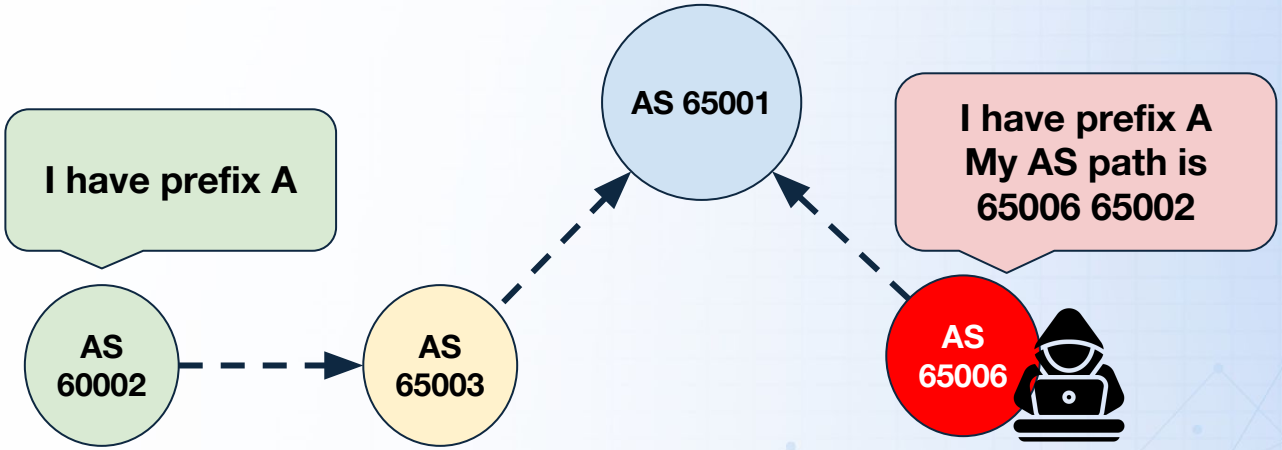
ARISTA

Autonomous System Provider Authorization and RFC 9234 for BGP Route Leak Detection and Prevention

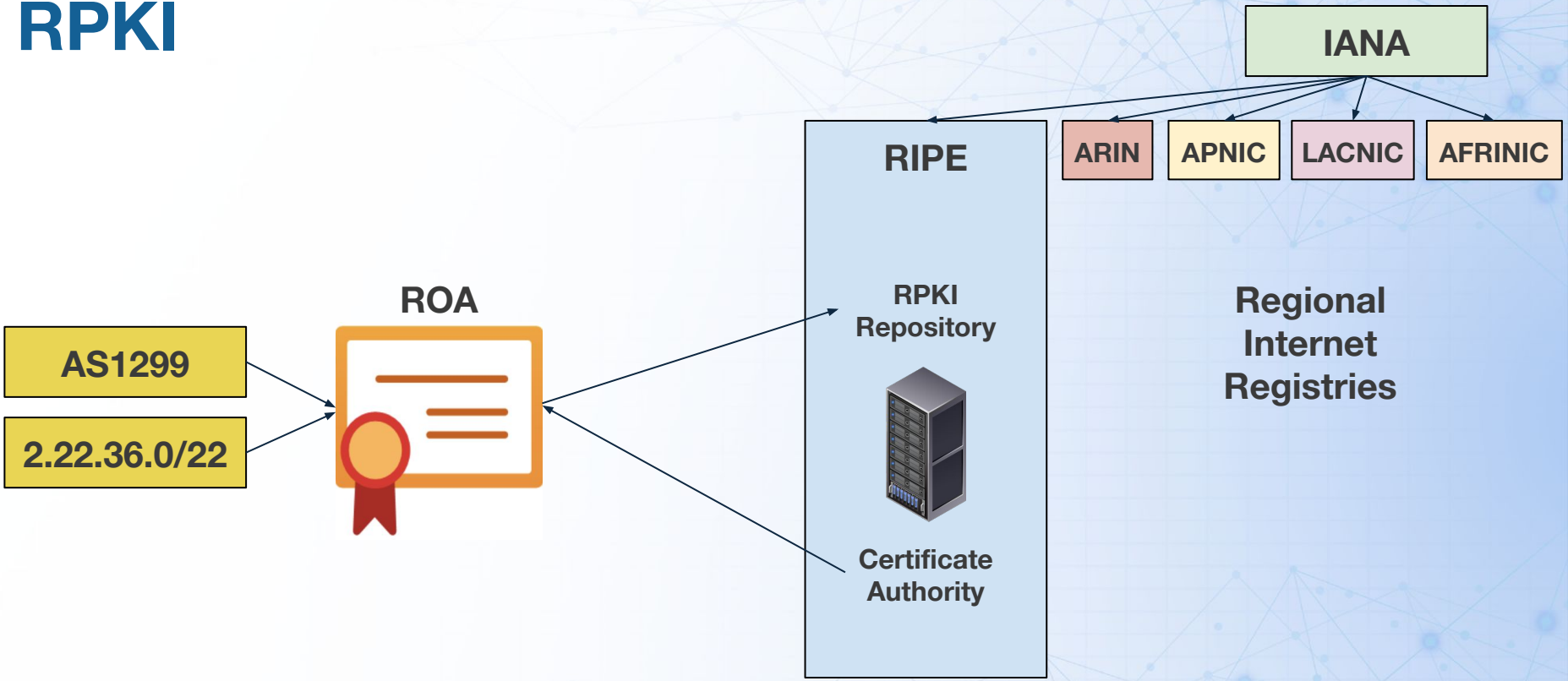
Johan Ervenius
Systems Engineer, Arista Networks

