



**RIPE
NCC**

Routing Security

3 March 2014

Massimiliano Stucchi
Ferenc Csorba

10:00 - 11:15	First Session
11:15 - 11:30	Break
11:30 - 13:00	Second Session
13:00 - 14:00	Lunch
14:00 - 16:00	Afternoon Session

- Introduction to the Routing Registry
- RIPE Database
- Routing Policy Specification Language
- Certification
- Transfers

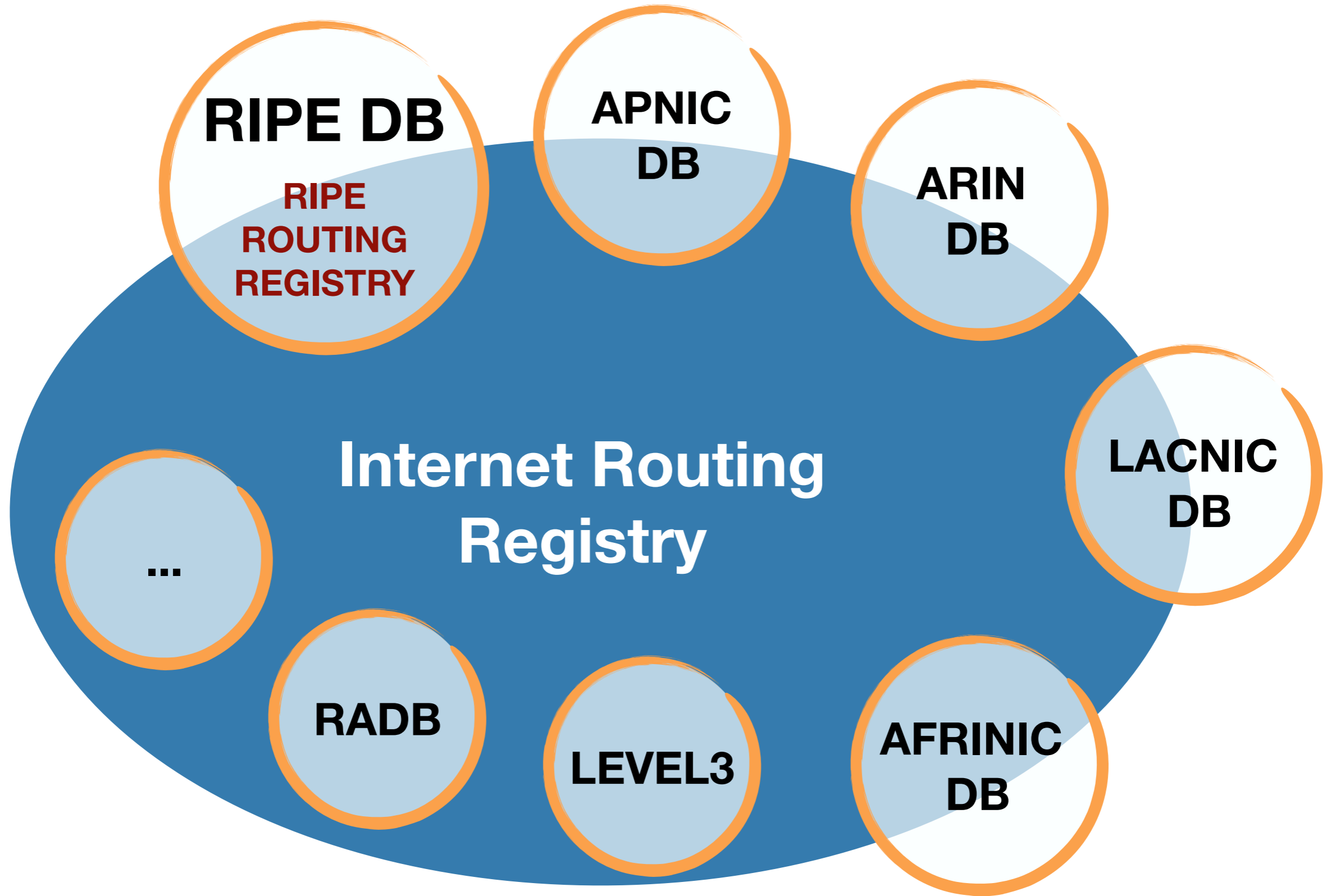


Introduction to the Routing Registry

1



- Several public databases that contain routing policy information that mirror each other:
 - RIPE, APNIC, RADB, JPIRR, Level3, etc.
 - <http://www.irr.net>
- RIPE NCC operates the RIPE Routing Registry
 - Part of the RIPE Database
 - Part of the Internet Routing Registry



- To be able to answer the question:
 - Is that ASN authorised to originate that address range?

- What prefixes do you announce?
- Who are your neighbours?
 - Peers, transits and customers
- Which prefixes do you accept from them?
- What are your preferences?

