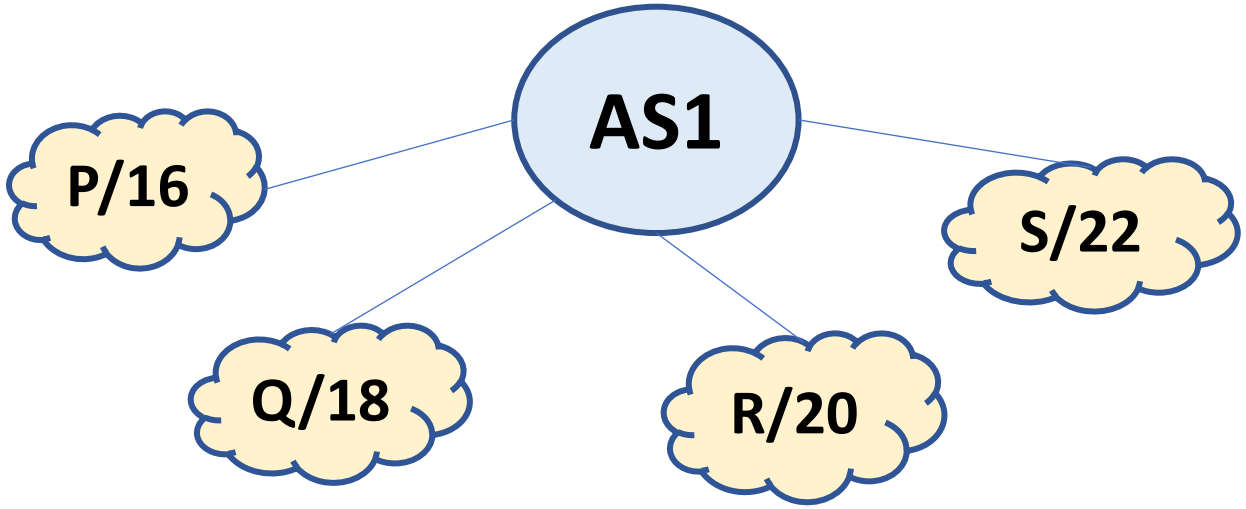
Design Analysis of RPKI PrefixList and Operational Considerations

K. Sriram
(with J. Snijders, D. Montgomery)

IETF SIDROPS Meeting
November 2023

RPKI PrefixList Object

Asserts that the listed set of prefixes includes **all prefixes** originated or intended to be originated by the listed (signing) AS.



Example:

RPKI PrefixList object: AS1 {P/16, Q/18, R/20, S/22}

IETF Draft: https://datatracker.ietf.org/doc/draft-ietf-sidrops-rpki-prefixlist/00/

Route Selection Policy Recommendation

A relying party may discard a route if its {Prefix, origin AS} pair is such that the prefix is not included in the PrefixList published by the origin AS.

More Specific Prefixes of an Included Prefix

The draft currently leaves it ambiguous if more specific prefixes of an included prefixes are meant to be allowed or disallowed by the PrefixList.

State-Space of ROV and PrefixList Verification

	ROV	PrefixList Verification	Route Selection
1	Valid	Not Invalid	Accept
2	Valid	Invalid	Reject
3	NotFound	Not Invalid	Accept
4	NotFound	Invalid	Reject
5	Invalid	Not Invalid	Reject
6	Invalid	Invalid	Reject

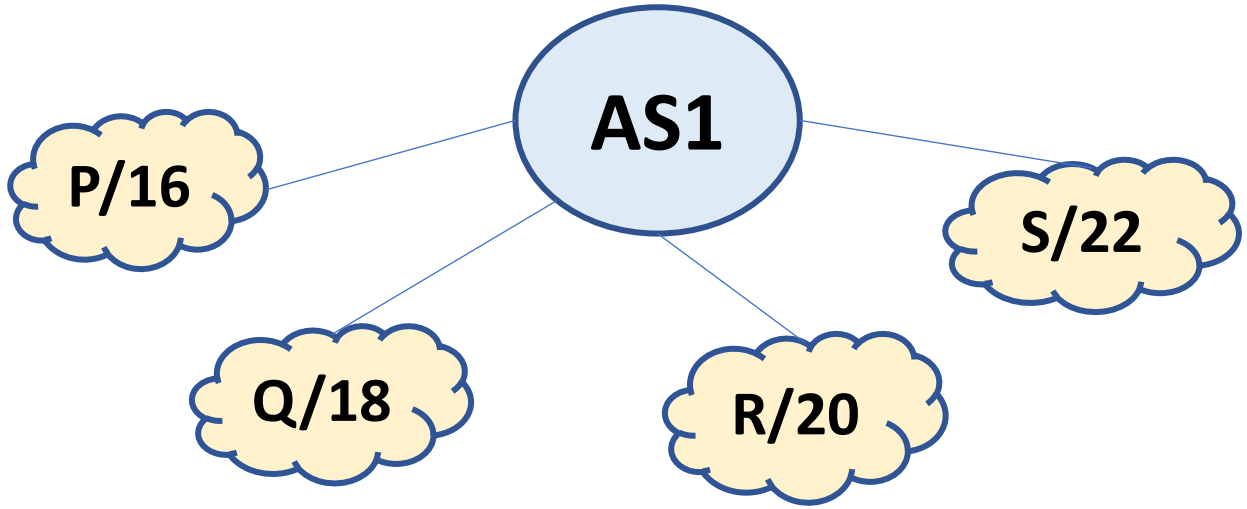
Mitigates AS Abuse together with a Bogus ROA (slide 8)

