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 120 July 2024

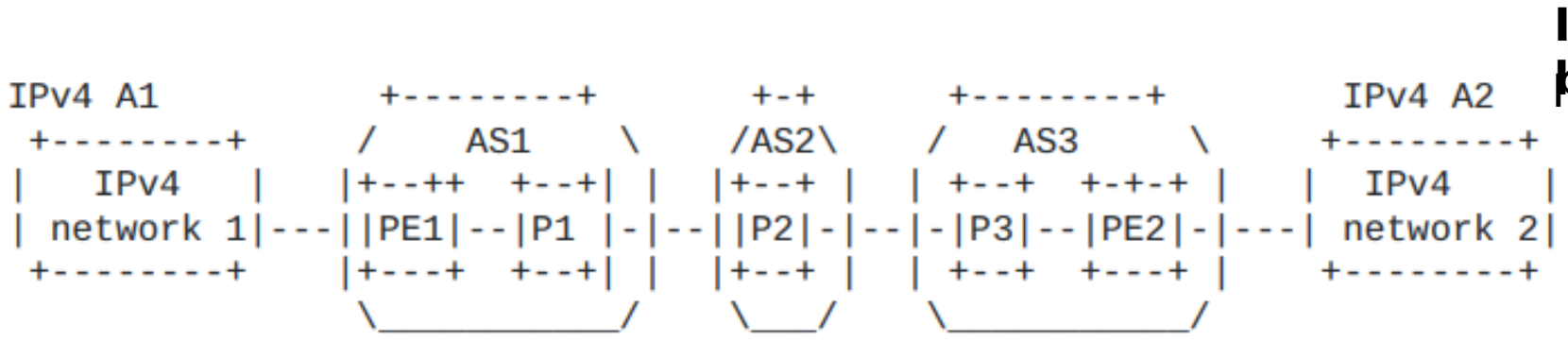
Overview

- 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 firstly submitted to SIDROPS before IETF 119 , the current version is -04.

Scenario

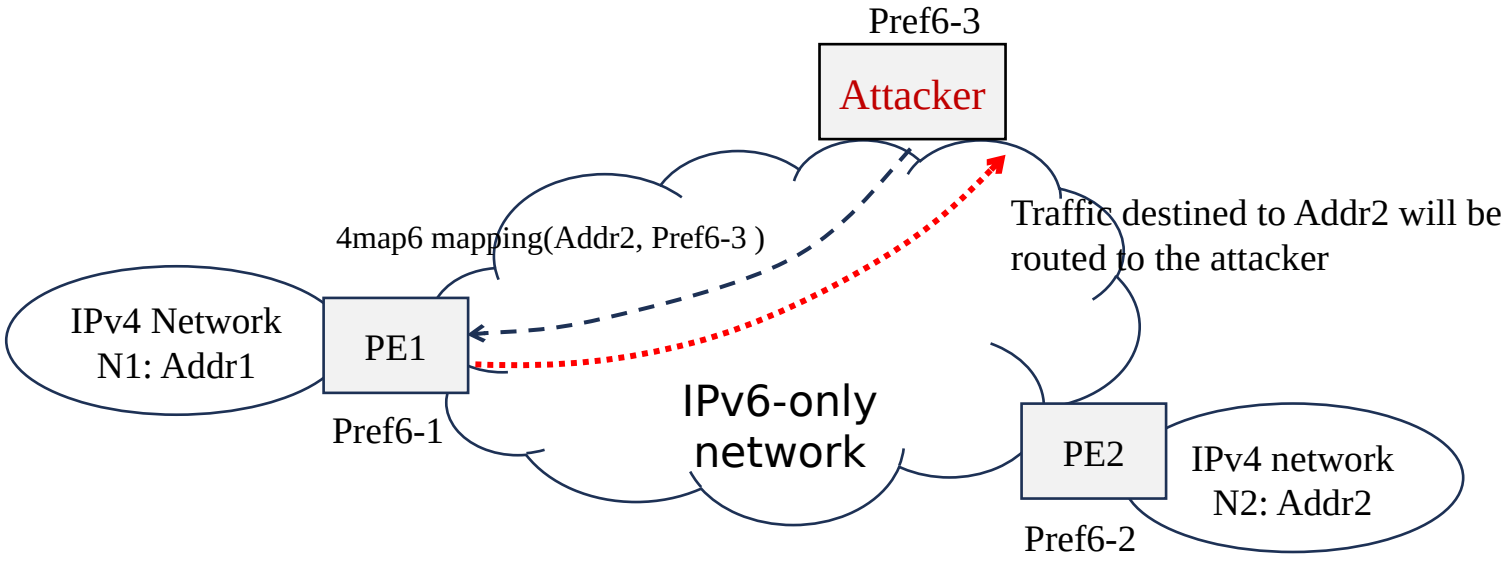
- For IPv4 service delivery in IPv6-only network(proposed in [*draft-ietf-v6ops-framework-md-ipv6only-underlay*]), IPv6 mapping prefixes are configured at the PE to identify the location of each IPv4 network. So IPv6 mapping prefix is considered as the **mapping origin** of given IPv4 address block.