- Some transit providers and IXPs (Internet Exchange Points) require it for filtering
- Contributes to make routing more secure and stable
- Can help with troubleshooting

- Close relation between registry information and routing policy
 - The holder of the resource knows how it should be routed
- The Routing Policy Specification Language (RPSL) originates from a RIPE Document
 - Shares attributes with the RIPE Database

- Accuracy and completeness
- Not every Routing Registry is linked directly to an Internet Registry
 - Online verification of the resource holder is needed
- Different authorisation methods
- Mirrors are not always up to date





RIPE Database

2



- Public internet resource and routing registry database
 - All internet resources (IPv4, IPv6, AS numbers) are registered
 - Provides contact information
 - It is also the RIPE Routing Registry with routing policy information

- **inetnum** = IPv4 address range
- **inet6num** = IPv6 address range
- **aut-num** = AS number
- **route, route6** = address range announced by an AS number

inet6num: 2001:db8::/32

org: ORG-BB2-RIPE
admin-c: LA789-RIPE
tech-c: LA789-RIPE
admin-c: JD1-RIPE
mnt-by: RIPE-NCC-HM-MNT

person: John Doe

nic-hdl: JD1-RIPE
address: Sesame Street 1
phone: +1 555 0101
email: john@xmpl.org
mnt-by: RED-MNT

route6: 2001:db8::/32


tech-c: LA789
admin-c: JD1-RIPE
origin: AS2
mnt-by: LIR-MNT

Add passwords

Session passwords

0 stored password(s) ?

121ir +



inet6num: 2001:db8::/32

tech-c: LA789-RIPE
admin-c: JD1-RIPE
mnt-by: RIPE-NCC-HM-MNT
mnt-by: LIR-MNT

aut-num: AS2

tech-c: LA789-RIPE
admin-c: JD1-RIPE
mnt-by: RIPE-NCC-HM-MNT
mnt-by: LIR-MNT

route6: 2001:db8::/32

tech-c: LA789
admin-c: JD1-RIPE
origin: AS2
mnt-by: LIR-MNT

Add passwords

Session passwords

0 stored password(s)

121ir



inet6num: 2001:db8::/32

tech-c: LA789-RIPE
admin-c: JD1-RIPE
mnt-by: RIPE-NCC-HM-MNT
mnt-by: LIR-MNT

aut-num: AS2

tech-c: LA789-RIPE
admin-c: JD1-RIPE
mnt-by: RIPE-NCC-HM-MNT
mnt-by: AS-MNT
mnt-routes: LIR-MNT

```
inet6num:      2001:db8::/32
```

```
org:           ORG-BB2-RIPE  
admin-c:      LA789-RIPE  
tech-c:       LA789-RIPE  
admin-c:      JD1-RIPE  
mnt-by:       RIPE-NCC-HM-MNT  
mnt-routes:   LIR-MNT  
mnt-routes:   AS-MNT
```





Exercise: Create a route or a route6 Object

3



- Group A
 - Create a route object for your IPv4 allocation
 - List your AS Number as the origin
- Group B
 - Create a route6 object for your IPv6 allocation
 - List your AS Number as the origin