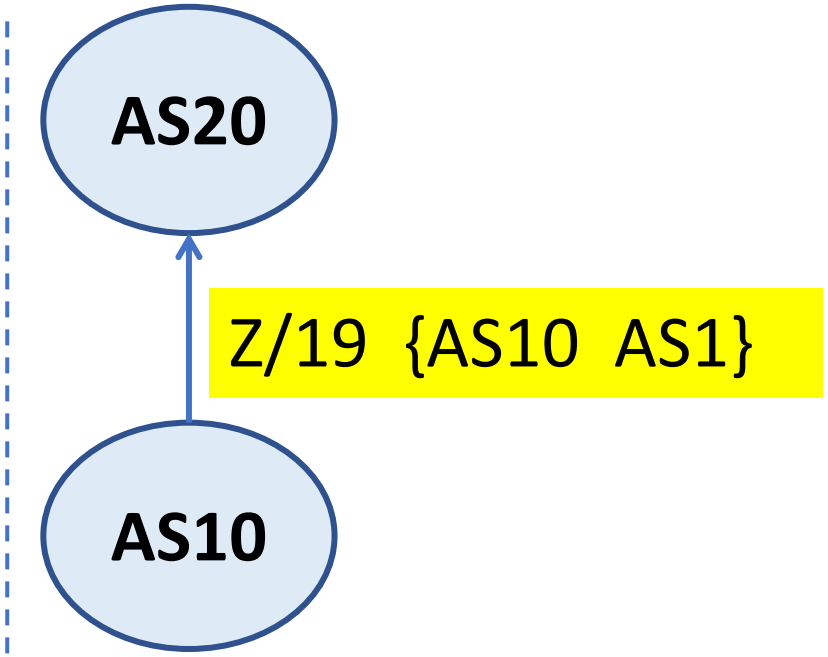
Mitigates AS Abuse while hijacking an ROV-NotFound Prefix (slide 7)

Problems Solved by PrefixList

Problems Solved by PrefixList:

(1) AS Abuse while Hijacking an ROV-NotFound Prefix





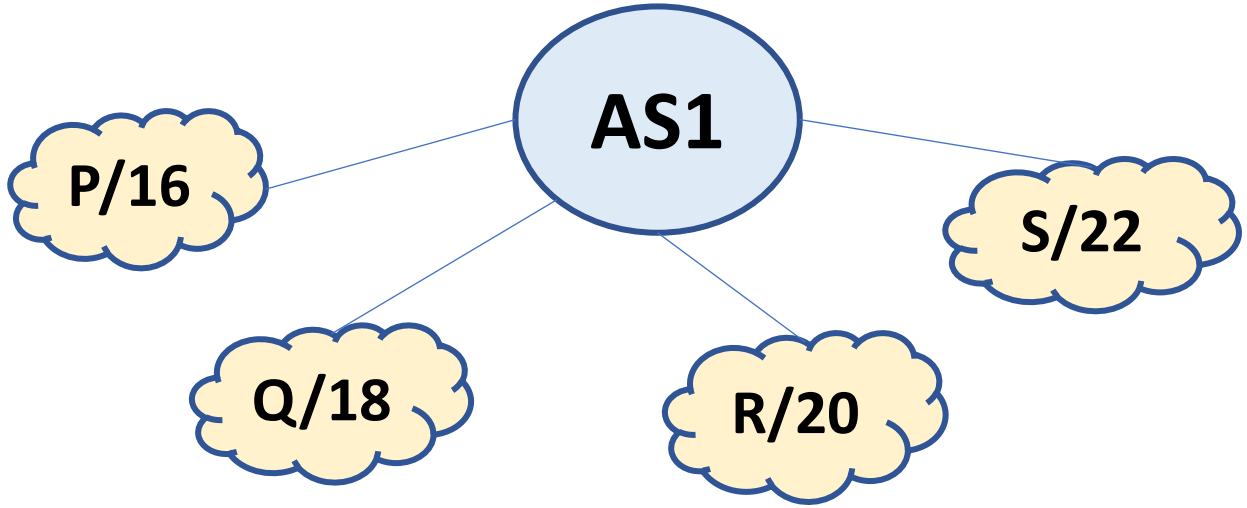
Example:

