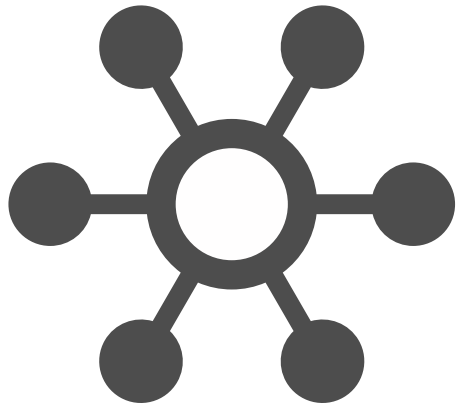
Emerging Route Leak Mitigation Approaches

CORE BACKBONE

CHARACTERISTICS OF ROUTE LEAKS

CORE BACKBONE

- Type 1 - **Hairpin Turn with Full Prefix**
  Prefixes learned from one provider are propagated to another upstream provider
- Type 2 - **Lateral ISP-ISP-ISP Leak**
  Peers propagate more than their own and customer prefixes
- Type 3 - **Leak of Transit-Provider Prefixes to Peer**
  Prefixes learnt from transit provider propagated to peer
- Type 4 - **Leak of Peer Prefixes to Transit Provider**
  Prefixes learnt from peer propagated to transit provider



CHARACTERISTICS OF ROUTE LEAKS

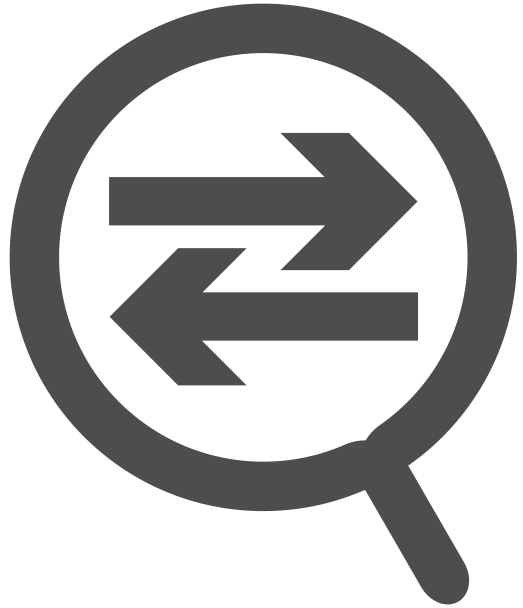
CORE BACKBONE

- Type 5 **- Prefix Re-origination with Data Path to Legitimate Origin**
  Propagation of prefixes learnt from provider to another provider, but as if it being originated by it
- Type 6 - **Accidental Leak of Internal Prefixes and More-Specific**
  Propagation of internal prefixes (often more specifics) to providers or peers

- **Possible Consequences of Route Leaks**
  - Delays
  - Packet Loss
  - Blackholing
  - Eavesdropping / Sniffing

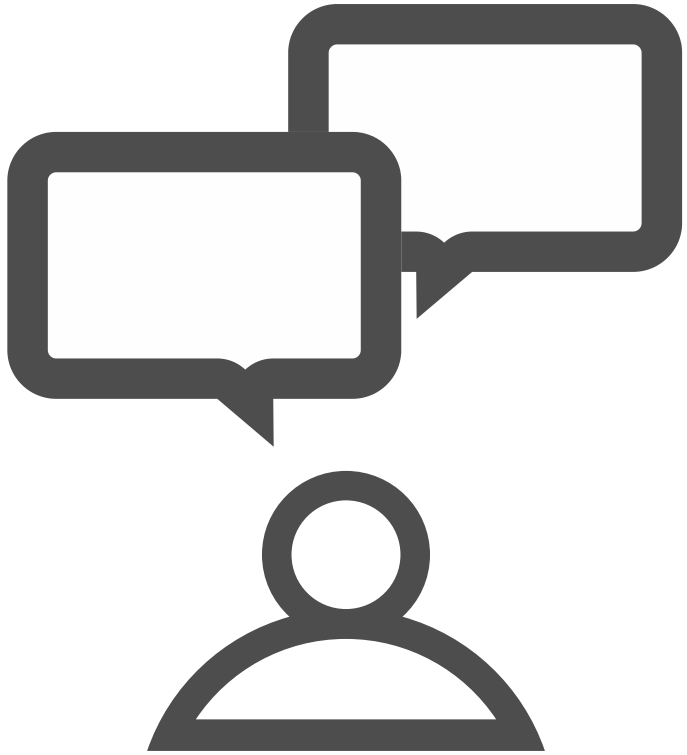
CURRENT ROUTE LEAK APPROACHES

- **RPKI** to filter misoriginations
- Ingress **Filtering** based on **IRR** data and according to best practices
- Egress **Filtering** according to best practices
- **BGP Monitoring** and **Incident Response**
  - Reach out to leaking AS and/or their upstreams
  - Try to announce more preferred routes (e.g. more specifics)



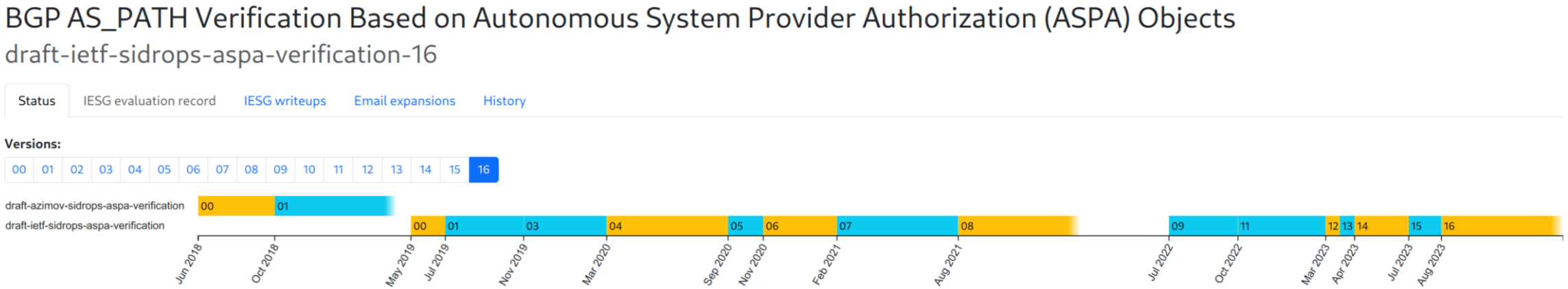
EMERGING ROUTE LEAK MITIGATION APPROACHES

- **Better solutions are required!**
  - Automated Leak Detection and Prevention
- New approaches
  - **ASPA - A**utonomous **S**ystem **P**rovider **A**uthorization
  - **BGP Roles**
  - **Down Only Community**