BGP is Based on Trust



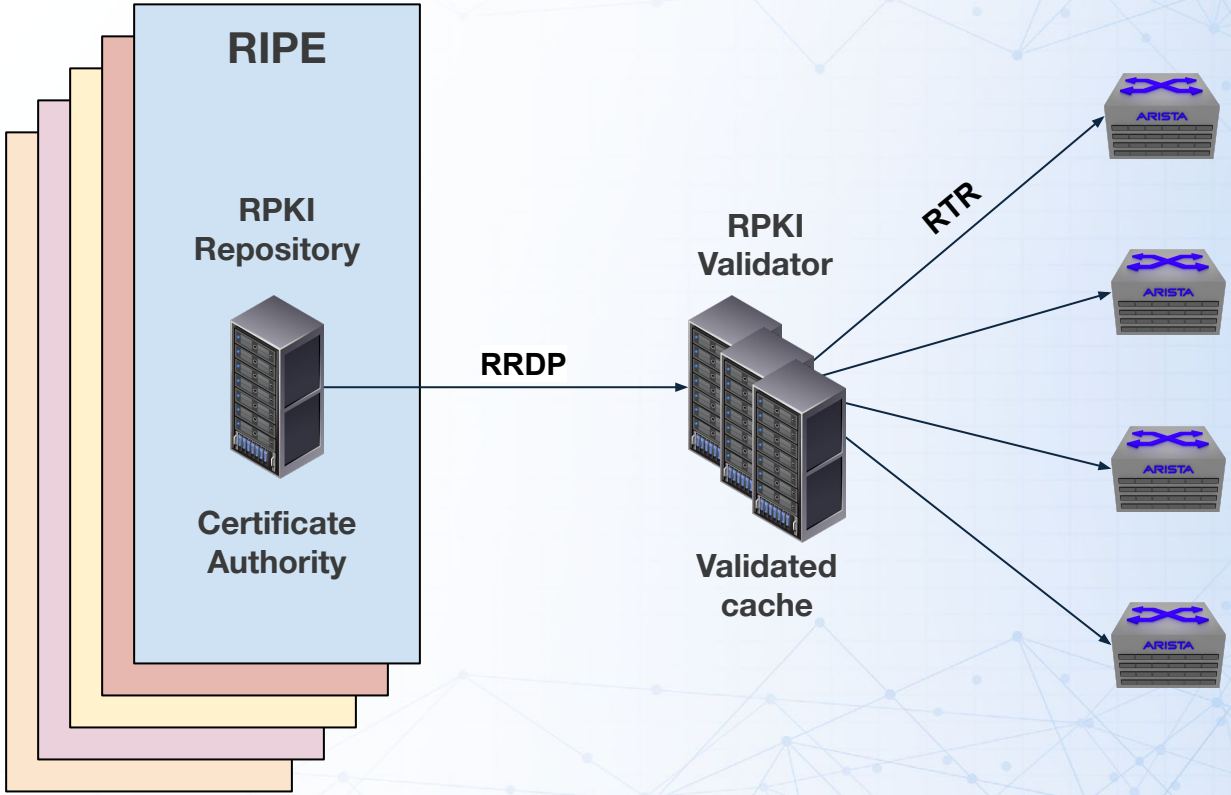
ARISTA

RPKI


IANA
RIPE
ARIN
APNIC
LACNIC
AFRINIC
ROA
AS1299
2.22.36.0/22
RPKI
Repository
Certificate
Authority
Regional
Internet
Registries

ARISTA

RPKI


RIPE
RPKI
Repository
Certificate
Authority
RRDP
RPKI
Validator
Validated
cache
RTR
ARISTA
ARISTA
ARISTA
ARISTA

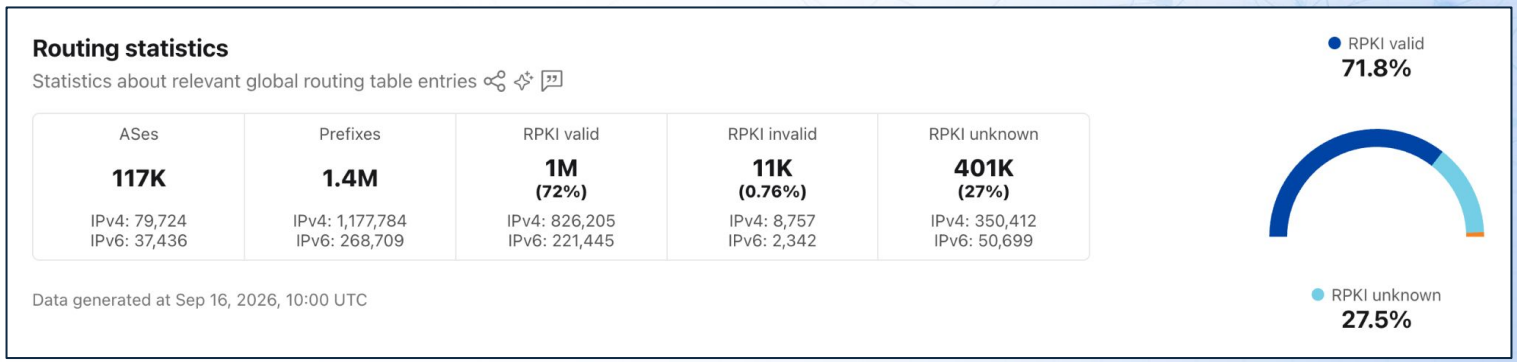
ARISTA

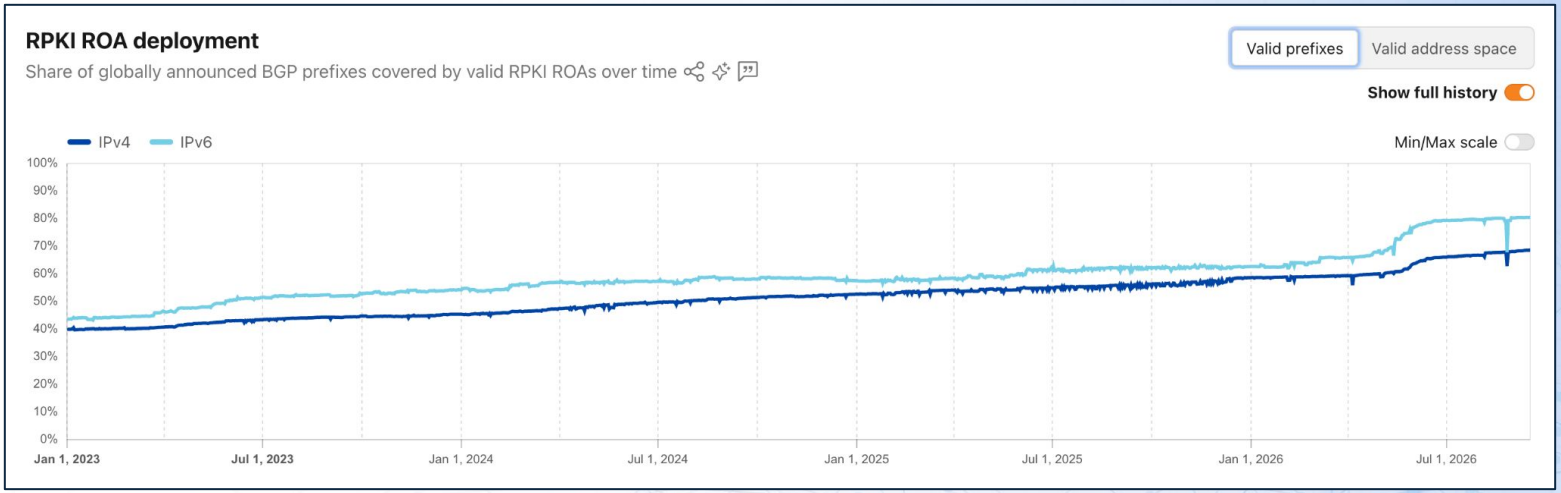
RPKI

```
Arista#show bgp ipv4 unicast
...
            Network          Next Hop       ...  Path
 * >     V 1.0.0.0/24      192.168.0.0    ...  680 13335 i
 * >     U 1.0.16.0/24     192.168.0.0    ...  680 30781 2497 2519 i
 * >     V 1.0.64.0/18     192.168.0.0    ...  680 30781 2497 2519 7670 18144 i
 * >     V 1.0.128.0/17    192.168.0.0    ...  680 6939 38040 23969 i
...
```


