RPKI – Resource Public Key Infrastructure
Origin Validation in BGP

Alejandro Acosta

alejandro @ lacnic.net

Who can use a resource?

Who can use a resource?

- When an organization receives Internet number resources (IPv6/IPv4/ASN):
  - It informs its upstream/peers which prefixes it will announce
  - Via e-mail, web forms, IRR (Internet Routing Registry)

Providers/peers:
verify the right to use

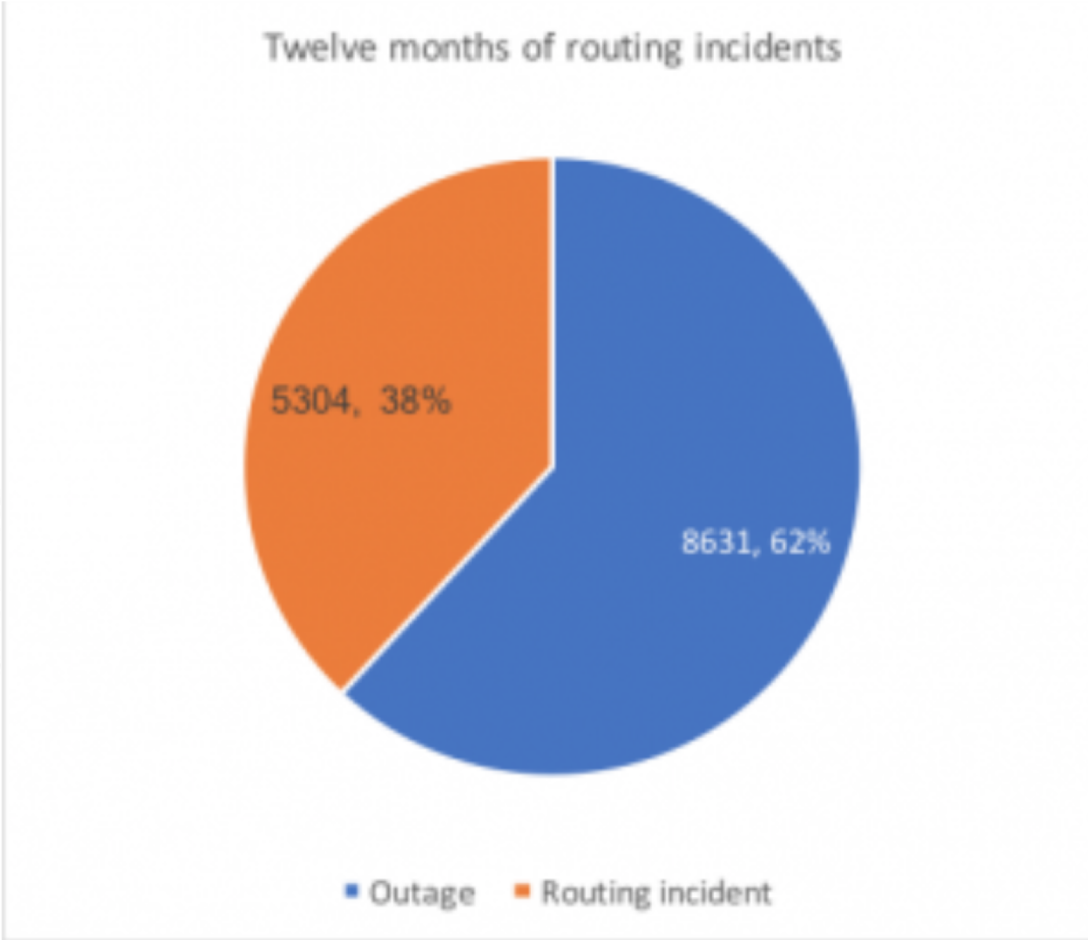
RIRs Whois: Data not digitally signed, cannot be used directly for routing

IRR Whois: Data not digitally signed, few mechanisms to authenticate the right to use

- Verification is not alwayss as thorough as it should be
- The system's integrity depends on **trust among peers**

Routing incidents in 2017

- Approx. 14,000 routing incidents (including leaks/hijacks and outages) – **Over 38 cases per day**
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks caused at least one incident