RPSL

4

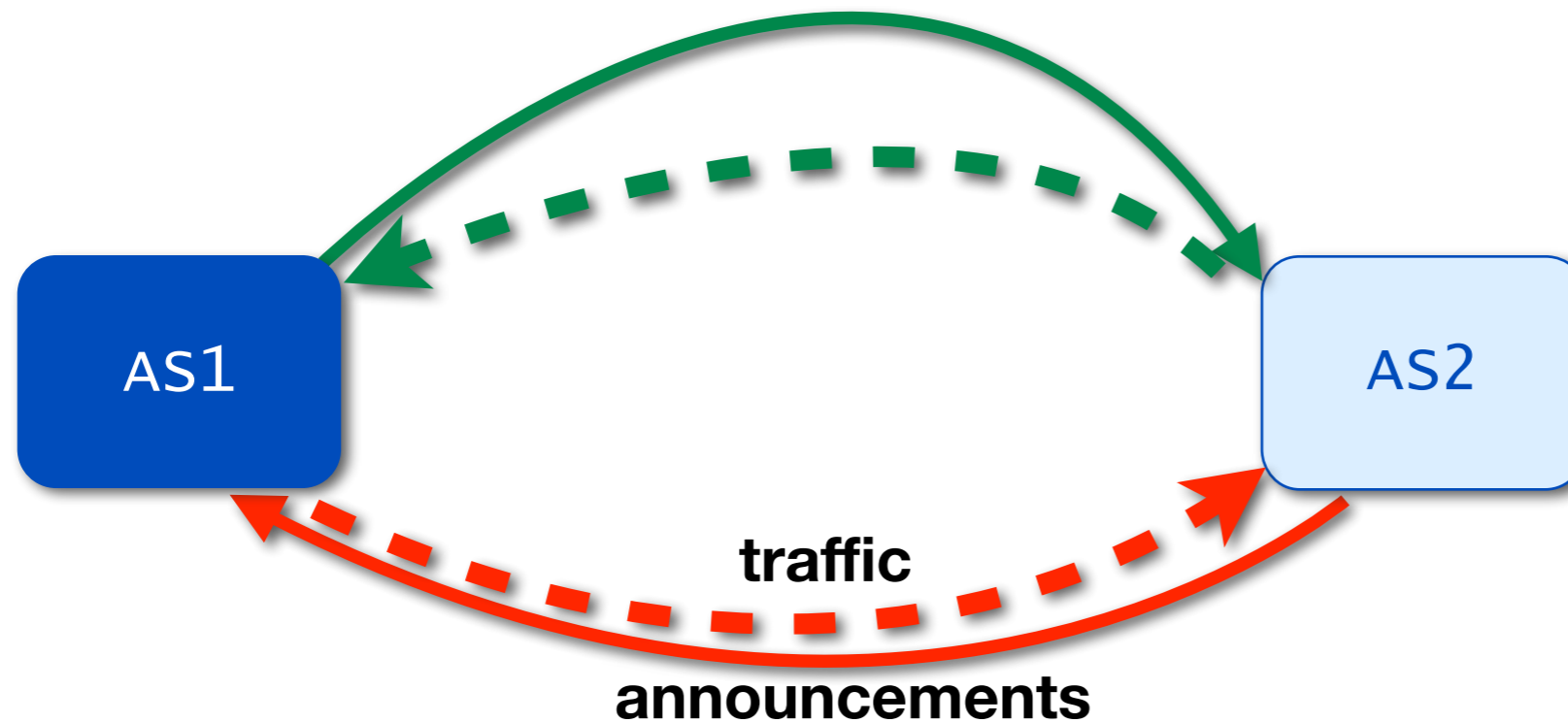


- A routing policy describes how a network works:
 - Who do you connect with
 - Which prefixes or routes do you announce
 - Which routes do you accept from others
 - What are your preferences
- In your router, this is your BGP configuration
 - Neighbours
 - route-maps
 - localpref

- Language used by the IRRs
- Not vendor specific
- Documented in RFC 2622 and 2650
- Can be translated into router configuration

- route or route6 object
 - Connects a prefix to an origin AS
- aut-num object
 - Registration record of an AS Number
 - Contains the routing policy
- Sets
 - Objects can be grouped in sets, i.e. as-set, route-set
- Keywords
 - “ANY” matches every route

- AS Numbers are written as ASxxx
- Prefixes are written in CIDR notation
 - 193.0.4.0/24
- Any value can be replaced by a list of values of the same type
 - AS1 can be replaced by “AS1 AS2 AS3”
- You can reference a set instead of a value
 - “...announce AS1” or “...announce as-myname”



```
aut-num: AS1
```

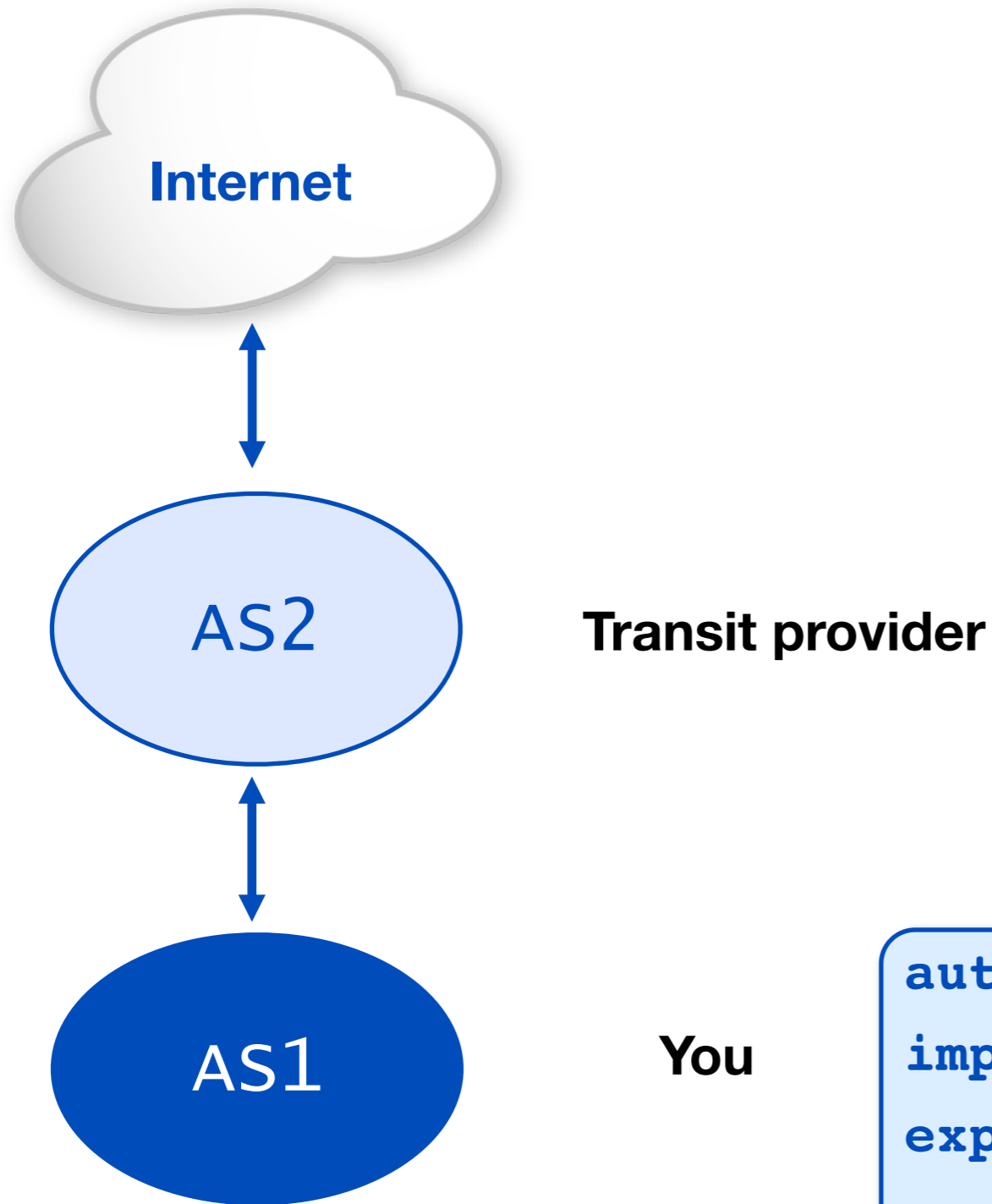
```
import: from AS2 accept AS2
```

```
export: to AS2 announce AS1
```