ARISTA

Status of RPKI

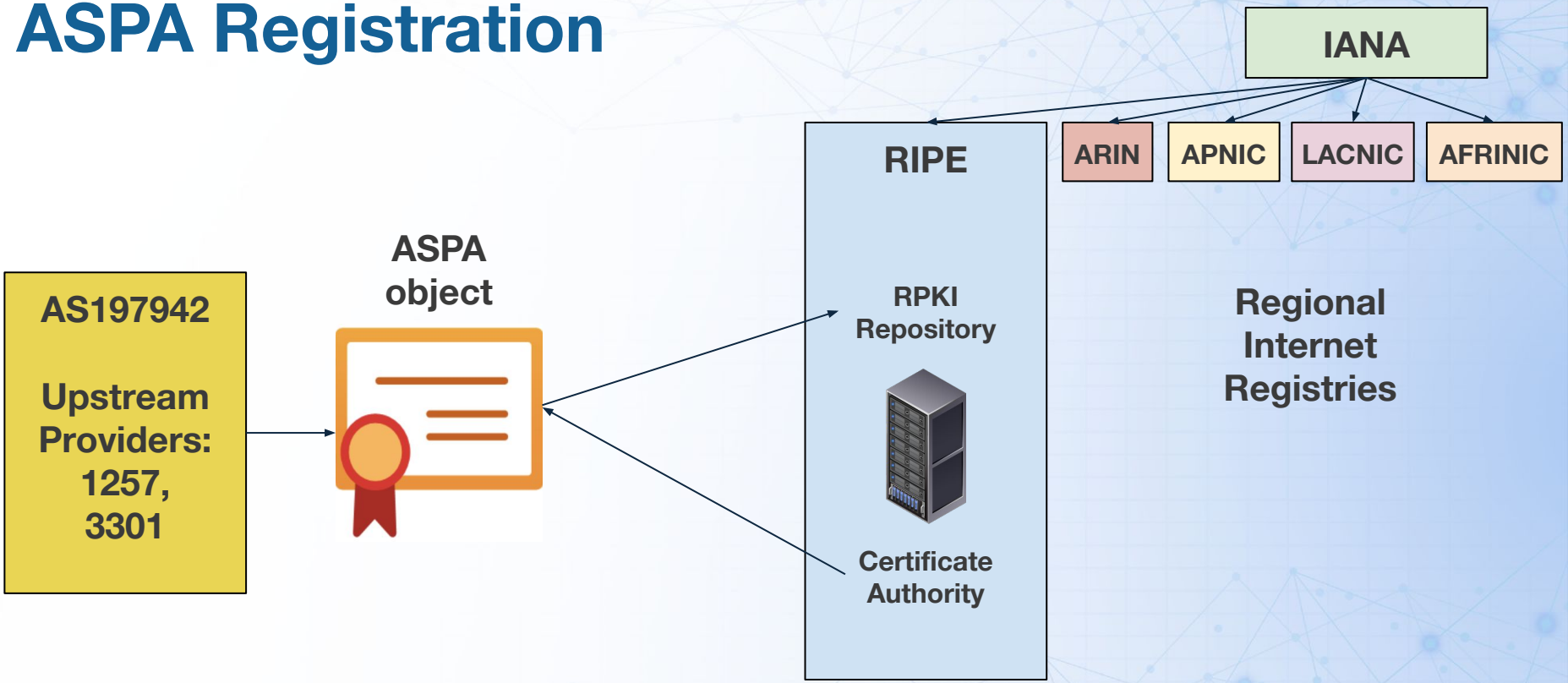




Source: https://radar.cloudflare.com/routing/rpki

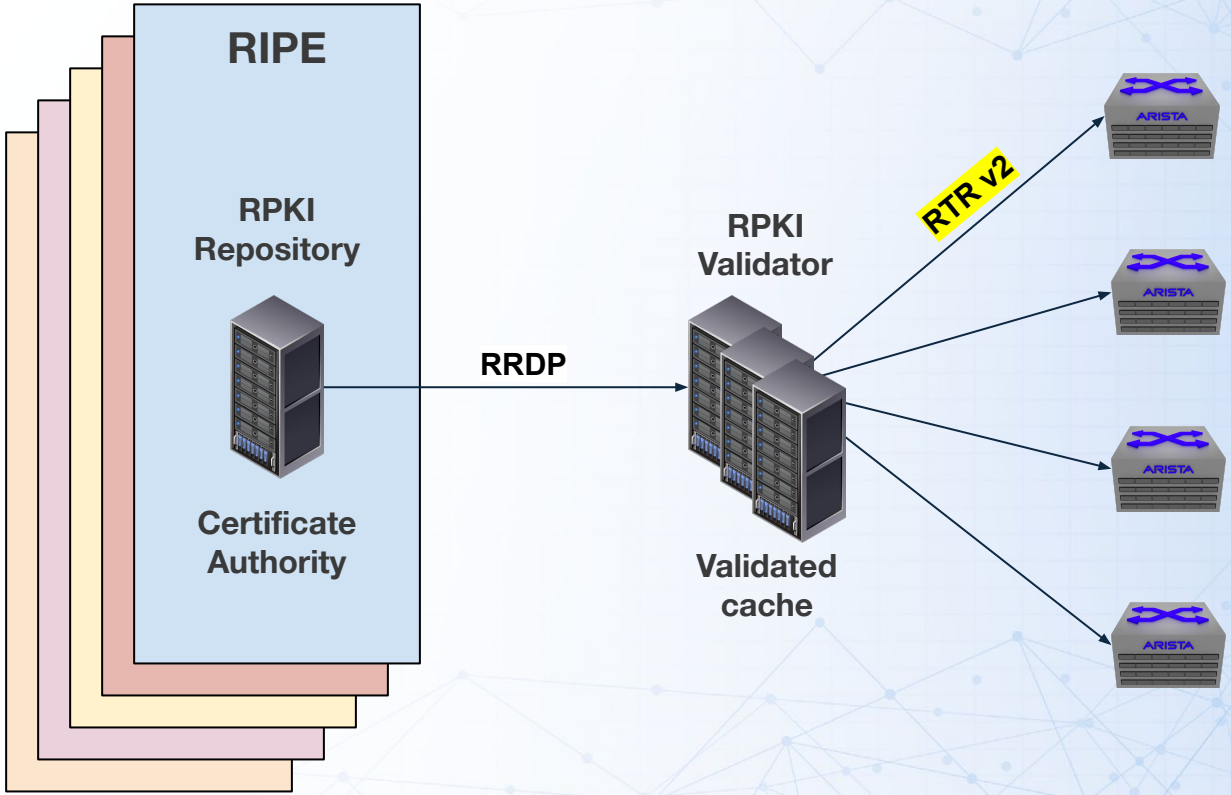
ARISTA

ASPA Registration



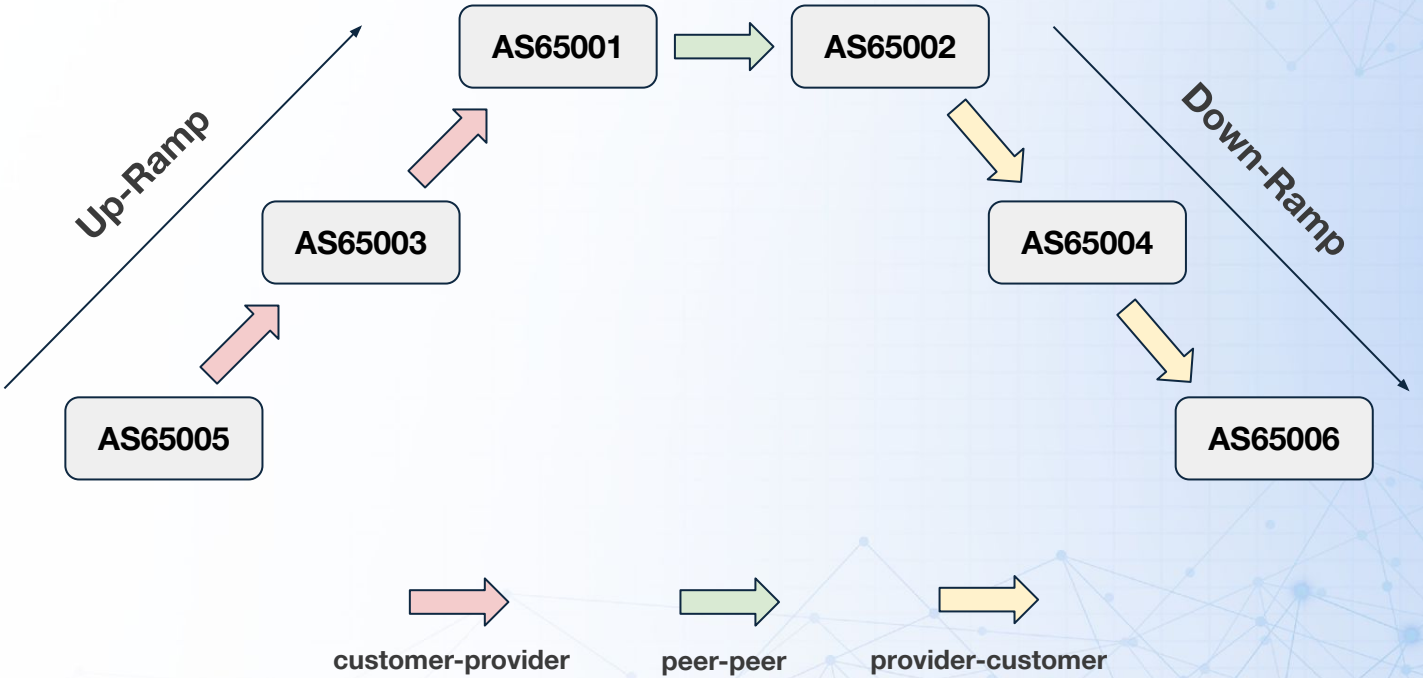
ARISTA

ASPA Validation



ARISTA

ASPA - Relies on Internet hierarchy



ARISTA

ASPA - How does validation work?

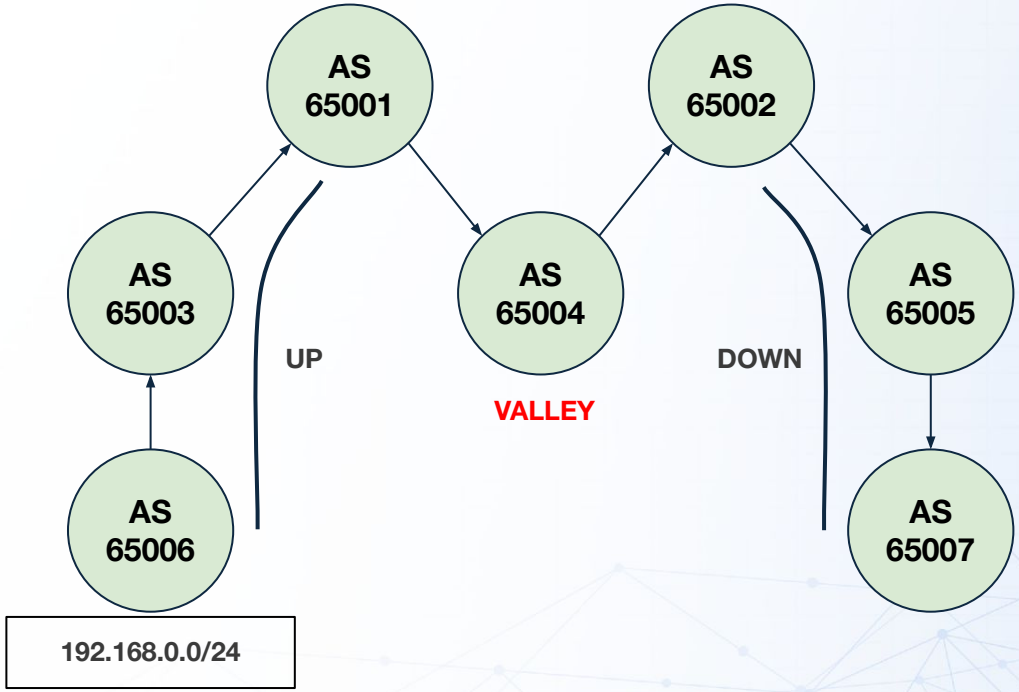
- **Checking the Up-Ramp:**
  - Starts at the origin and moves forward
  - At every hop, verify that the next-hop is an authorized provider of the customer network.
  - Keep going until the Up-Ramp stops.

- **Checking the Down-Ramp**
  - Start at the destination of a BGP update and do the same verification, moving backwards

- If the Up-Ramp and the Down-Ramp covers the entire AS path, the route is **valid**, otherwise the route is **invalid**.