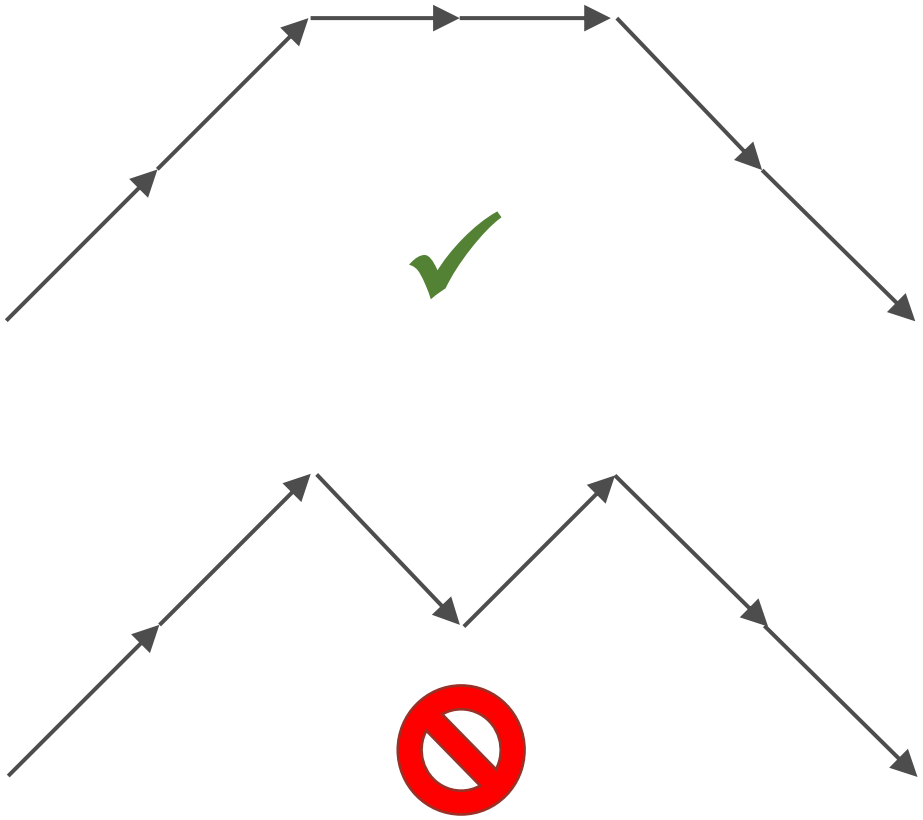
ASPA

- **ASPA: A**utonomous **S**ystem **P**rovider **A**uthorization
  - Verification of AS Path
- Each AS lists all its authorized provider AS numbers in its **ASPA object**
  - Similar to ROAs
  - Cryptograhically signed and distributed using the RPKI ecosystem



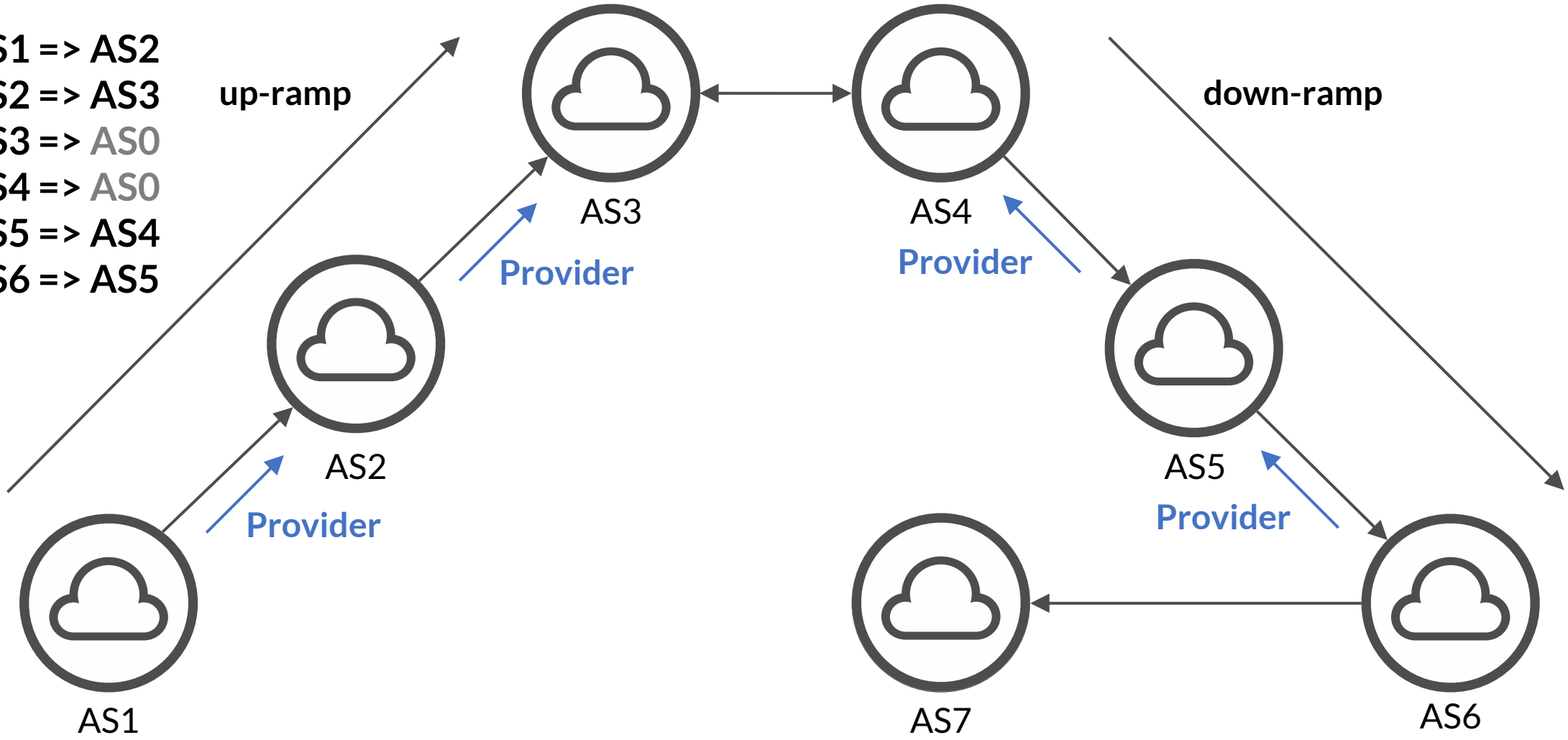
ASPA

- **Full deployment of ASPA**
  - Customer-to-Provider:
    ASPA „forward“ / „up-ramp“
  - Peer-to-Peer: no ASPA
  - Provider-to-Customer:
    ASPA „backward“ / „down-ramp“
- **Valley Free Routing**
- **Partial deployment**
  - AS Path partially matches some „forward“ and „backward“ ASPAs
  - Any other ordering is a policy violation!
- **Validation States:** Valid, Unknown, Invalid



