

# ENFORCING RPKI-BASED ROUTING POLICY ON THE DATA PLANE AT AN INTERNET EXCHANGE

Josh Bailey, Dean Pemberton, Andy Linton, Cristel Pelsser and Randy Bush

## Prefix mis-origination

Multiple events. For example:

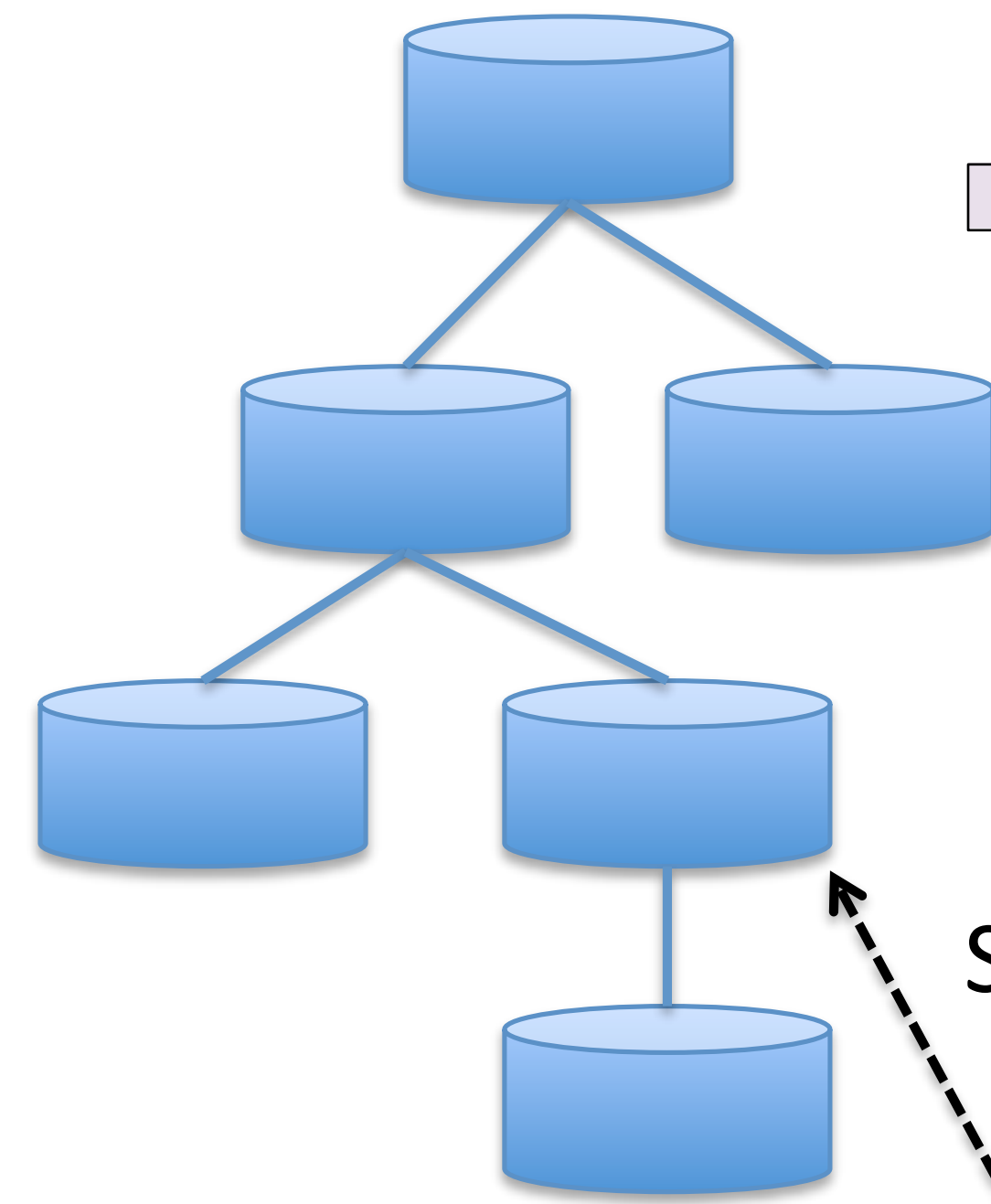
"Starting at 18:26 UTC (April 2, 2014) AS4761 began to originate 417,038 new prefixes normally announced by other Autonomous Systems. The 'mis-origination' event by Indosat lasted ... until approximately 21:15 UTC."

<http://www.bgpmon.net/hijack-event-today-by-indosat/>

BGP Hijacking for crypto currency profit, <http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/>, August 7, 2014.