AS1 accepts prefixes **from** AS2 that originate in AS2.
Outbound traffic for AS2 can go **towards** AS2

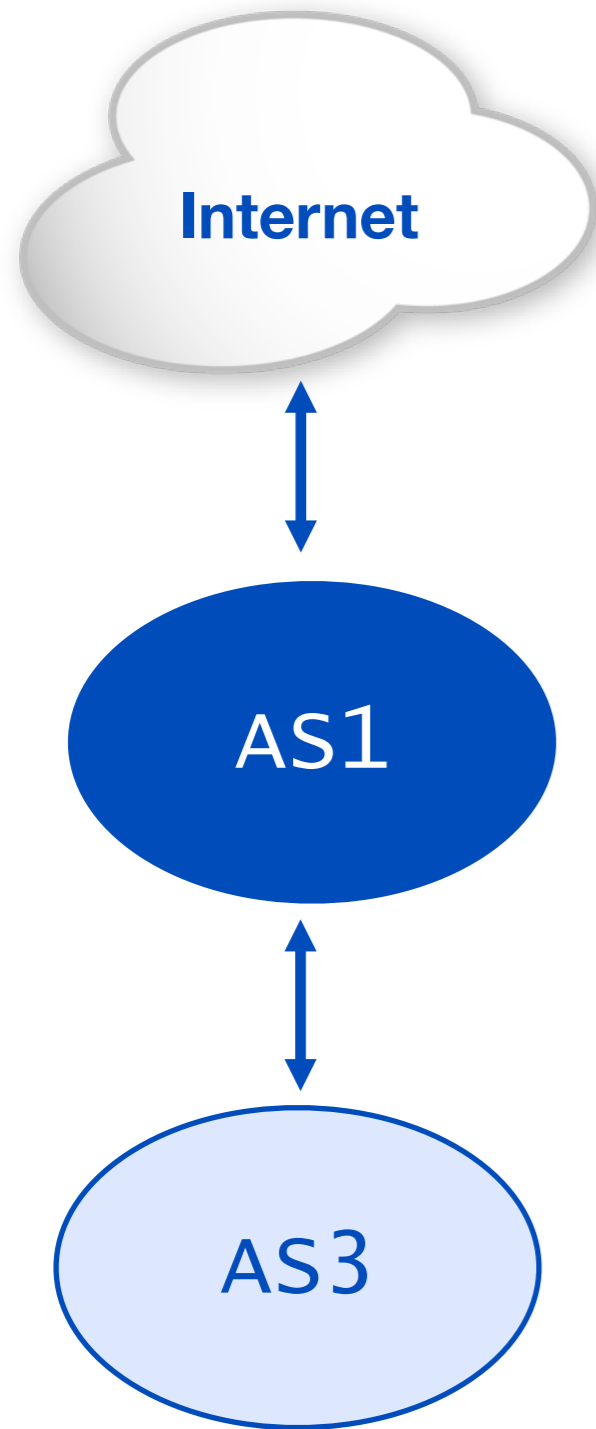
AS1 announces prefixes (originating in AS1) **to** AS2.
Incoming traffic for AS1 can flow **from** AS2

3 scenarios: 1. You are downstream



```
aut-num: AS1
import: from AS2 accept ANY
export: to AS2 announce AS1
```