- If ASPA information is missing in parts of the Up- or Down-Ramp the route is **unknown**

ASPA - Validation Example



Prefix announced from AS6

AS1 and AS2 are Tier1s and have no provider (AS0)

AS7 sees the following path:
5 2 4 1 3 6

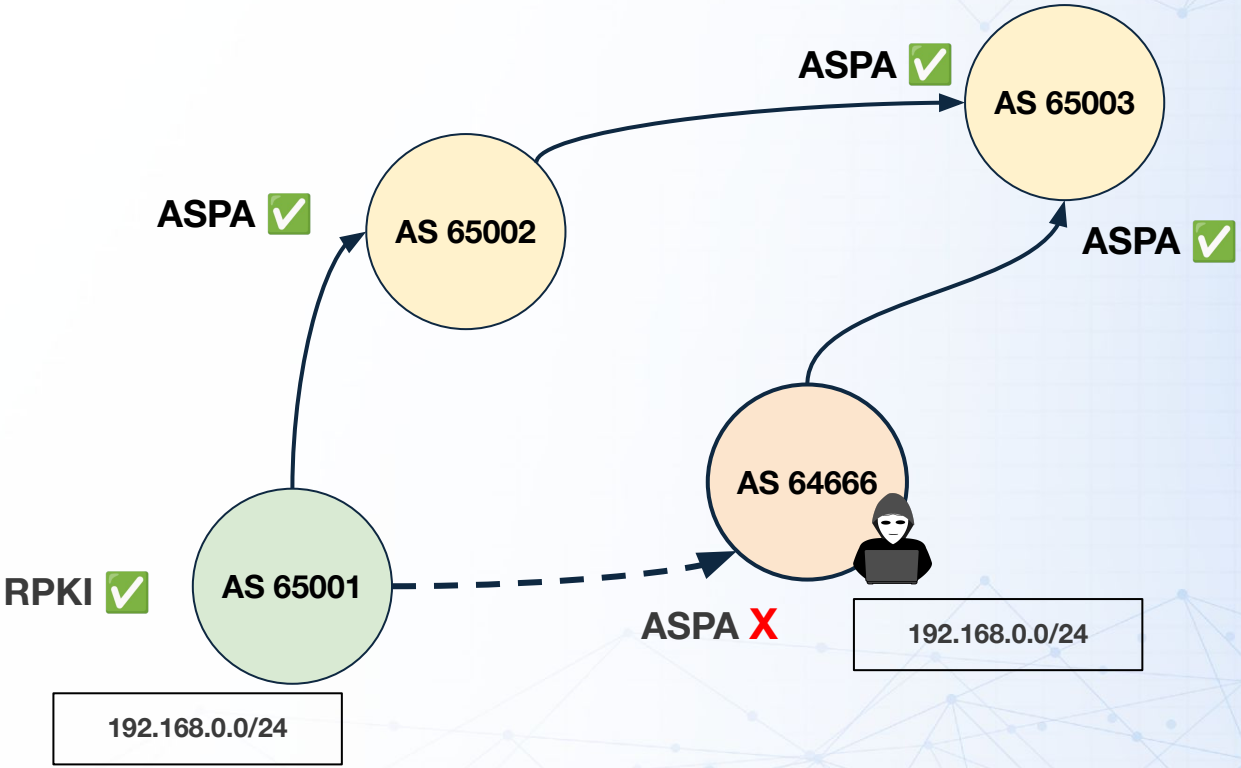
AS4 is not a provider for AS1:
- Up path: 1 3 6

AS4 is not a provider for AS2:
- Down path: 5 2

The entire path is not covered. AS4 is a valley.