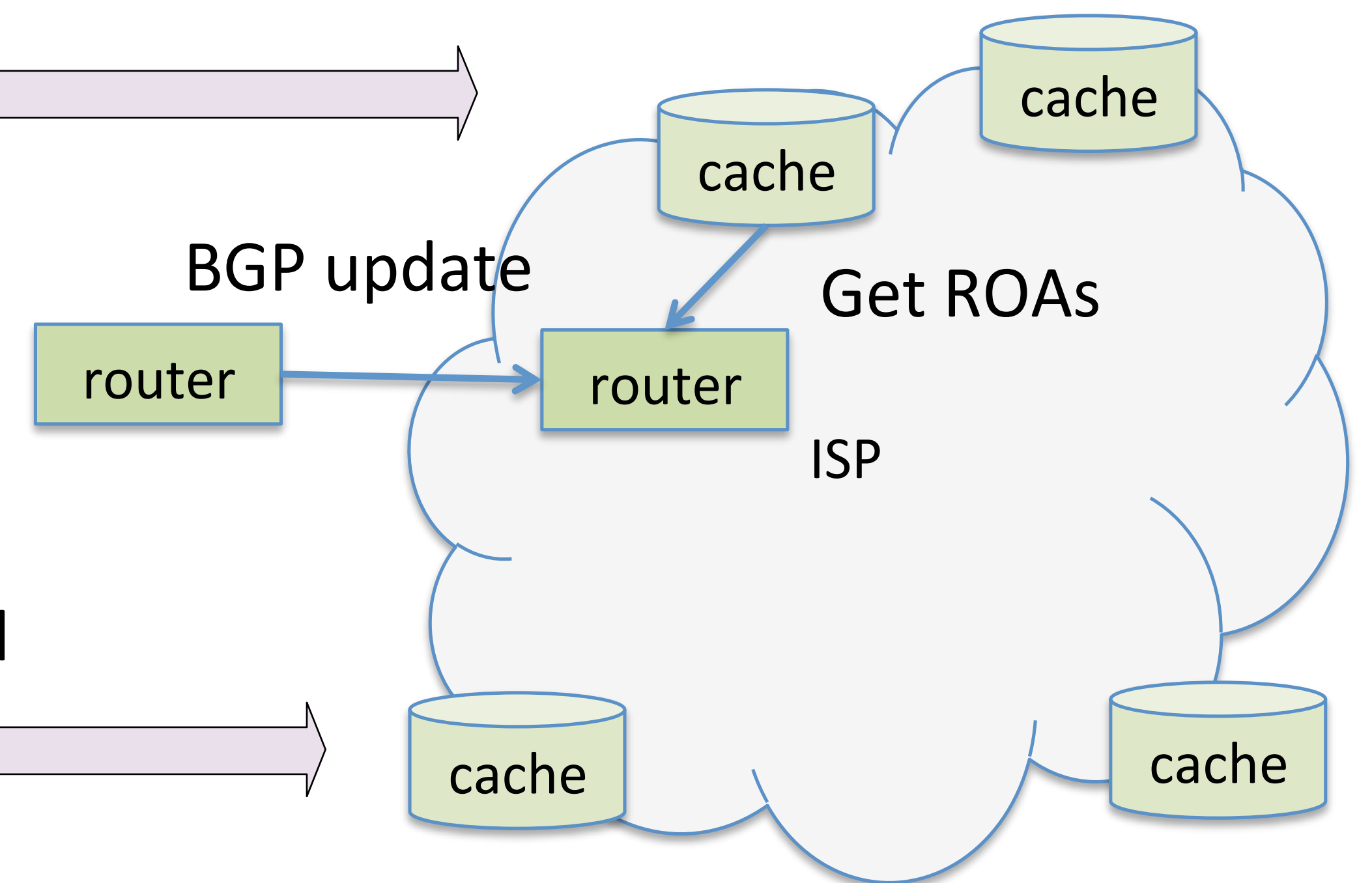
## Route origin validation

RPKI infrastructure  
Distributed database for ROAs



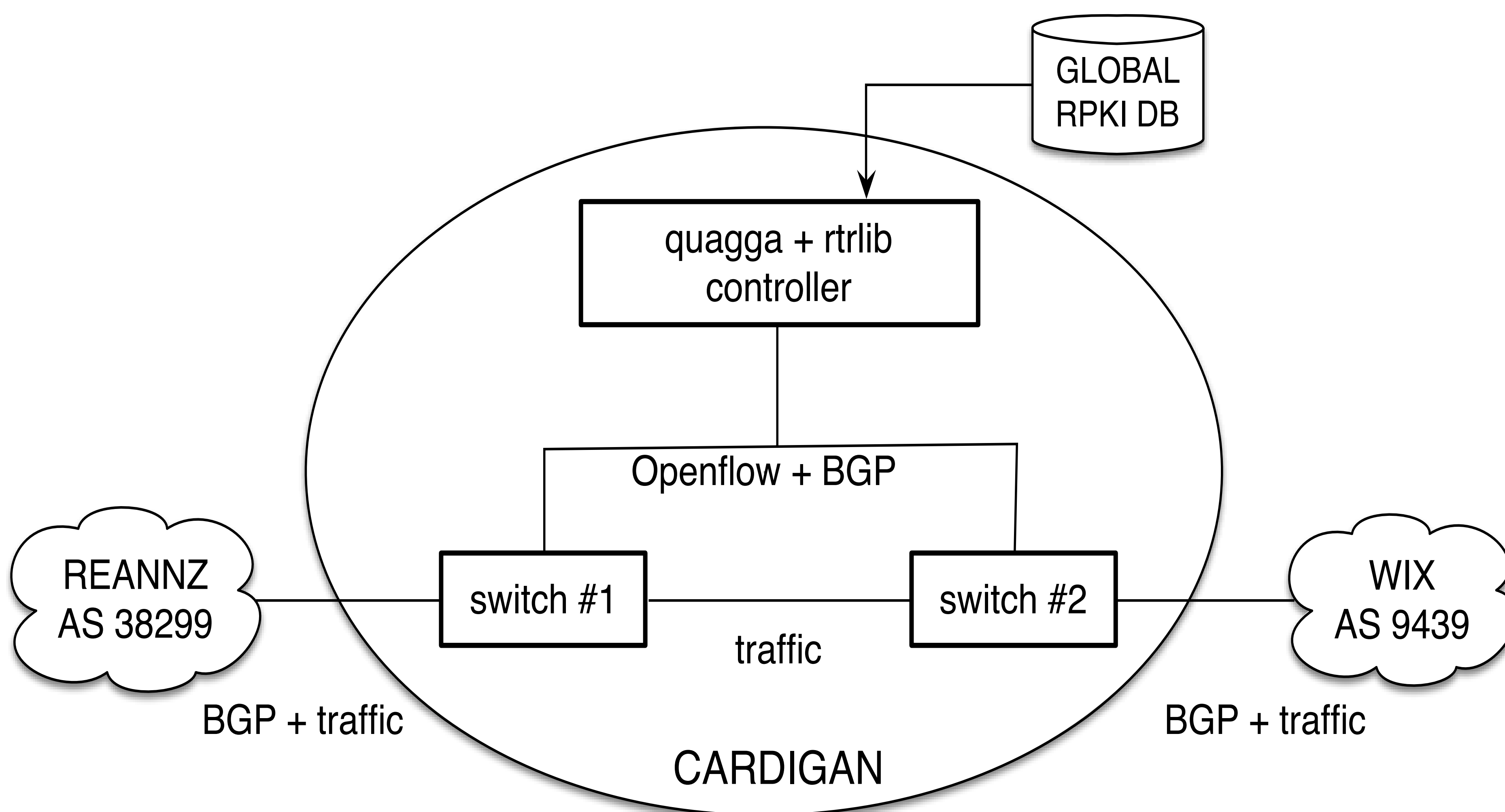
ROA
Prefix/length-maxlength
ASN

Caches regularly travels the RPKI infrastructure or request latest info from another cache



Routers check the validity of an origin AS based on the locally stored ROAs

## Deployment of BGP route origin validation



BGP sessions established with Quagga RTRlib to get ROAs  
Origin validation in Quagga RouteFlow to convert routes to openflow entries for the two switches

From March 17, 2014 to March 24, 2014  
Out of 566 routes from the 2 WIX sessions  
23 have a valid origin  
19 have invalid route origin  
The rest has no ROA associated

**Most invalid routes are due to the advertised prefix length not matching the ROA**  
**One prefix advertised by an an AS not matching the ROA**

Use OpenFlow counters to count the amount of traffic per flow  
Counters can be used to predict the amount of traffic that will be dropped due to origin invalidity

18.81 GB of traffic from REANNZ  
20.18 GB from the WIX

A single entry is used to forward most of the traffic.  
89.31% of the traffic for the switch facing REANNZ  
83.22% for the switch facing WIX

Very little traffic is dropped.  
959 bytes at REANNZ' facing switch  
42.60 KB at WIX facing switch

Normalized cumulative distribution of the traffic