Source: https://blog.apnic.net/2018/01/24/14000-incidents-routing-security-2017/

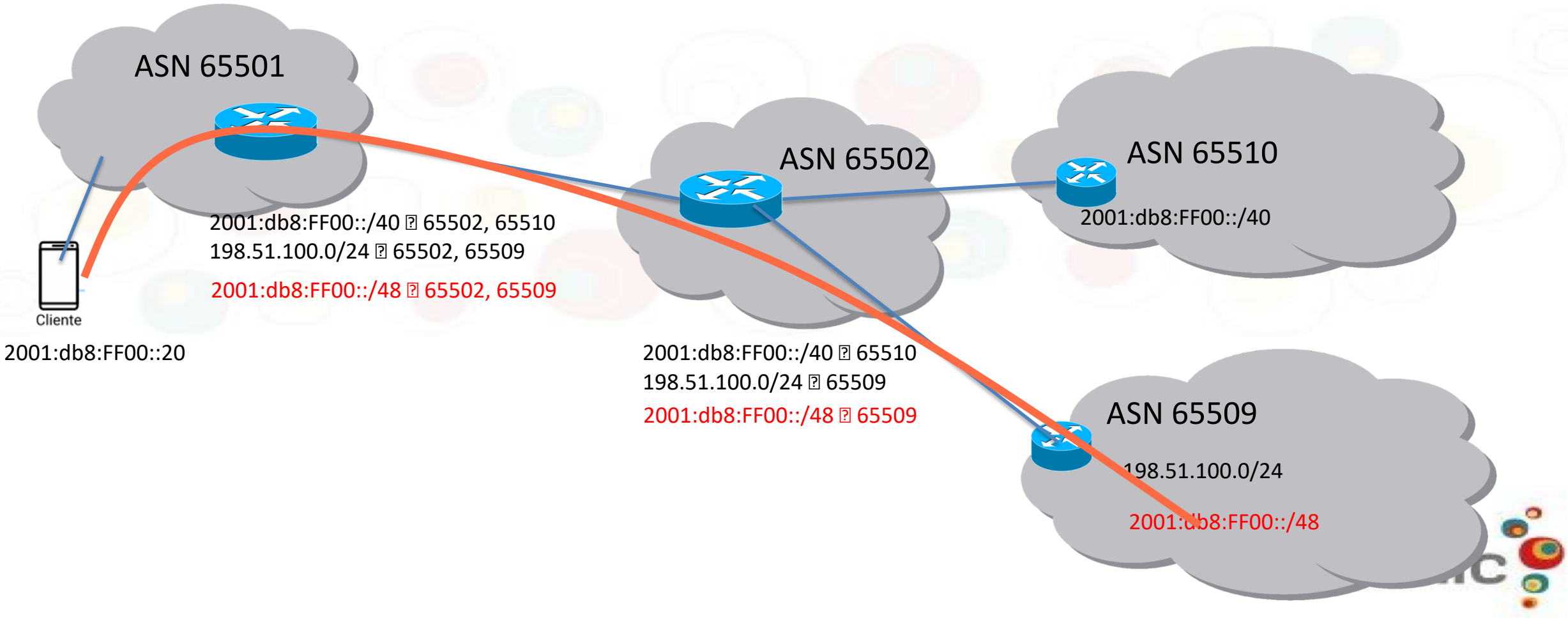
lacnic

Let’s recap the two most common incidents

1) Route hijacking

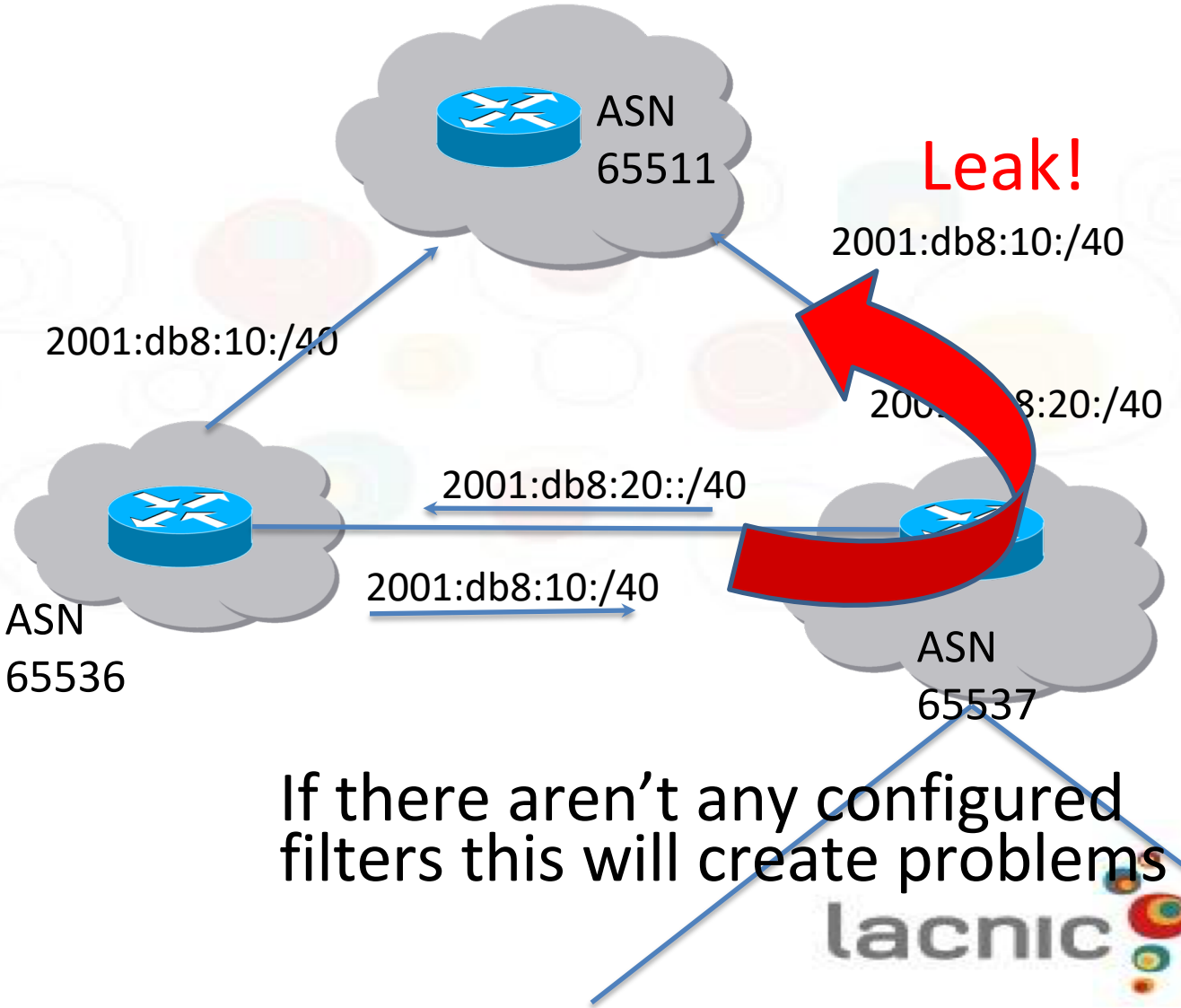
Route hijacking:
Act of announcing NON authorized prefixes