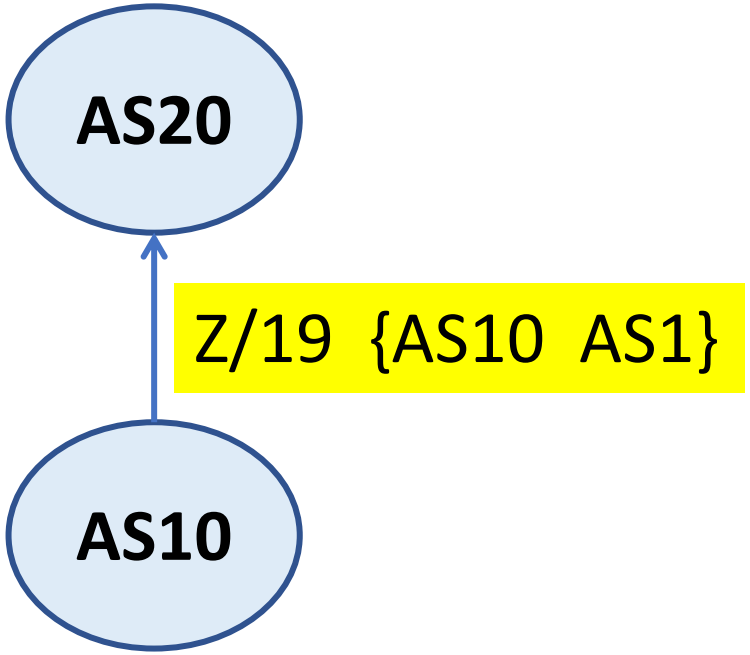
RPKI PrefixList object: AS1 {P/16, Q/18, R/20, S/22}

- AS10 sends prefix Z/19 (unrelated to prefixes originated by AS1) not covered by any ROA but inserts AS1 as the origin AS
- It is an AS abuse or hijack of AS1 by AS10 (harms AS1's reputation)
  - ➢ AS path manipulation
- AS20 detects that the route is ROV-NotFound and Z/19 is not in AS1's PrefixList; hence rejects the route

#4 in the table on slide 5

Problems Solved by PrefixList:
(2) AS Abuse Together with a Bogus ROA





Example:

RPKI PrefixList object: AS1 {P/16, Q/18, R/20, S/22}

- The owner of Z/19 creates a bogus ROA with AS1 as the origin AS
- AS10 is colluding with or could be owning Z/19
- The route Z/19 {AS10 AS1} is RPKI-ROV Valid but PrefixList Invalid -- rejected at AS20