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

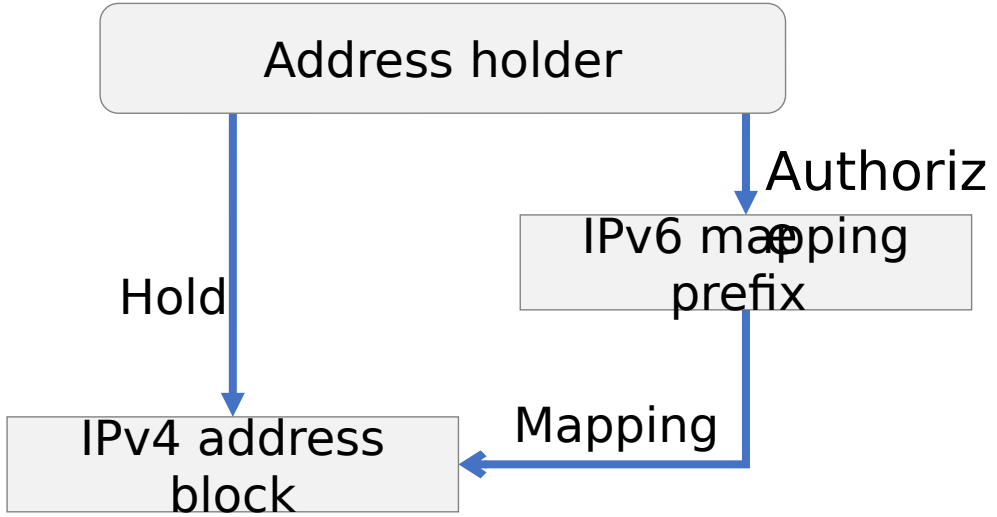
Problem statement

- The validity of transmitting IPv4 service data in IPv6-only underlay network lies 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.

Based on the comments of Russ Housley and Job Snijders, the ASN.1 format of MOA is revised as below,

```
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.

Comments and Contributions Received

- Job Snijders
  - Give several improvements to MOA eContent.
  - Add the definition of canonical ordering of v4Prefixs, which will allow RP software to more easily verify the contents of the eContent.
  - Propose to replace RFC6482 by RFC9582, in the reference section.
- Russ Housley
  - Give a new version of ASN.1 module and one significant enhancement, which allows for several IPv6 prefixes, and each of them is mapped to a list of IPv4 addresses.
- Geoff Huston and Di Ma joined as co-authors

Next Steps

- Comments and suggestions are welcome, and further refinement will be made to improve the document.
- Authors would like to ask for WG adoption of this document.

Thank you
Q&A