VALID AS PATH – ASPA

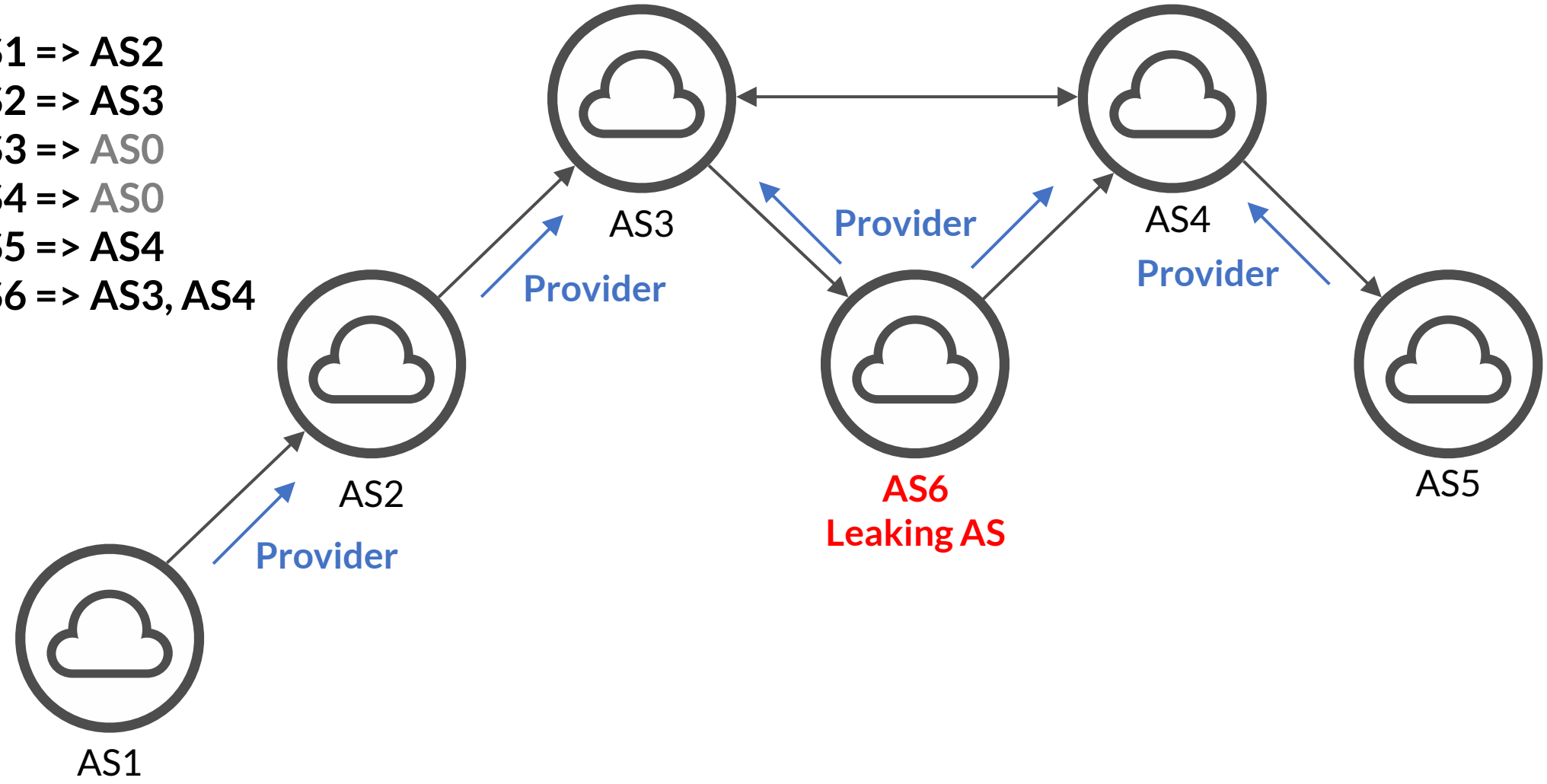
AS1 => AS2
AS2 => AS3
AS3 => AS0
AS4 => AS0
AS5 => AS4
AS6 => AS5