- Intentional.
- Operational mistake



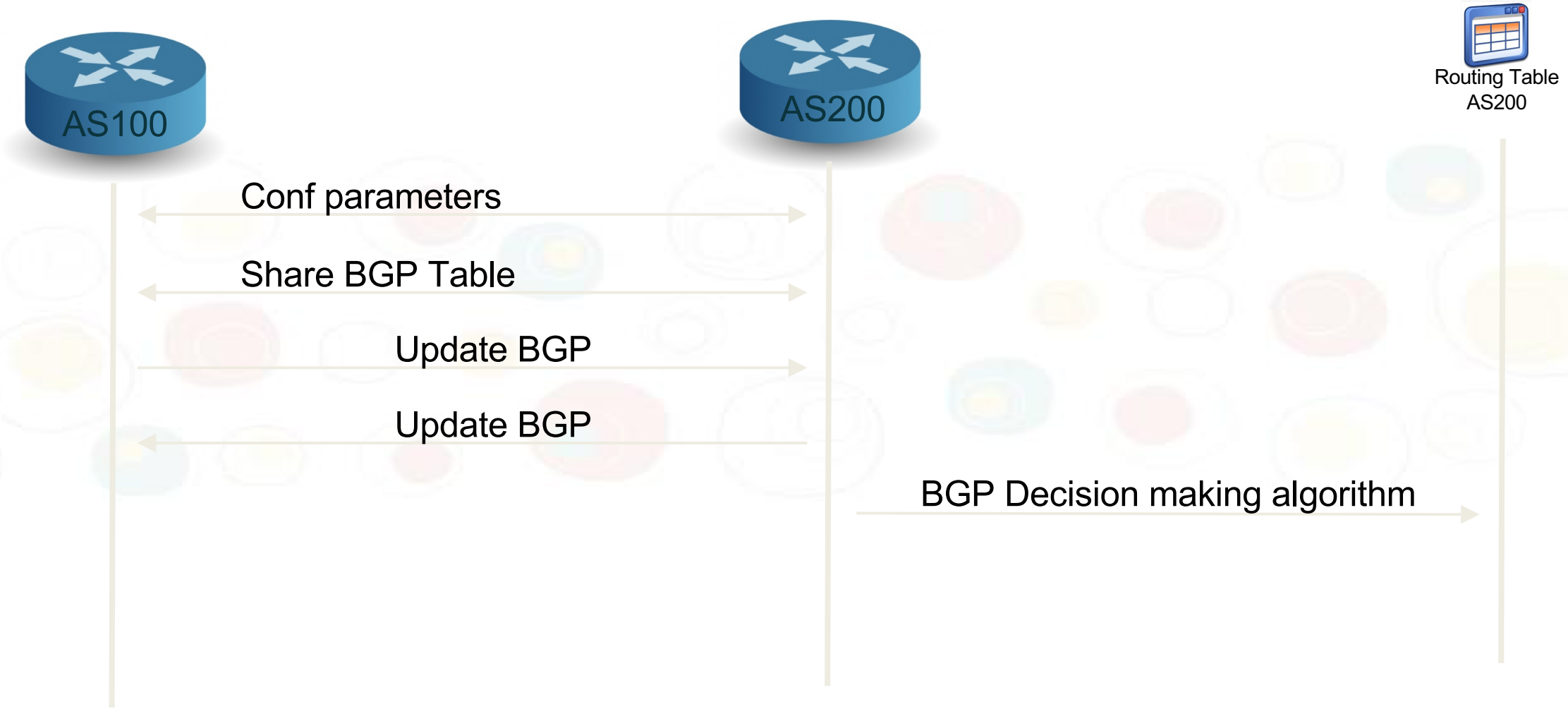
2) Route leaks

- Prefixes learnt from the ***provider*** must not be announced to another ***peer*** or ***provider***
- Prefixes learnt from a ***peer*** also must not be announced to other ***peers*** or to the ***provider***
- These prefixes should only be announced to ***clients***