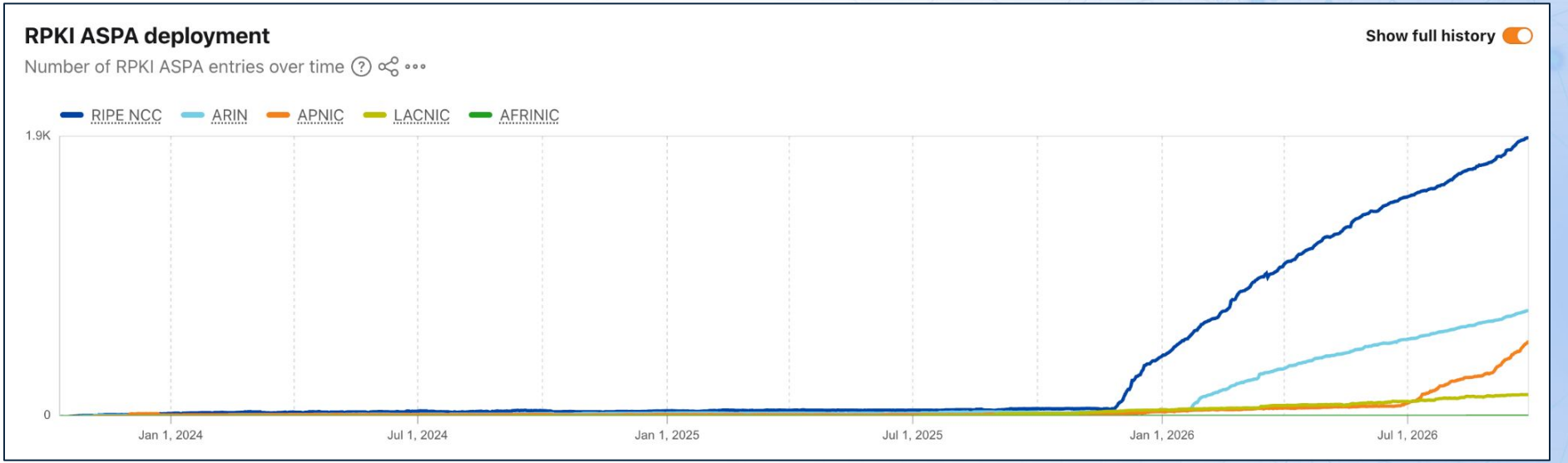
ARISTA

ASPA - blocking forged-origin hijacks



ARISTA

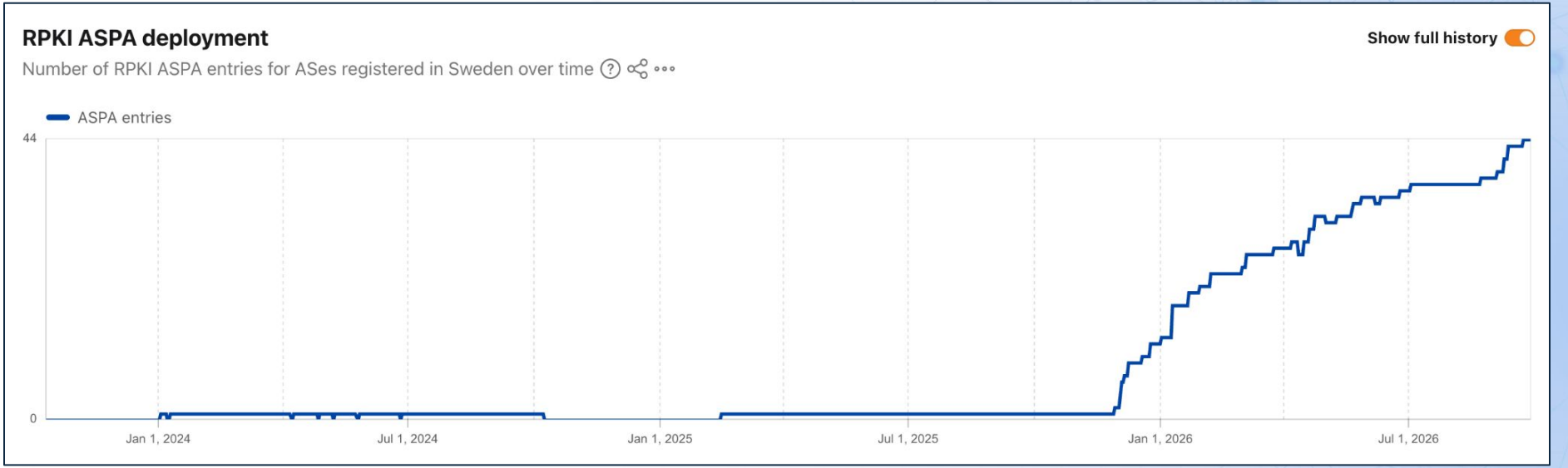
Status of ASPA - Worldwide



Source: https://radar.cloudflare.com/routing/rpki

ARISTA

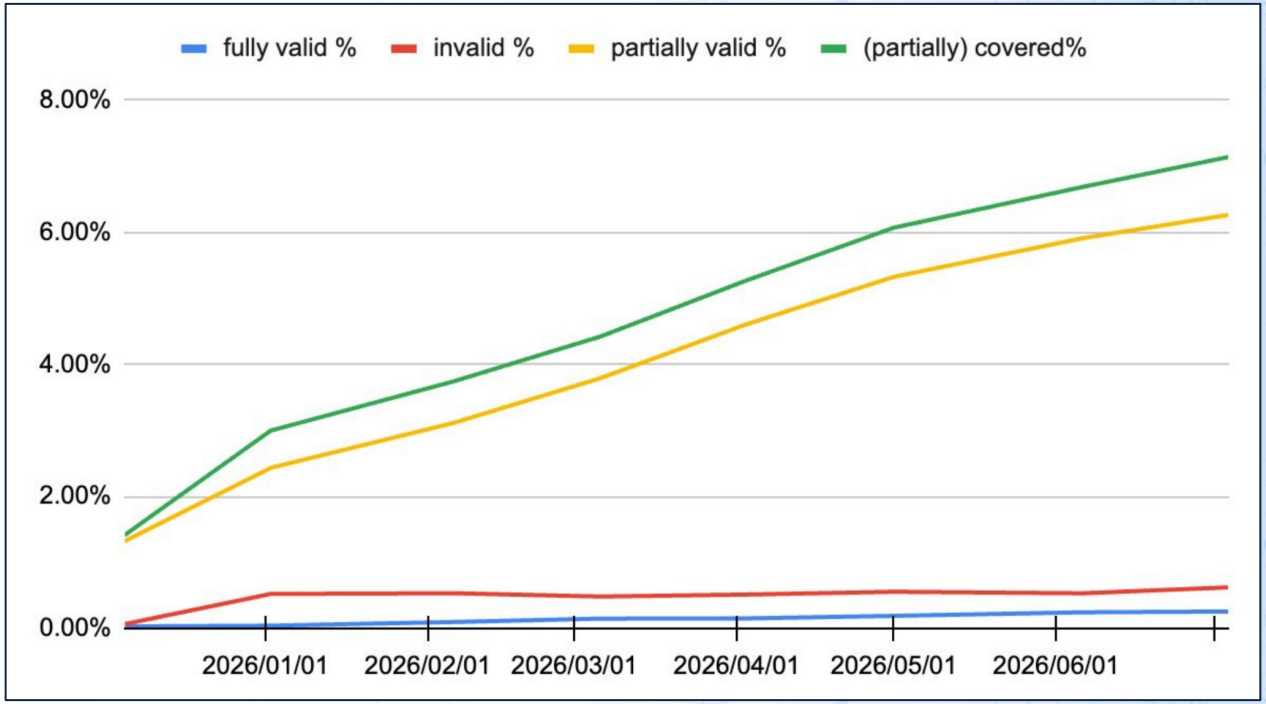
Status of ASPA - Sweden



Source: https://radar.cloudflare.com/routing/rpki

ARISTA

ASPA Path Validity to AS0 Networks



Source: Tim Bruijnzeels, RIPE NCC.
Presented at NLNOG Day on September 4, 2026

ARISTA

ARISTA

RFC 9234 - Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages

RFC 9234

- **BGP Role Capability**
  - Peers explicitly negotiate their relationship type, enabling automatic detection of misconfigured sessions.

- **Only-to-Customer Attribute**
  - Marks routes that should only flow toward customers, preventing accidental upstream propagation.

BGP Role Capability

```
router bgp 65001
   bgp role-based peering [strict]
   neighbor 10.0.0.1 remote-as 65002
   neighbor 10.0.0.1 local-role provider
```

EBGP

```
router bgp 65002
   bgp role-based peering [strict]
   neighbor 10.0.0.0 remote-as 65001
   neighbor 10.0.0.0 local-role customer
```

```
Border Gateway Protocol – OPEN Message
   Marker: ffffffffffffffffffffffffffffffff
   Length: 60
   Type: OPEN Message (1)
   Version: 4
   My AS: 65001
   Hold Time: 180
   BGP Identifier: 10.10.10.1
   Optional Parameters Length: 31
   Optional Parameters
      Optional Parameter: Capability
         Parameter Type: Capability (2)
         Parameter Length: 29
         Capability: Route refresh capability
         Capability: Enhanced route refresh capability
         Capability: Support for 4-octet AS number capability
         Capability: Multiprotocol extensions capability
         Capability: Graceful Restart capability
         Capability: Support for Additional Paths
         Capability: BGP Role
            Type: BGP Role (9)
            Length: 1
            BGP Role: Provider (0)
```

OPEN →

← OPEN

```
Border Gateway Protocol – OPEN Message
   Marker: ffffffffffffffffffffffffffffffff
   Length: 60
   Type: OPEN Message (1)
   Version: 4
   My AS: 65002
   Hold Time: 180
   BGP Identifier: 10.10.10.2
   Optional Parameters Length: 31
   Optional Parameters
      Optional Parameter: Capability
         Parameter Type: Capability (2)
         Parameter Length: 29
         Capability: Route refresh capability
         Capability: Enhanced route refresh capability
         Capability: Support for 4-octet AS number capability
         Capability: Multiprotocol extensions capability
         Capability: Graceful Restart capability
         Capability: Support for Additional Paths
         Capability: BGP Role
            Type: BGP Role (9)
            Length: 1
            BGP Role: Customer (3)
```


ARISTA

BGP Role Capability

Allowed role pairings

Local Role		Remote Role
Provider	⟷	Customer
Customer	⟷	Provider
Peer	⟷	Peer
Route Server	⟷	Route Server Client
Route Server Client	⟷	Route Server