VALID

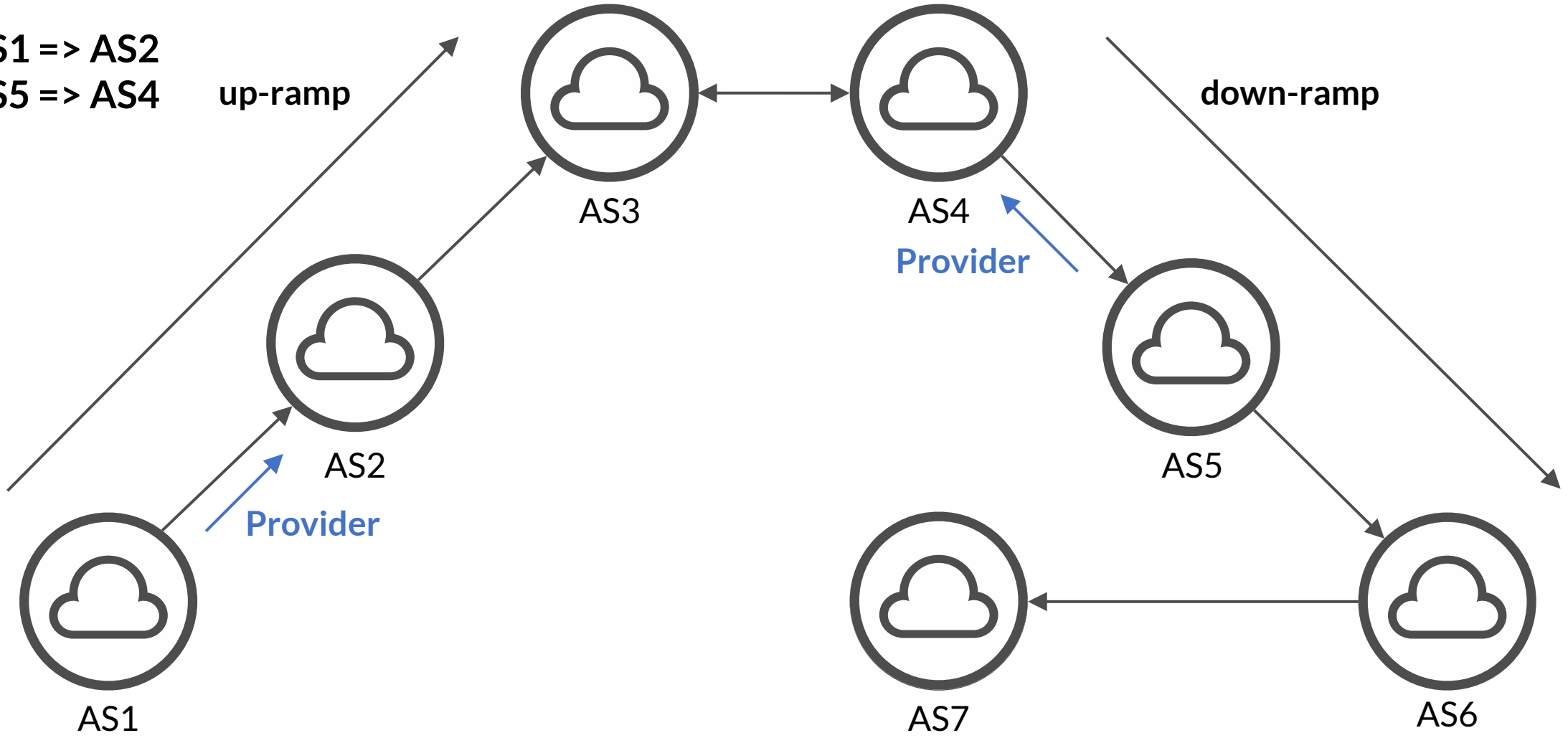
INVALID AS PATH – ASPA

AS1 => AS2
AS2 => AS3
AS3 => AS0
AS4 => AS0
AS5 => AS4
AS6 => AS3, AS4



INVALID

PARTIAL DEPLOYMENT – ASPA

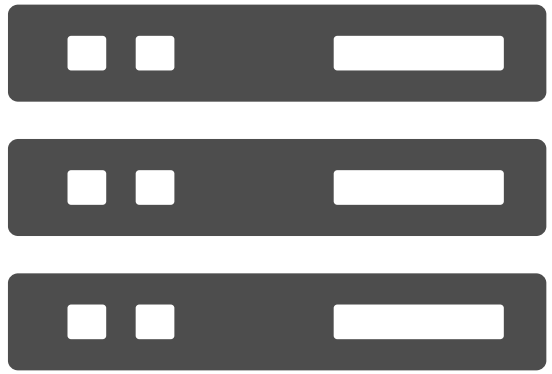


ASPA

CORE BACKBONE

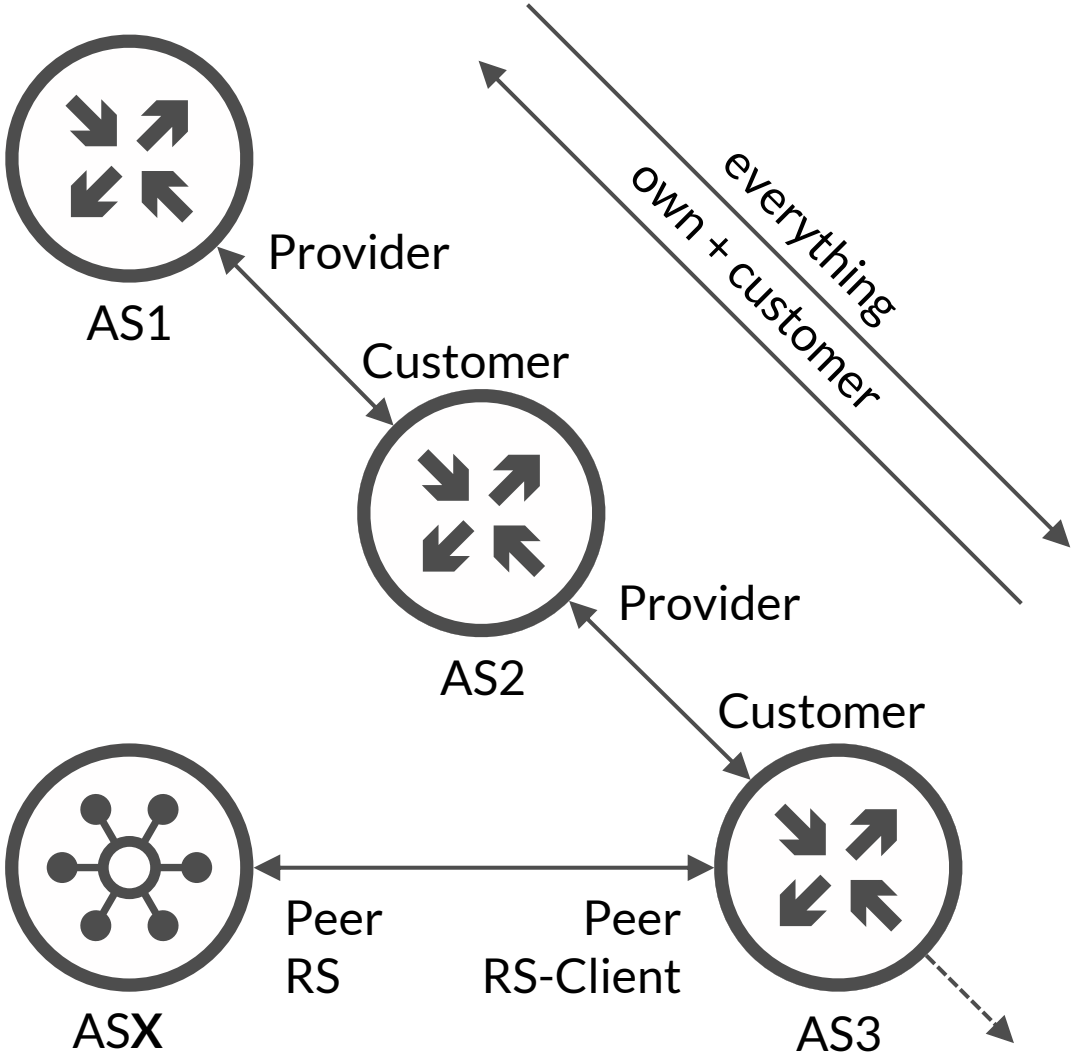
→ Most route leaks are detectable if related ASPA attestations exist

- Lightweight process → offloaded via RTRv2
- Software Support
  - Krill
  - Routinator
  - OpenBGPD
  - rpki-client
- Release of RFC expected for 2024
- Support of first RIRs in the next 1-2 years
- Availability in commercial BGP speaker implementations expected in ~2 years



BGP Roles (RFC9234)

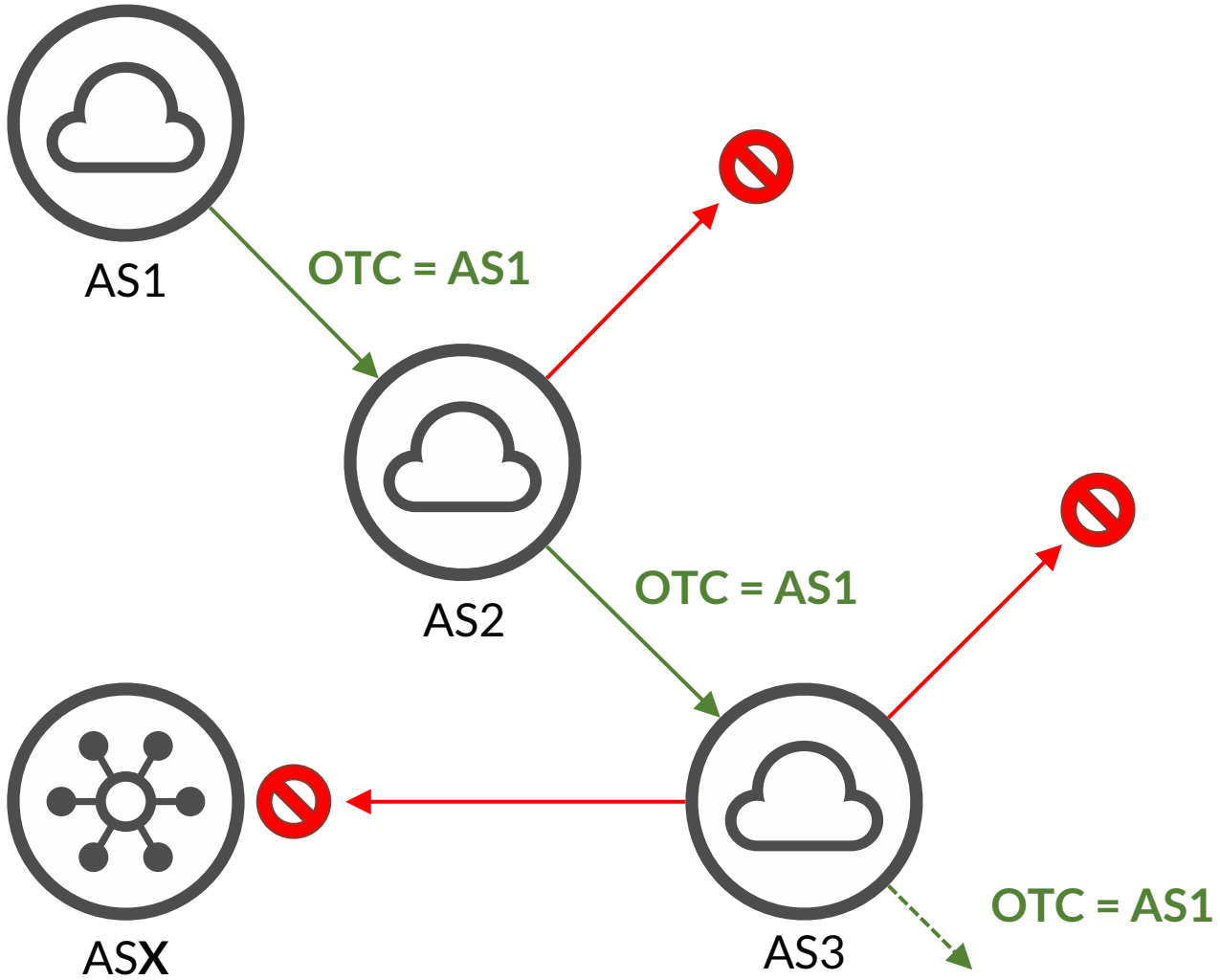
- **Idea**: Assigning roles to BGP neighbors
- Roles
  - Provider
  - Customer
  - Route Server (RS)
  - Route Server Client (RS-Client)
  - Peer
- Valid Relationships
  - Provider ↔ Customer
  - Peer ↔ Peer
  - RS ↔ RS-Client
- Negotiation of Roles
  - Session not established on mismatch