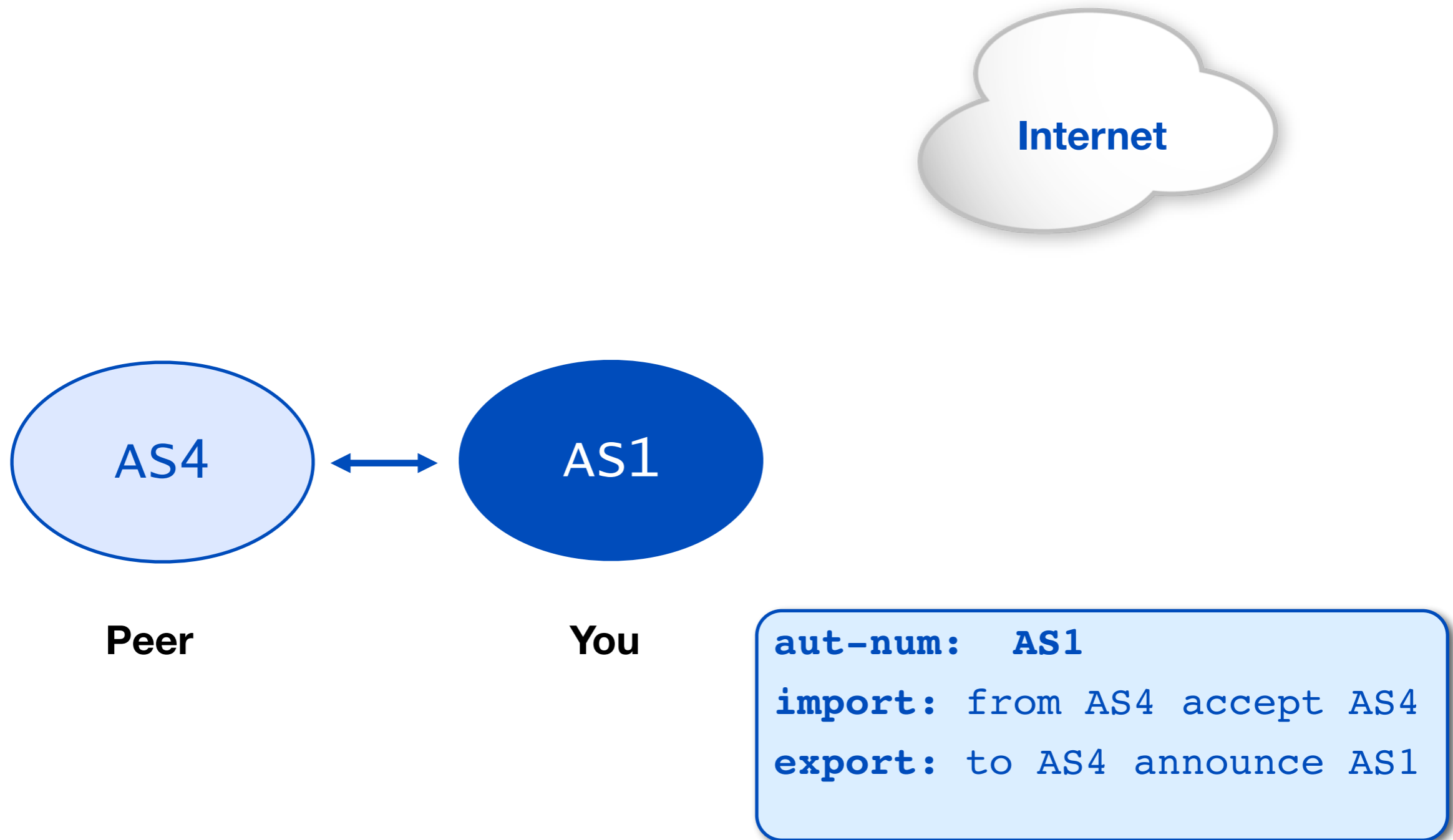
3 scenarios: 2. You are upstream



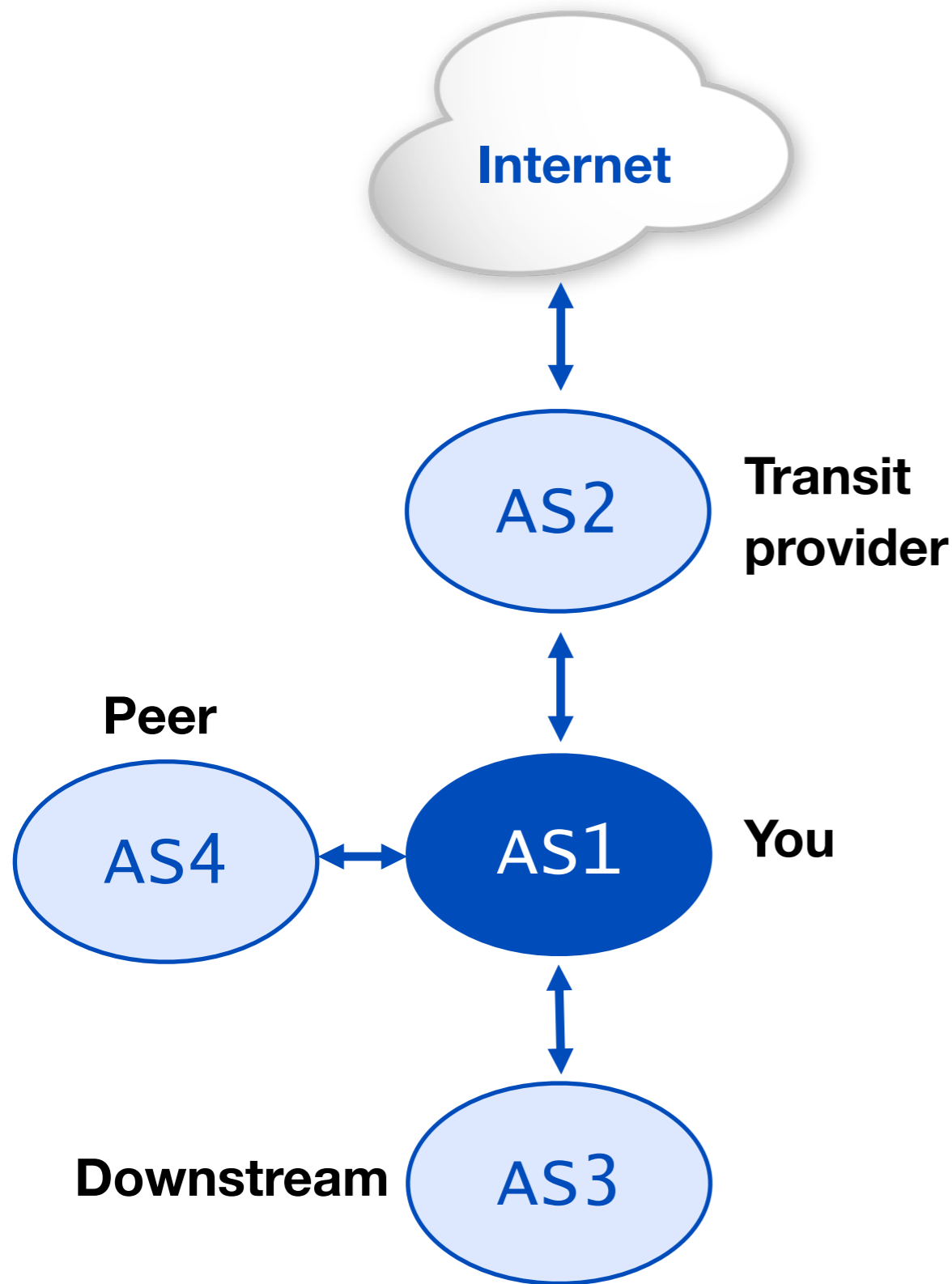
You

```
aut-num: AS1
import: from AS3 accept AS3
export: to AS3 announce ANY
```