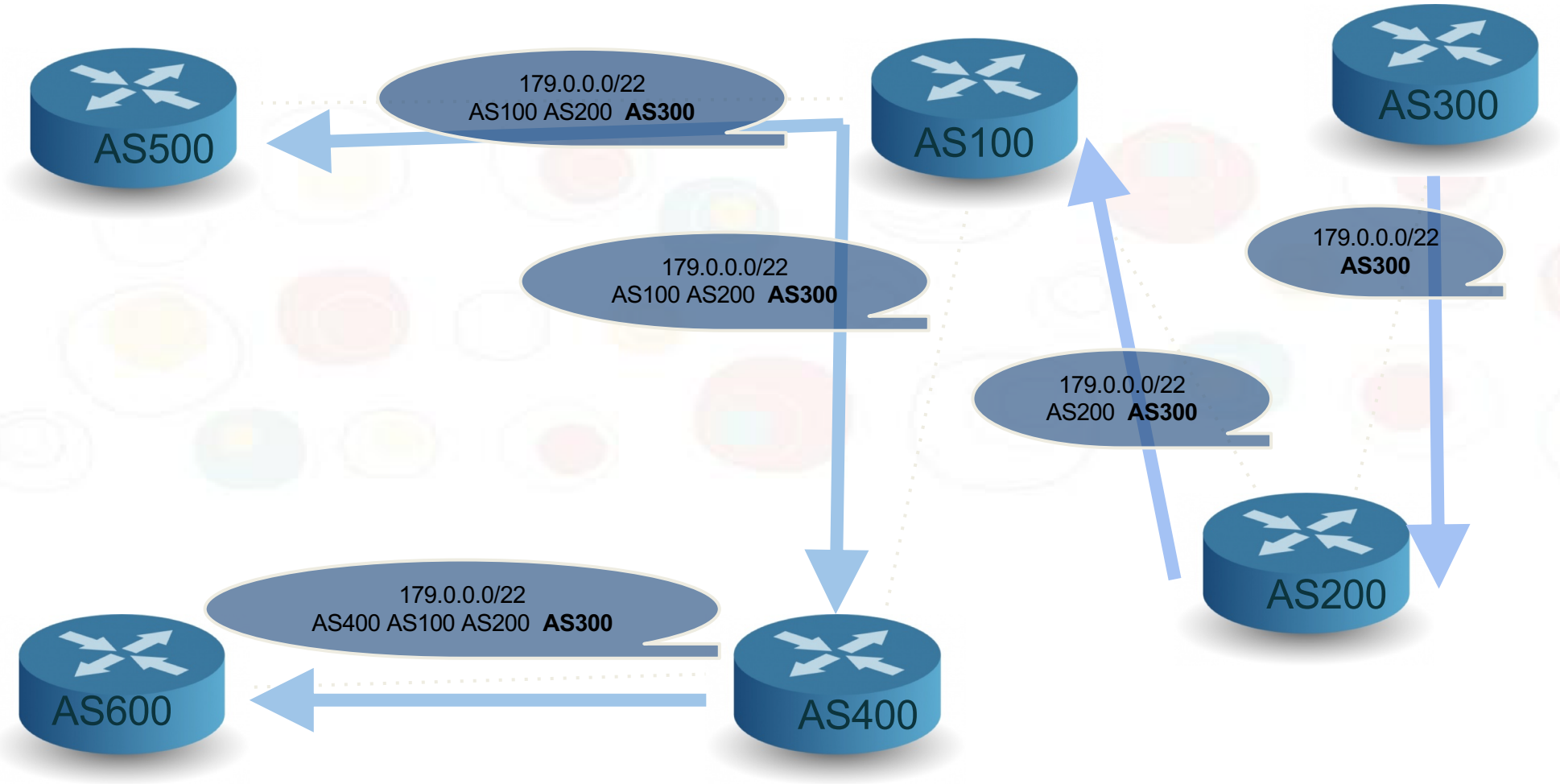


Now let’s review some concepts of BGP

BGP – How Internet Works



Update BGP



Who originatedl 179.0.0.0/22?

AS 300

Who are the neighbors of AS100?