BGP Roles (RFC9234)

- Only to Customer (OTC) Attribute
  - Sent to Customer, RS-Client or Peer
- OTC carries AS number

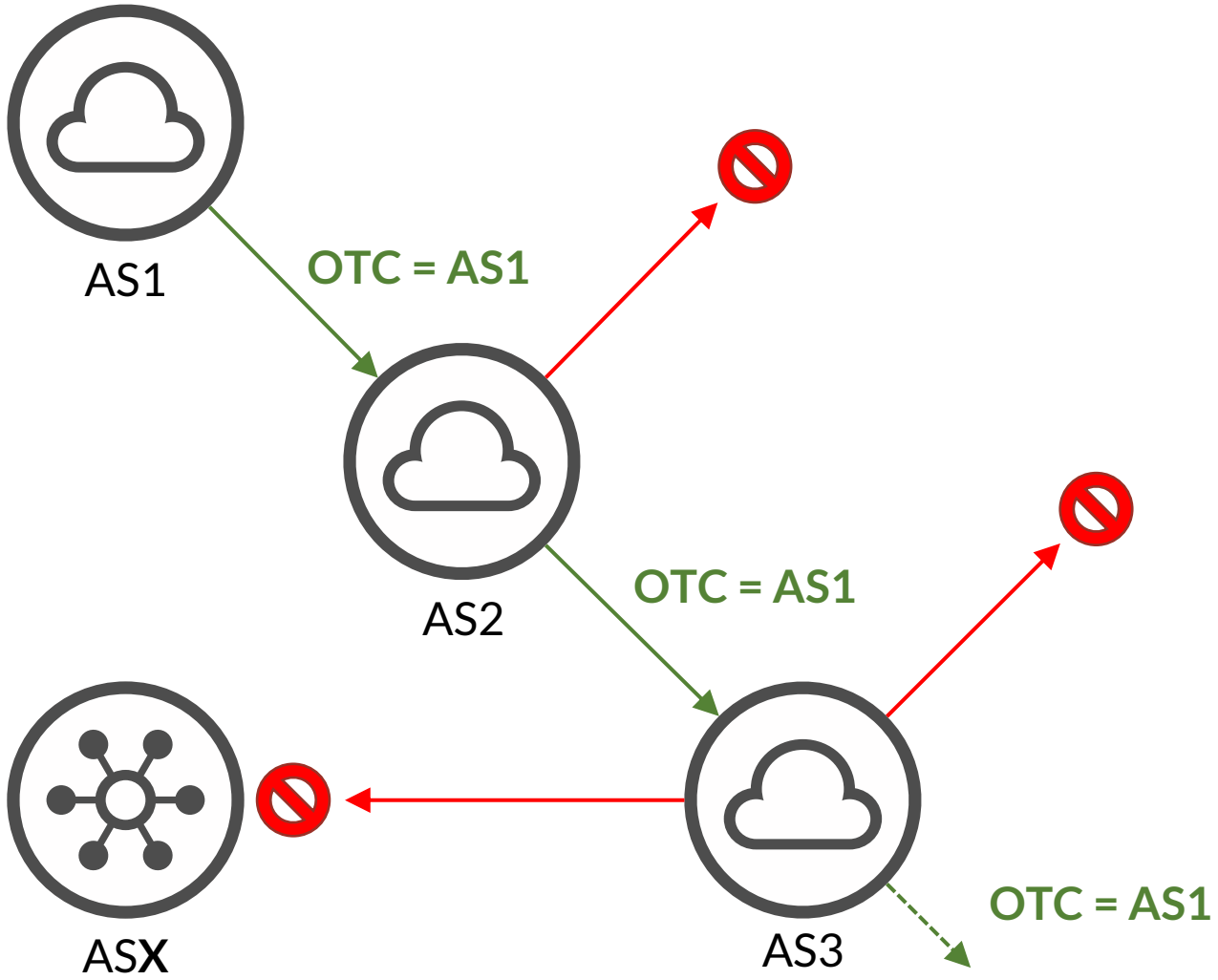
- OTC checking **Ingress**:
  1. **OTC present:** sender is Customer or RS-Client: **reject**
  2. **OTC present**: sender is Peer and sender AS not equals AS value in OTC: **reject**
  3. **OTC not present:** sender is Provider, Peer or RS: **set OTC with sender AS**