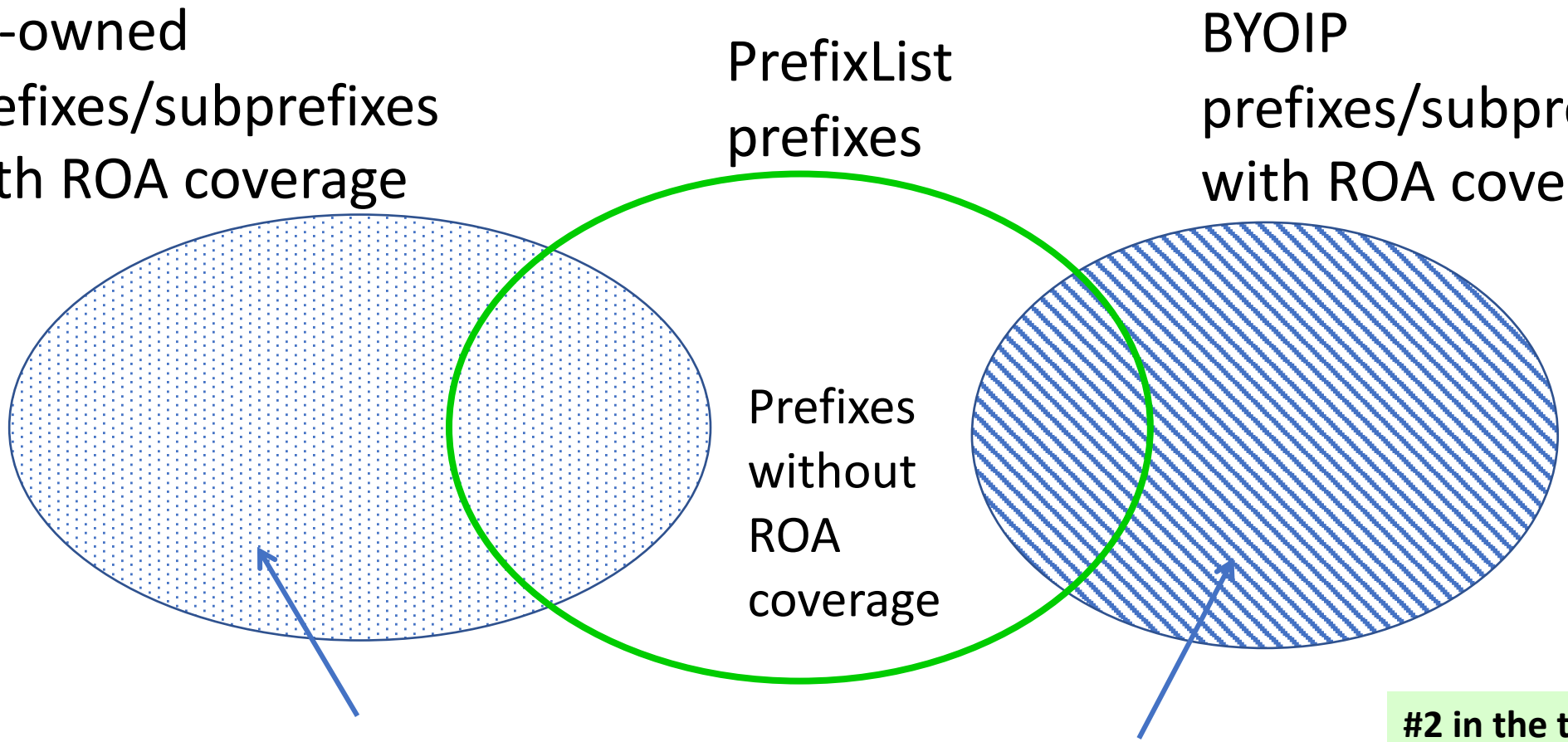
#2 in the table on slide 5

Problems Solved by PrefixList:
(3) AS Accidentally Strips AS_PATH and Mis-Originates Prefixes

- Route leaks of Type 5 in RFC 7908
- E.g., route optimizer malfunction (AS_PATH stripped and leaked)
- These are in effect accidental prefix hijacks by the AS that has created the PrefixList
- If the affected prefixes have ROAs, that helps the receiving ASes in detecting the hijacks
- If not, the PrefixList helps the receiving ASes to detect

#4 in the table on slide 5

Problems Solved by PrefixList:
(4) Reduction of Hijack Attack Surface



#2 in the table on slide 5

Forged-origin prefix hijack attack surface eliminated by PrefixList

Assume: More specific prefixes of an included prefix are considered disallowed by PrefixList (slide 4)

Problems Solved by PrefixList:
(5) AS can declare that it originates no prefixes

- PrefixList can be created with an empty list in it
- By doing this, the AS asserts that it originates no prefixes in the global routing system
- Any route showing this AS as the origin AS is PrefixList Invalid and hence discarded

Operational Considerations

Considerations when Prefix Owner Splits a Prefix

Sequence of events:

1. An existing BYOIP customer wants to split an existing prefix
2. AS operator updates its PrefixList (less-specific prefix stays included)
3. Announces the more-specific prefix but also continues to announce the less-specific prefix (make-before-break principle)
4. Allows time to let the PrefixList propagate through the global RPKI system
5. Withdraws the less-specific prefix (if requested by the owner)

* BYOIP customer updating their ROA can progress independently

Considerations when Prefix Owner has a New Prefix

Sequence of events:

1. An existing BYOIP customer wants to announce a newly acquired prefix
2. They may expect the new prefix announced quickly by the AS (but some wait time is crucial)
3. AS operator updates its PrefixList
4. Allows time to let the PrefixList propagate through the global RPKI system
5. Announces the new prefix and informs the prefix owner

* BYOIP customer updating their ROA can progress independently

Future Readiness for Instantaneous Announcements

- Prefix owner wishes readiness for future instantaneous announcement of some split prefixes
- They include them (more-specific prefixes) in their ROA a priori, and simultaneously inform the AS operator to include them in the PrefixList as well (a priori)
- The split prefixes can be announced any time they are called for

Questions / WG Feedback Items

- Should the draft specify/clarify that more specific prefixes of an included prefix are considered Invalid if announced with the PrefixList AS as the origin AS?
- PrefixList verification outcome in case the route has an AS_SET in the AS_PATH?
- Is a NotFound outcome in PrefixList verification (similar to ROV) useful to include for diagnostics purposes?
- Have separate drafts for PrefixList profile and PrefixList verification/operations?