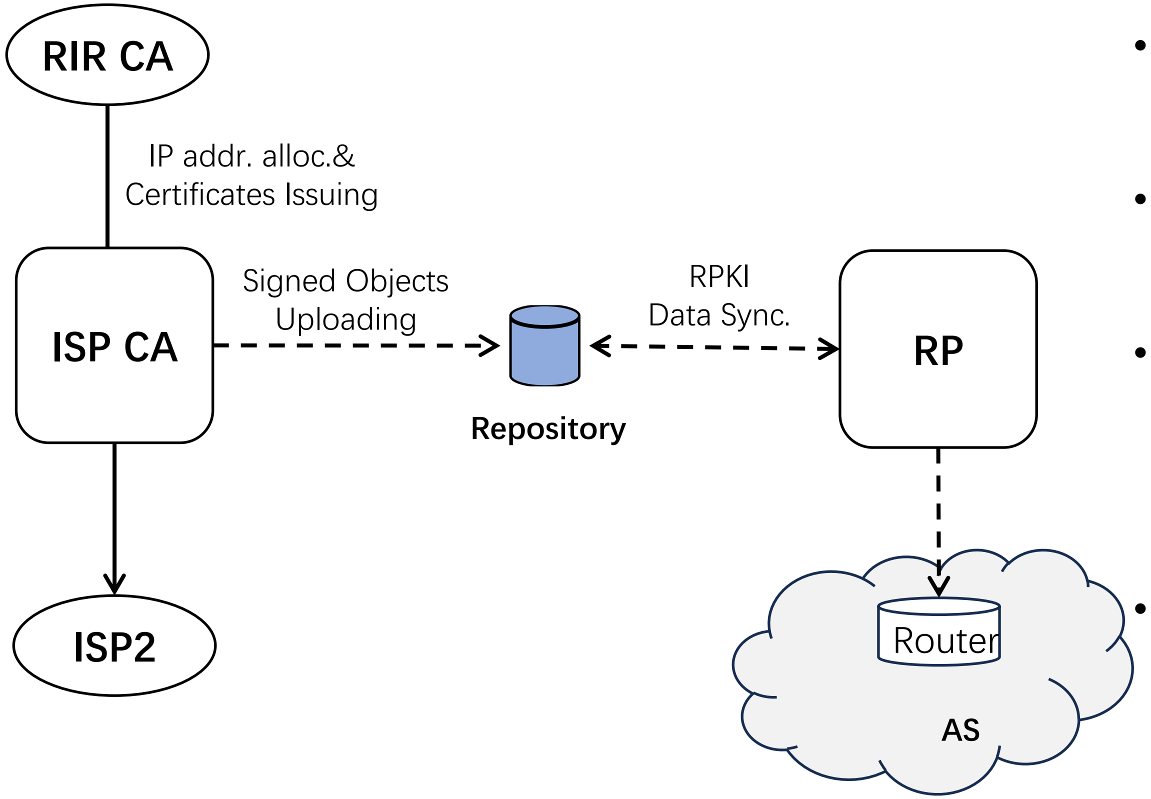
Draft update

- draft-ietf-idr-mpbgp-extension-4map6 is moved from Normative reference to Informative reference.

Major Functional Components

Signing Process of ISP CA

- Confirm that a CA certificate has been received from the upstream CA
- Use this CA certificate to issue an EE certificate containing an IPv6 address prefix
- Use the EE certificate to issue a digital object containing the IPv6 address prefix and a set of IPv4 address prefixes;
- Encapsulate the EE certificate and this digital object into a single MOA file and upload it to the **Repository**



Verification Process of RP

- Build a certificate chain from EE certificate embedded in MOA to TA certificate
- Verify the legality and validity of all certificates on the certificate chain
- Verify whether the IPv6 Mapping Prefix and IPv4 address prefixes in MOA are included in each certificate in the certificate chain
- Obtain<IPv6 Mapping Prefix, [IPv4 address block]>binding relationships

Status of System Implementation

- The MOA certificate can be successfully issued on the CA side

```
ContentInfo  SEQUENCE  (2 elem)
  contentType  ContentType  OBJECT IDENTIFIER  1.2.840.113549.1.7.2  signedData  (PKCS #7)
  content  [0]  (1 elem)
    SignedData  SEQUENCE  (5 elem)
      version  CMSVersion  INTEGER  3
      digestAlgorithms  DigestAlgorithmIdentifiers  SET  (1 elem)
        DigestAlgorithmIdentifier  SEQUENCE  (1 elem)
          algorithm  OBJECT IDENTIFIER  2.16.840.1.101.3.4.2.1  sha-256  (NIST Algorithm)
      encapContentInfo  EncapsulatedContentInfo  SEQUENCE  (2 elem)
        eContentType  ContentType  OBJECT IDENTIFIER  1.2.840.113549.1.9.16.1.24  routeOriginAttest  (S/MIME Content Types)
        eContent  [0]  (1 elem)
          OCTET STRING  (33 byte) 301F020100301A300B0309002001000002000100300B0304006E70710303000A01
            SEQUENCE  (2 elem)
              INTEGER  0
              SEQUENCE  (2 elem)
                SEQUENCE  (1 elem)
                  BIT STRING  (64 bit) 0010000000000001000000000000000000000010000000000000000100000000
                SEQUENCE  (2 elem)
                  BIT STRING  (24 bit) 011011100111000001110001
                  BIT STRING  (16 bit) 0000101000000001
```

V6MappingPrefix: "2001:0:200:100::/64“

V4Prefixes: {"110.112.113.0/24", "10.1.0.0/16"}

Next Steps

- Implement MOA certificate parsing and verification on the RP (Relying Party) side. Implement end-to-end verification of system functions and conduct a full demonstration.
- Design the protocol between RP and Router.
- Make further refinement to improve the document. Comments and suggestions are welcome,

Thank you！

Q&A