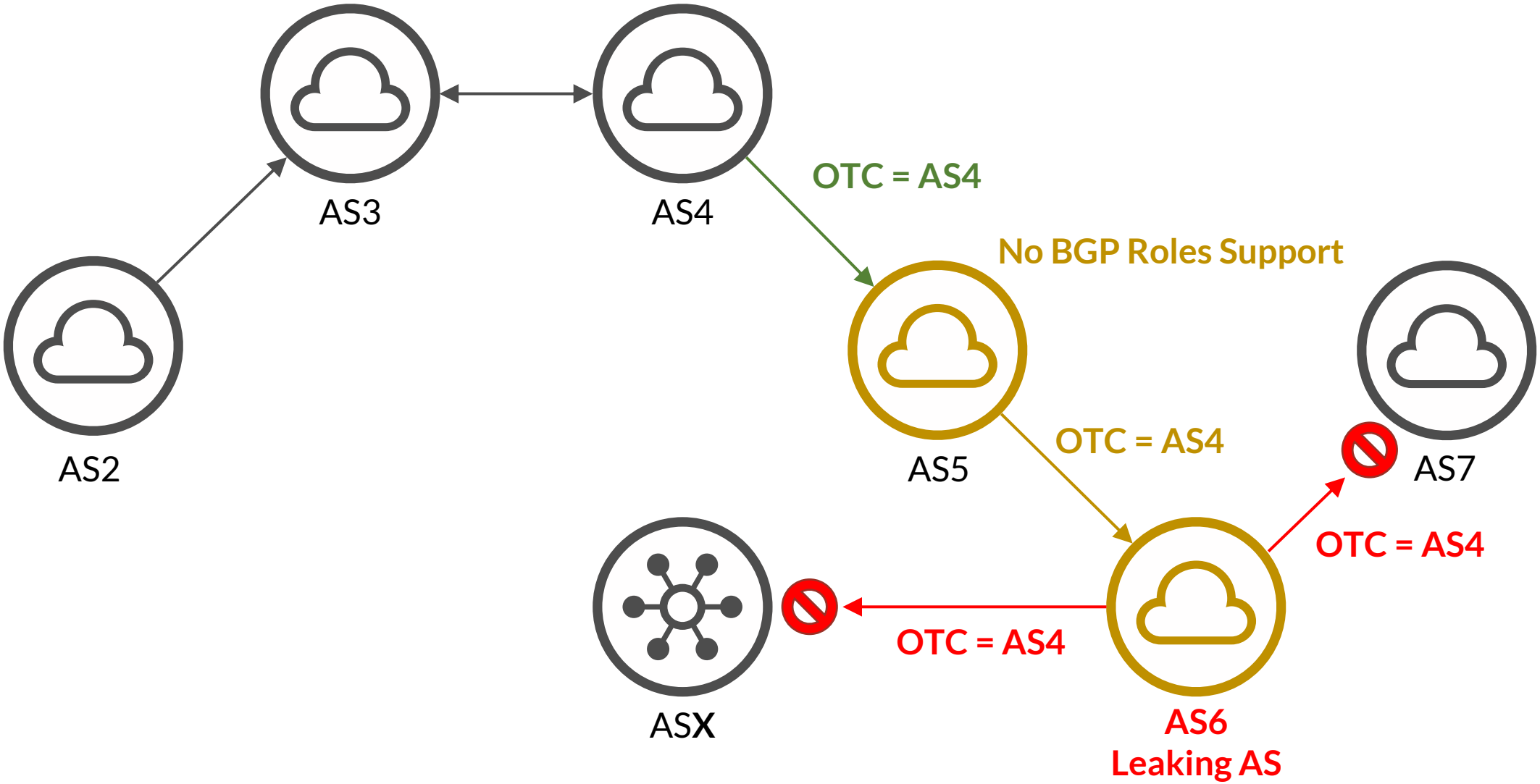
BGP Roles (RFC9234)

- OTC checking **Egress**:
  1. **OTC not present:** receiver is Customer, Peer or RS-Client: **set OTC with own AS value**
  2. **OTC present**: receiver is Provider, Peer or RS: **reject**

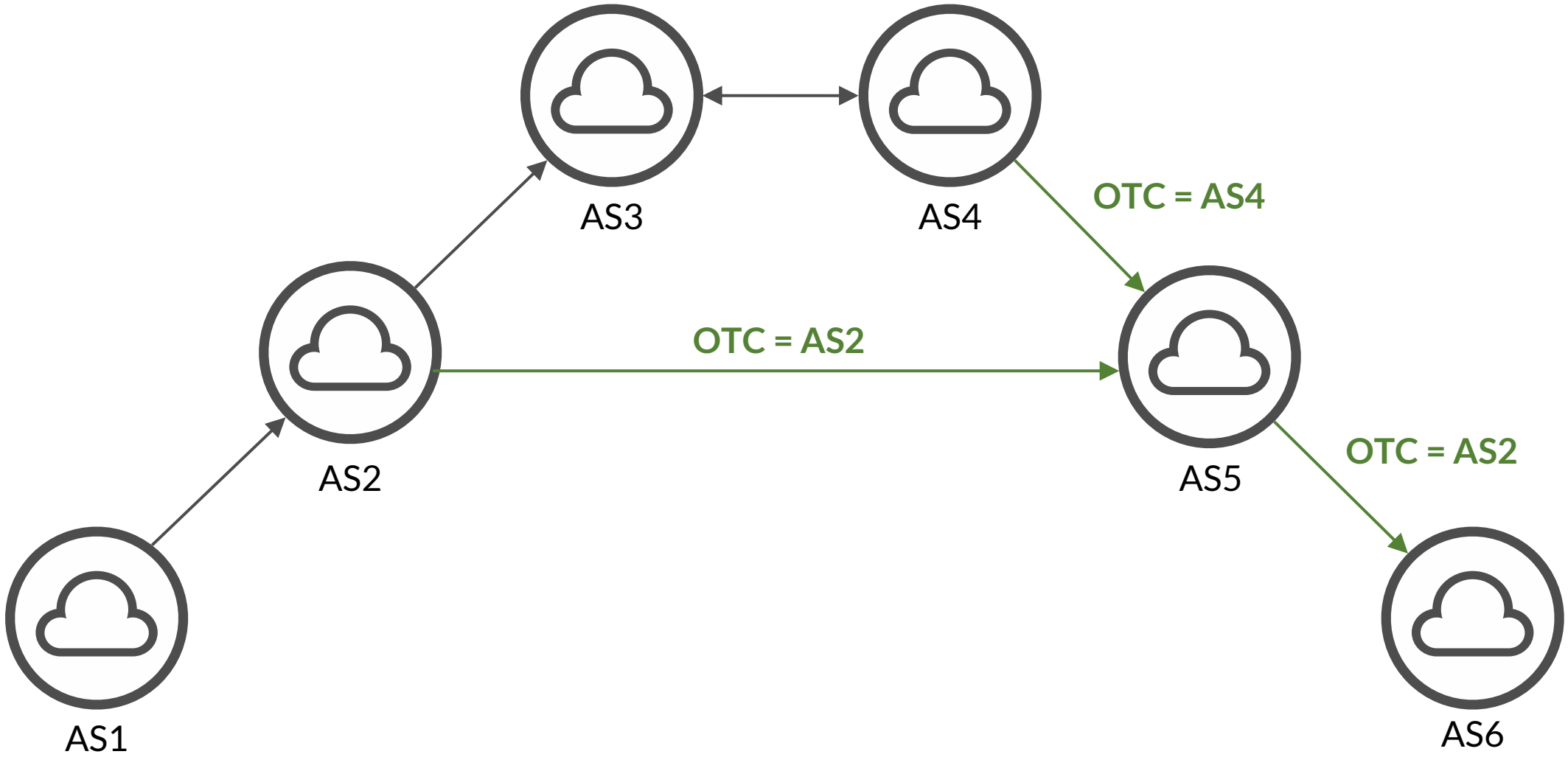
- OTC is set for both **Ingress and Egress**, if not set before
  → more robust
  → early adaptors profit



PARTIAL DEPLOYMENT EXAMPLE – BGP ROLES



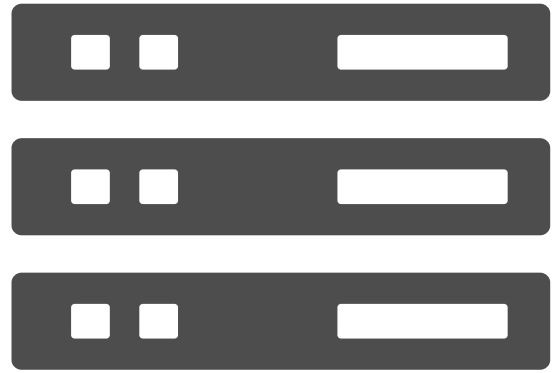
PEER EXAMPLE – BGP ROLES



BGP Roles (RFC9234)