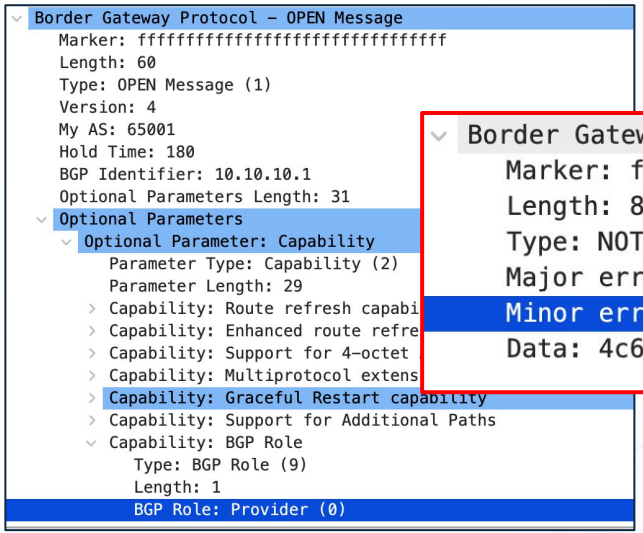
ARISTA

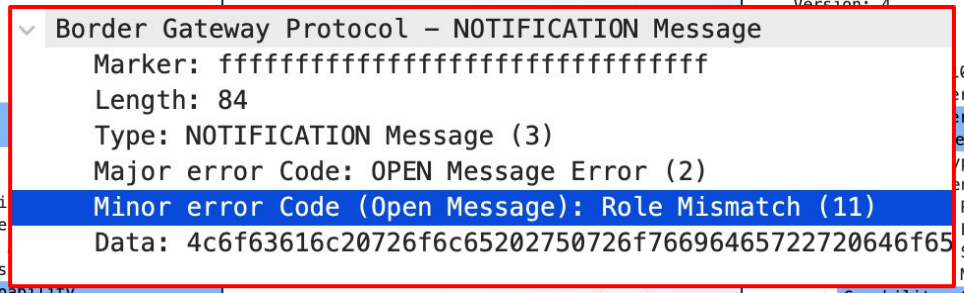
BGP Role Capability

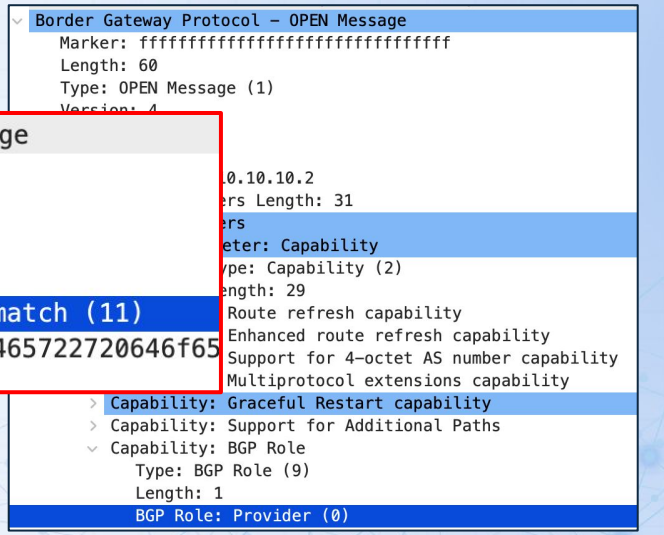
```
router bgp 65001
   bgp role-based peering
   neighbor 10.0.0.1 remote-as 65002
   neighbor 10.0.0.1 local-role provider
```

EBGP

```
router bgp 65002
   bgp role-based peering
   neighbor 10.0.0.0 remote-as 65001
   neighbor 10.0.0.0 local-role provider
```



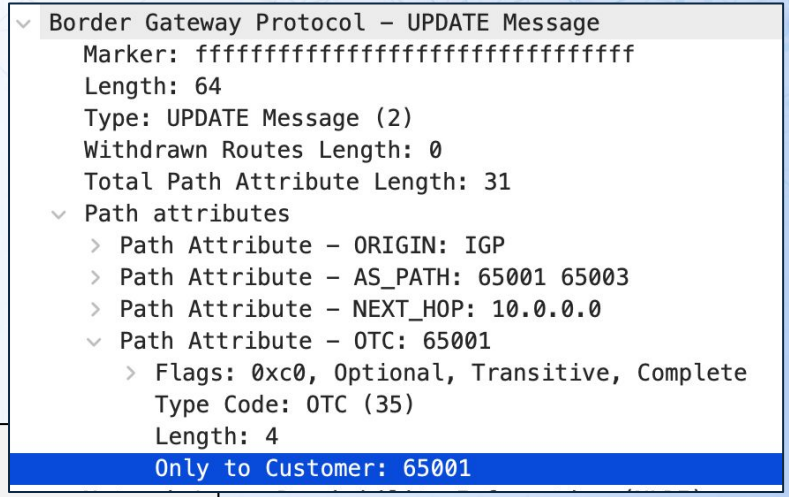




ARISTA

Only-to-Customer Attribute

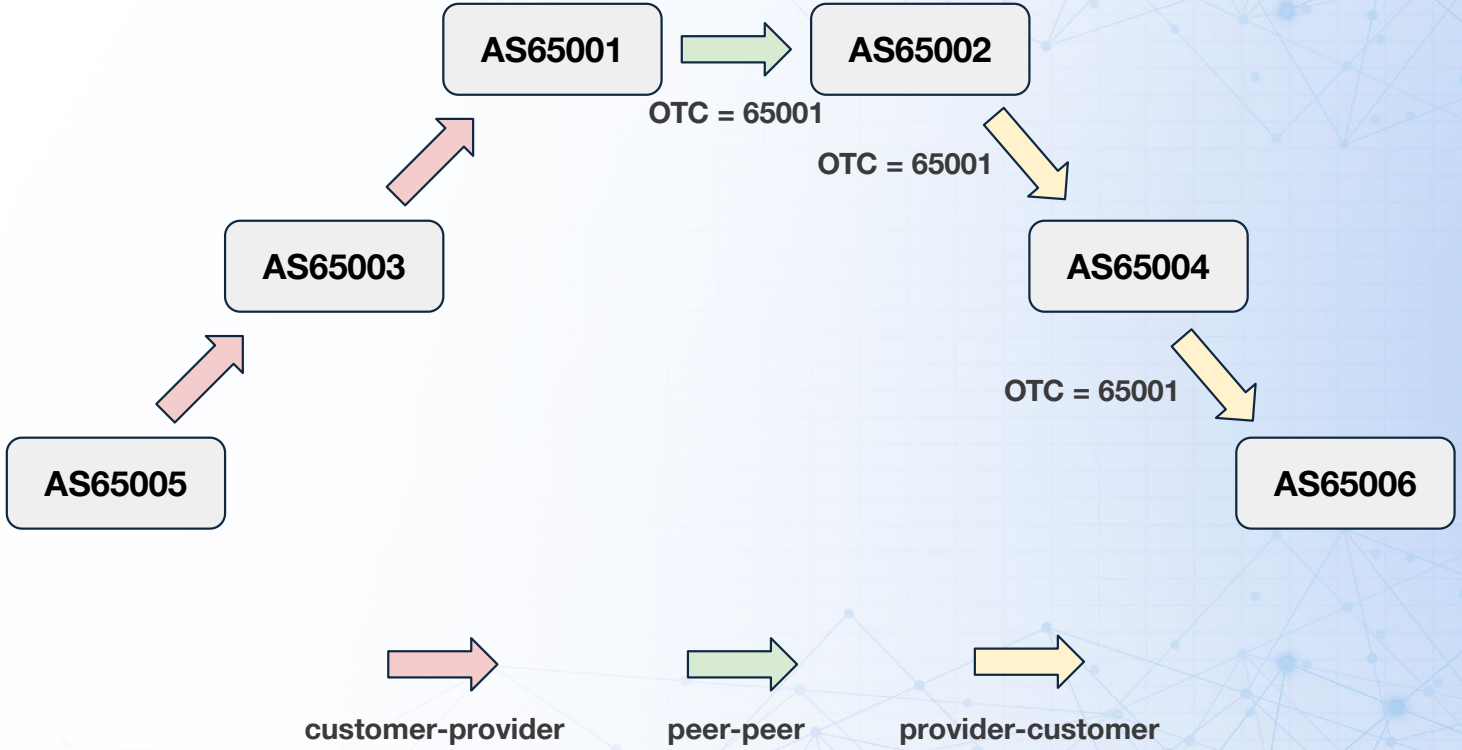
- Optional transitive attribute
- The value is an AS number
- Set by the first AS that first sends a route sideways or downwards




```
Arista#sh bgp ipv4 unicast detail
BGP routing table information for VRF default
Router identifier 10.10.10.2, local AS number 65002
BGP routing table entry for 10.0.0.2/31
 Paths: 1 available
  65001 65003
    10.0.0.0 from 10.0.0.0 (10.10.10.1)
      Origin IGP, metric 0, localpref 100, IGP metric 0, weight 0, tag 0
      Received 00:00:23 ago, valid, external, best, OTC 65001
      Rx SAFI: Unicast
```