AS 200, AS 400, AS 500

Who else announces the prefix?

AS 200, AS 100, AS 400

Who learned the prefix?

ALL

RPKI

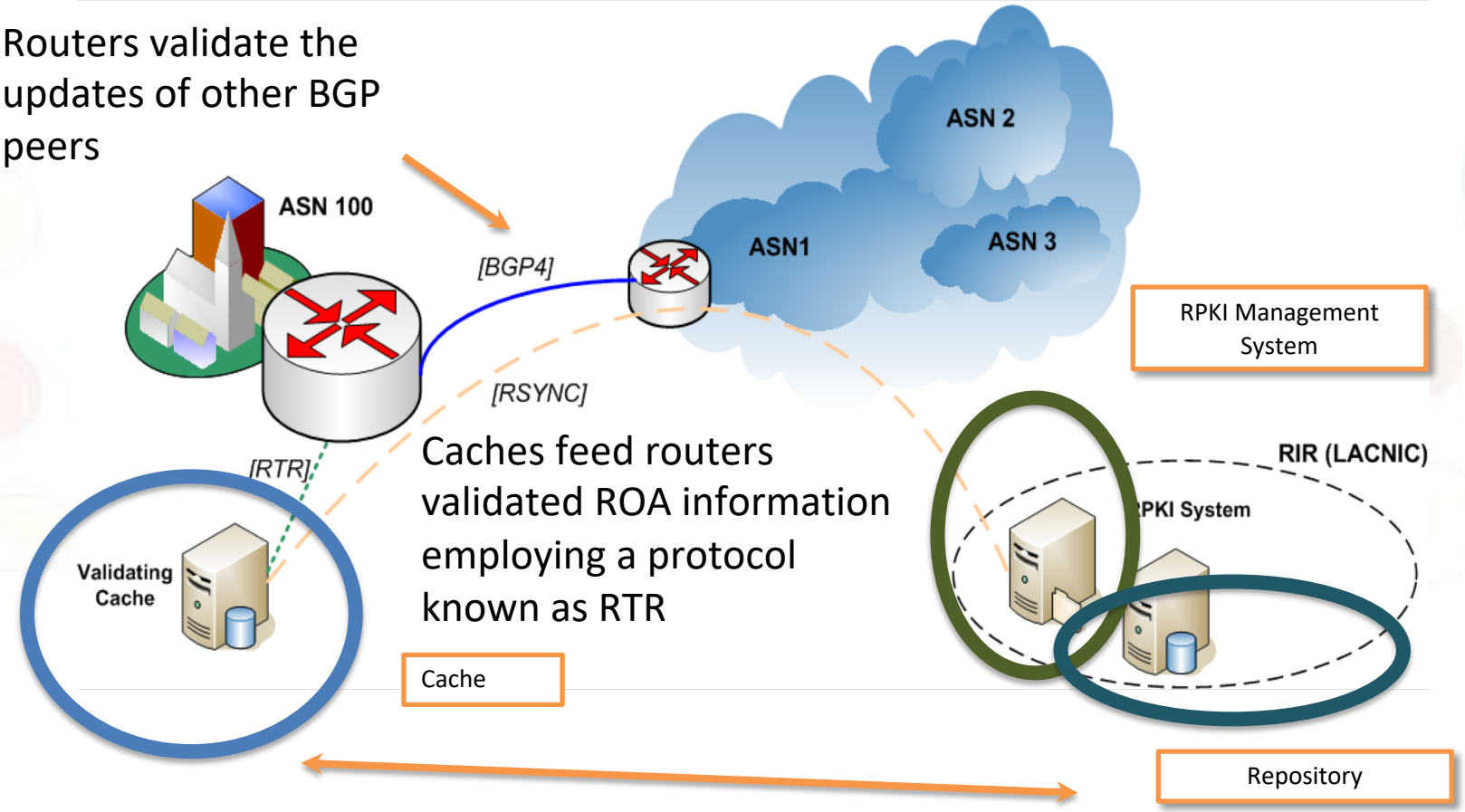
What is RPKI?