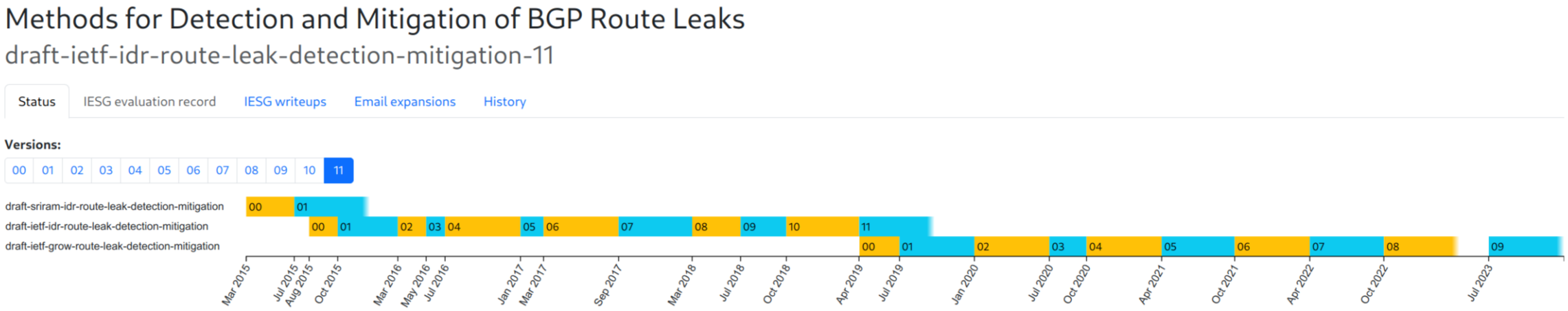
→ Automates Leak Detection and Prevention
→ Mitigation multiple hops away possible

- Software Support
  - Bird
  - FRR
  - OpenBGP
  - Mikrotik
- Unfortunately: nothing announced from the big vendors
  - Juniper, Arista, Cisco, Nokia …
  - if possible: Open Feature Requests!



DOWN ONLY COMMUNITY

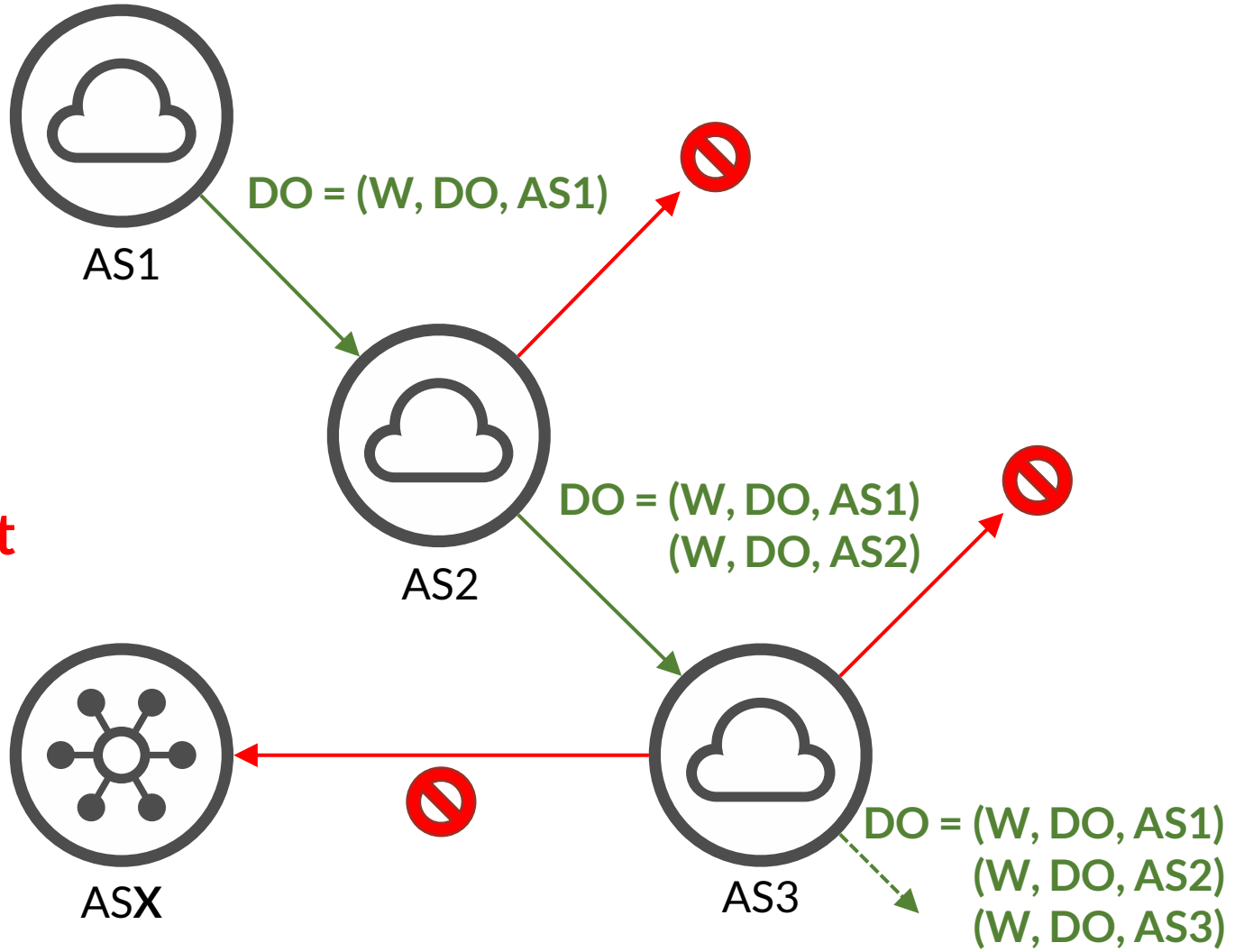
- Currently under specification (draft-ietf-grow-route-leak-detection-mitigation)
- Conecpt similar to BGP Roles
  → but use of well-known Large Community instead of transitive Attribute
- Communities and Policies have to be defined and assigned manually