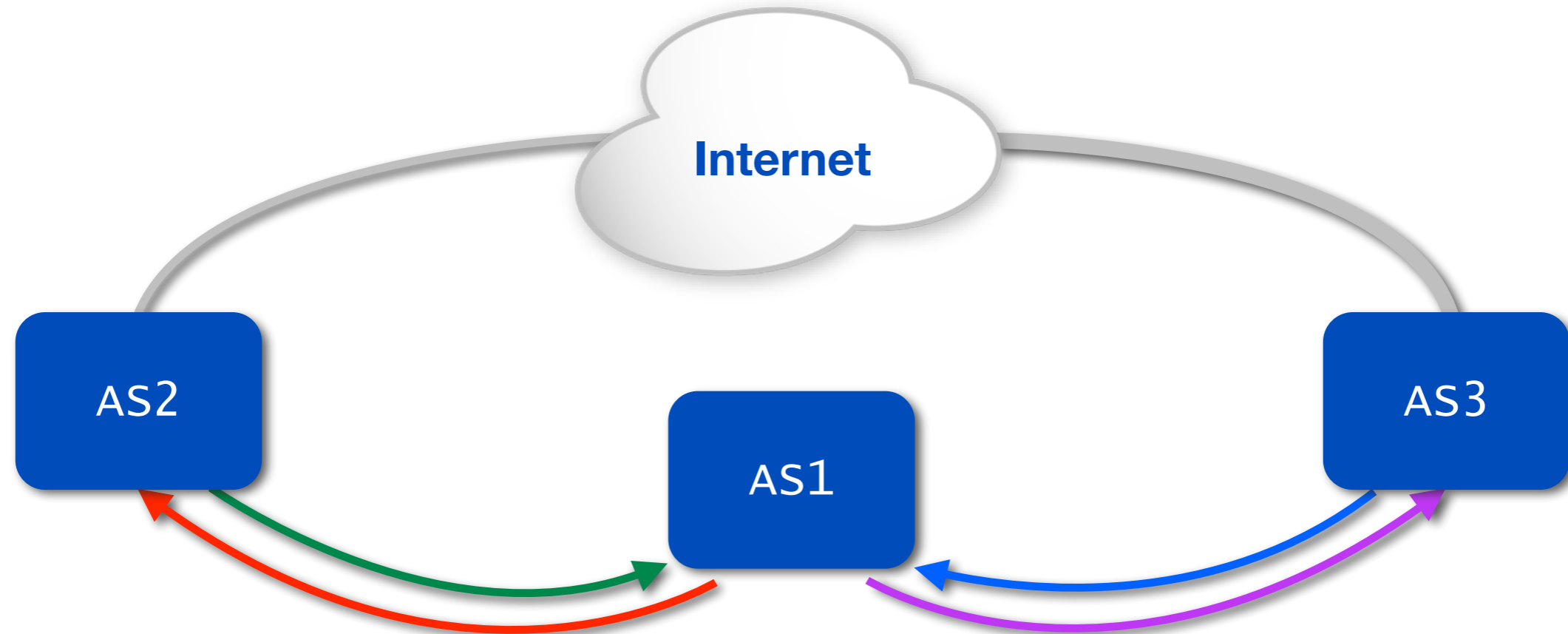
Downstream customer



3 scenarios: Summary



```
aut-num: AS1
import: from AS2 accept ANY
export: to AS2 announce AS1 AS3
import: from AS3 accept AS3
export: to AS3 announce ANY
import: from AS4 accept AS4
export: to AS4 announce AS1 AS3
```