- RPKI (Resource Public Key Infrastructure)
- Validation of the right to use a resource
  - IPv4
  - IPv6
  - Autonomous System
- Combines:
  - Hierarchical resource allocation through the RIRs
  - Use of X.509 digital certificates
- Standardization work by the IETF SIDR Working Group, RFCs 6480-6492
  - Great implementation work by the RIRs

lacnic

RPKI in Action

Routers validate the updates of other BGP peers



Caches fetch and cryptographically validate the certificates and ROAs from the repositories

Some examples

What is the router going to do? How does the validation takes place?

Origin Validation

UPDATE 200.0.0.0/9
ORIGIN-AS 20

VALID

max_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- If the prefix in the UPDATE message is not covered by any of the entries in the ROA table -> **not found**
- If the prefix in the UPDATE message is covered by at least one entry in the ROA table and the origin AS matches the AS in the table -> **valid**
- If the origin AS does not match -> **invalid**

Origin Validation

UPDATE 200.0.0.0/22
ORIGIN-AS 20

INVALID

[Prefix / Max_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- If the prefix in the UPDATE message is not covered by any of the entries in the ROA table -> **not found**
- If the prefix in the UPDATE message is covered by at least one entry in the ROA table and the origin AS matches the AS in the table -> **valid**
- If the origin AS does not match -> **invalid**

lacnic

Origin Validation

UPDATE 200.0.0.0/9
ORIGIN-AS 66

INVALID

[prefix, max_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- If the prefix in the UPDATE message is not covered by any of the entries in the ROA table -> **not found**
- If the prefix in the UPDATE message is covered by at least one entry in the ROA table and the origin AS matches the AS in the table -> **valid**
- If the origin AS does not match -> **invalid**

lacnic

Origin Validation

UPDATE 189.0.0.0/9
ORIGIN-AS 66

NOT FOUND

	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- If the prefix in the UPDATE message is not covered by any of the entries in the ROA table -> **not found**
- If the prefix in the UPDATE message is covered by at least one entry in the ROA table and the origin AS matches the AS in the table -> **valid**
- If the origin AS does not match -> **invalid**

lacnic

RPKI as Routing Policy

- ISPs and organizations may ***define and certify the route announcements they authorize***
  - Using digital objects known as ROAs
  - Signed with the certificate's private key
  - Equivalent to th route/route6 objects of an IRR (except in this case they are digitally signed)
- A major step towards increased routing security
  - Allows validating the Autonomous System that originates an announcement via BGP (origin validation)

Applying RPKI in an IXP

- The **{valid, invalid, not found}** status of a prefix can be a factor in route selection

```
route-map rpki permit 10
match rpki not-found
set local-preference 100

route-map rpki permit 20
match rpki valid
set local-preference 200

!descartamos invalidas
```

Questions?

Thank you!