DOWN ONLY COMMUNITY

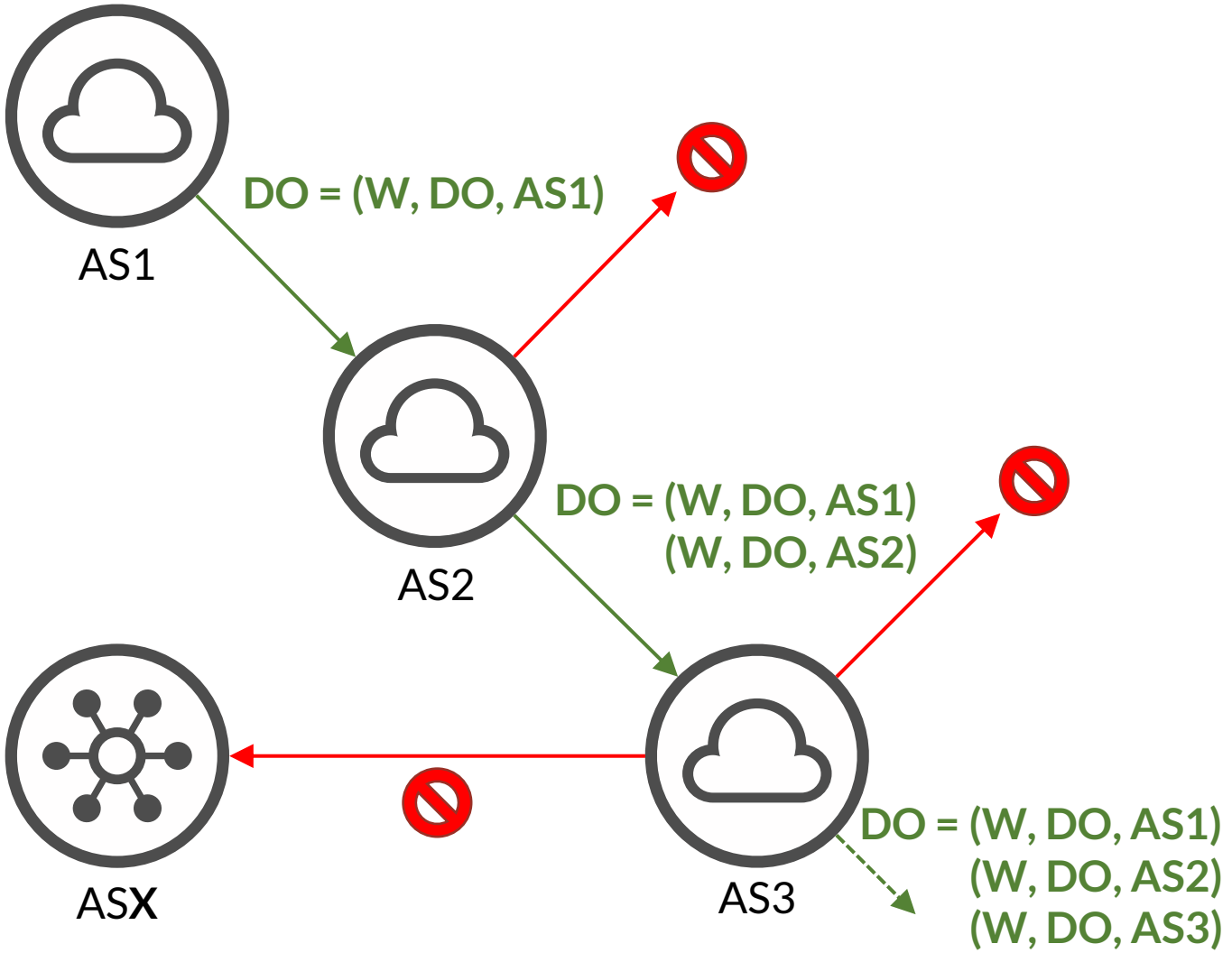
- Down Only (DO) Community
  - Sent to Customer, RS-Client or Peer
- DO carries AS number

- DO checking **Ingress**:
  1. **DO present:** sender is Customer or RS-Client: **reject**
  2. **DO present**: sender is Peer and at least one DO AS value does not match sender AS: **reject**
  3. sender is Provider, Peer or RS: **set DO with sender AS, if not present**

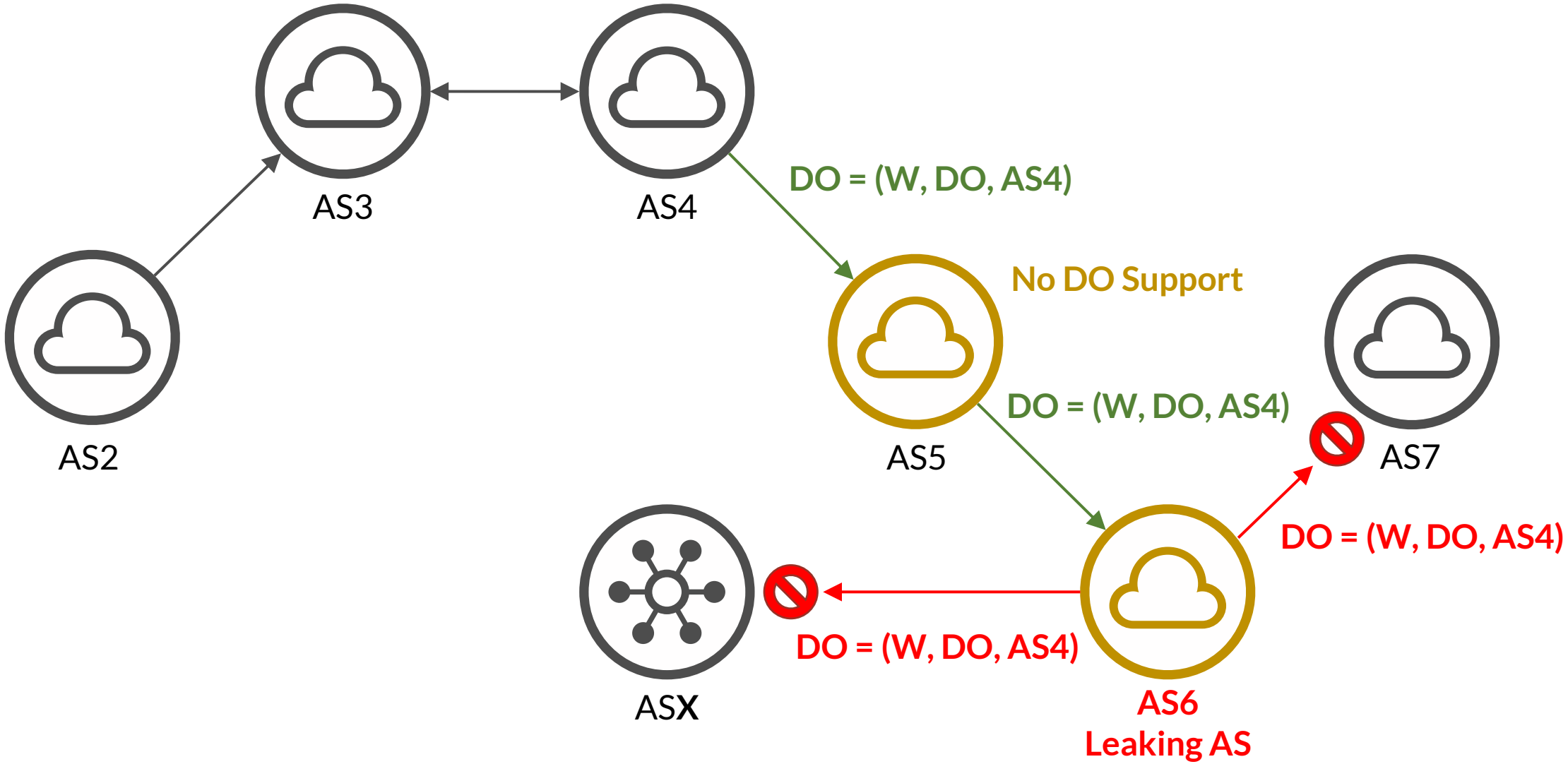


DOWN ONLY COMMUNITY

- DO checking **Egress**:
  1. **DO present**: receiver is Provider, Peer or RS: **reject**
  2. **DO not present:** receiver is Customer or Peer: **set DO with own AS value**



PARTIAL DEPLOYMENT – DOWN ONLY COMMUNITY



DOWN ONLY COMMUNITY

CORE BACKBONE

+ Advantages

- No update of Router OS necessary
- Incremental deployment possible
- Fast deployment possible

+ Disadvantages

- Not yet standardized
- Communities more likely to be dropped
- Lack of negative match communities like **a:b:!c** in most implementations
  - Compliant peer as sender: always one DO with value equals to peer AS
  - Ingress checking of peers simplified:
    DO present: sender is Peer and DO AS value not matches sender AS: **reject**


QUESTIONS?
CORE
BACKBONE