aut-num: AS2

```
import: from AS1 accept AS1
export: to AS1 announce AS2
```

aut-num: AS1

```
export: to AS2 announce AS1
import: from AS2
        accept AS2
import: from AS3
        accept ANY
export: to AS3 announce AS1
```

aut-num: AS3

```
export: to AS1 announce ANY
import: from AS1 accept AS1
```

- RPSL is older than IPv6, the default is IPv4
- IPv6 was added later using a different syntax
 - You have to specify that it's IPv6

```
mp-import:    afi ipv6.unicast from AS201 accept AS201  
mp-export:    afi ipv6.unicast to AS20 announce ANY
```



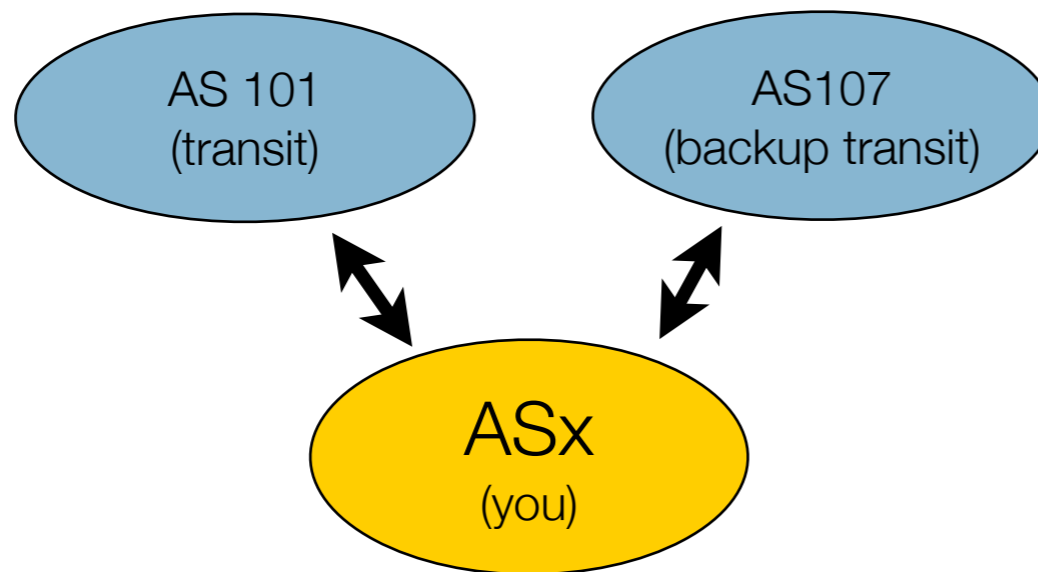


Exercise: Describing Your Policy

5



- Take the scenario as presented:



- In the TEST database update your AS, adding import and export attributes to describe your policy towards these neighbors





RPSL in Practice

6




```
aut-num:      AS99
as-name:      SMALL-ISP-EU
descr:        My network
remark:       *** Transit via 101 ***
import:       from AS101 accept ANY
export:       to AS101 announce AS99 AS201 AS202
remark:       *** Transit via 102 ***
import:       from AS102 accept ANY
export:       to AS102 announce AS99 AS201 AS202
remark:       *** AS201 is a customer ***
import:       from AS201 accept AS201
export:       to AS201 announce ANY
remark:       *** AS202 is a customer ***
import:       from AS202 accept AS202
export:       to AS201 announce ANY
```



- Adding and removing customers can become time consuming
- Create a set to list them all at once

```
as-set:      AS-SMALLISP
descr:      Customers' ASNs of a small ISP
members:    AS201
members:    AS202
```

- And use that to describe your policy

```
export:     to AS101 announce AS-SMALLISP
export:     to AS102 announce AS-SMALLISP
```

```
as-set: AS4:AS-CUSTOMERS
```

```
members: AS7, AS5, AS8
```

```
aut-num: AS4
```

```
export: to AS3 announce AS4 AS4:AS-customers
```

```
export: to AS4:AS-CUSTOMERS announce ANY
```

```
import: from AS4:AS-CUSTOMERS accept PeerAS
```