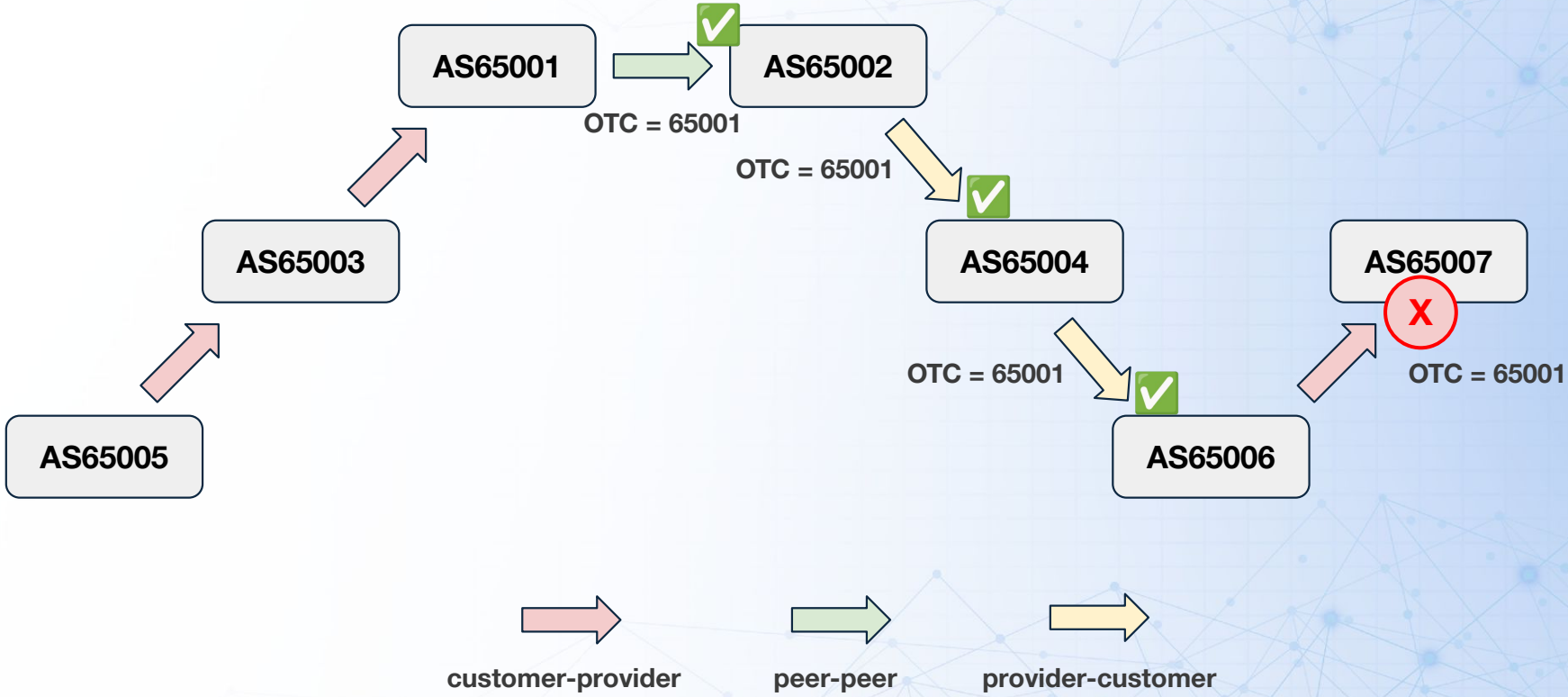

ARISTA

Only-to-Customer Attribute



ARISTA

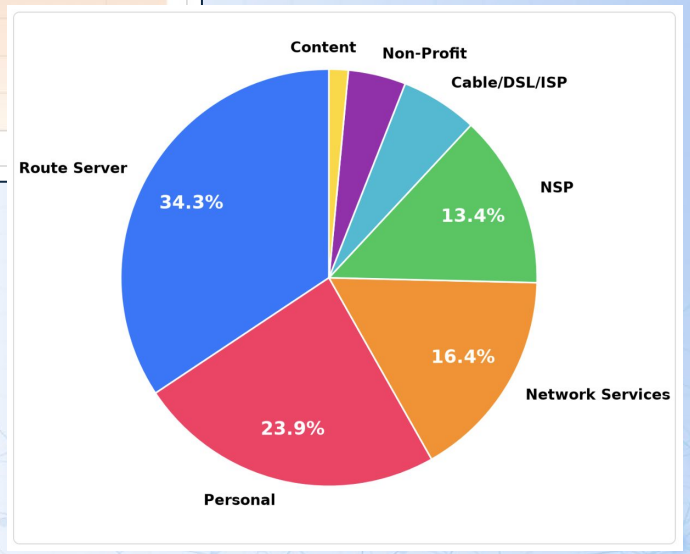
Only-to-Customer Attribute



ARISTA

Adoption of OTC





Source: https://blog.cloudflare.com/rfc9234-bgp-role-model/

ARISTA

ARISTA

Thank You

www.arista.com