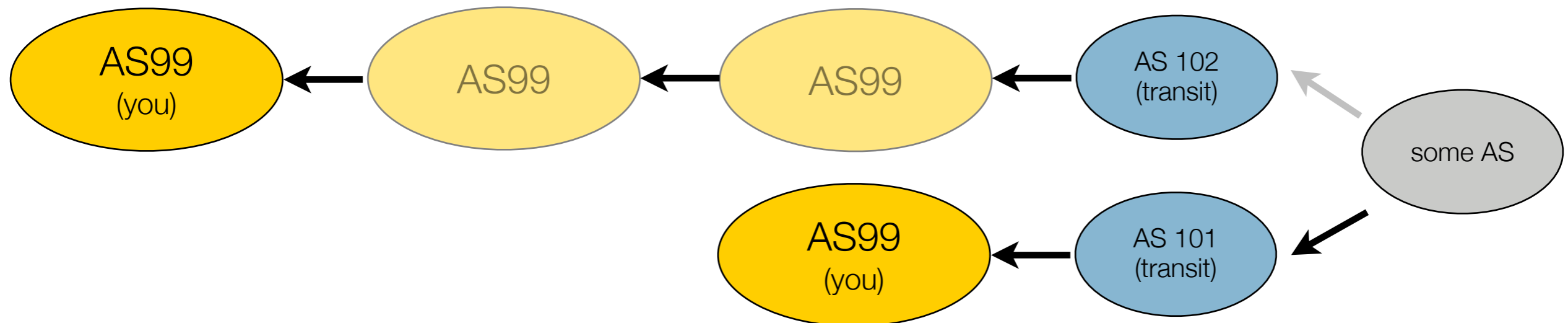
- peerAS means
 - from AS5 accept AS5
 - from AS7 accept AS7
 - from AS8 accept AS8

- BGP uses “localpref” to influence which received routes you want to prefer
- In RPSL you can use the “pref” action on your import attributes
- Important: lower value means more preferred!

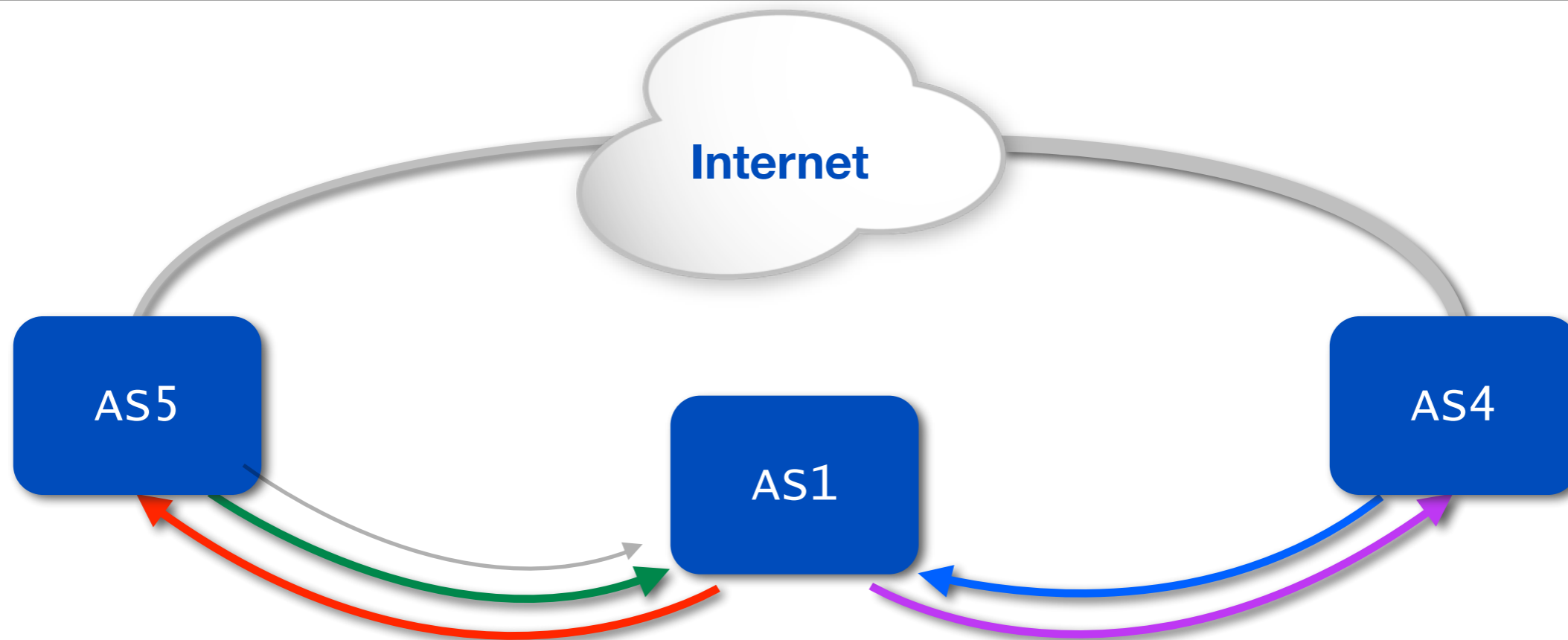
```
import:      from AS101 action pref=20;  
              accept ANY  
import:      from AS102 action pref=30;  
              accept ANY
```

- AS path prepending is used to influence routing, both inbound and outbound
- Prepending can also be notated in RPSL using another action statement:

```
export:      to AS102 action aspath.prepend  
                (AS99, AS99); announce AS-SMALLISP
```



An aut-num object (second example)



aut-num: AS5

```
import: from AS1 accept AS1
export: to AS1 announce ANY
```

aut-num: AS1

```
import: from AS4 action pref=80;
accept ANY
export: to AS4 announce AS1
import: from AS5 action pref=90;
accept ANY
import: from AS5 action pref=70
accept AS5
export: to AS5 [redacted]
action aspath.prepend (AS1, AS1);
announce AS1
```

aut-num: AS4

```
import: from AS1 accept AS1
export: to AS1 announce ANY
```



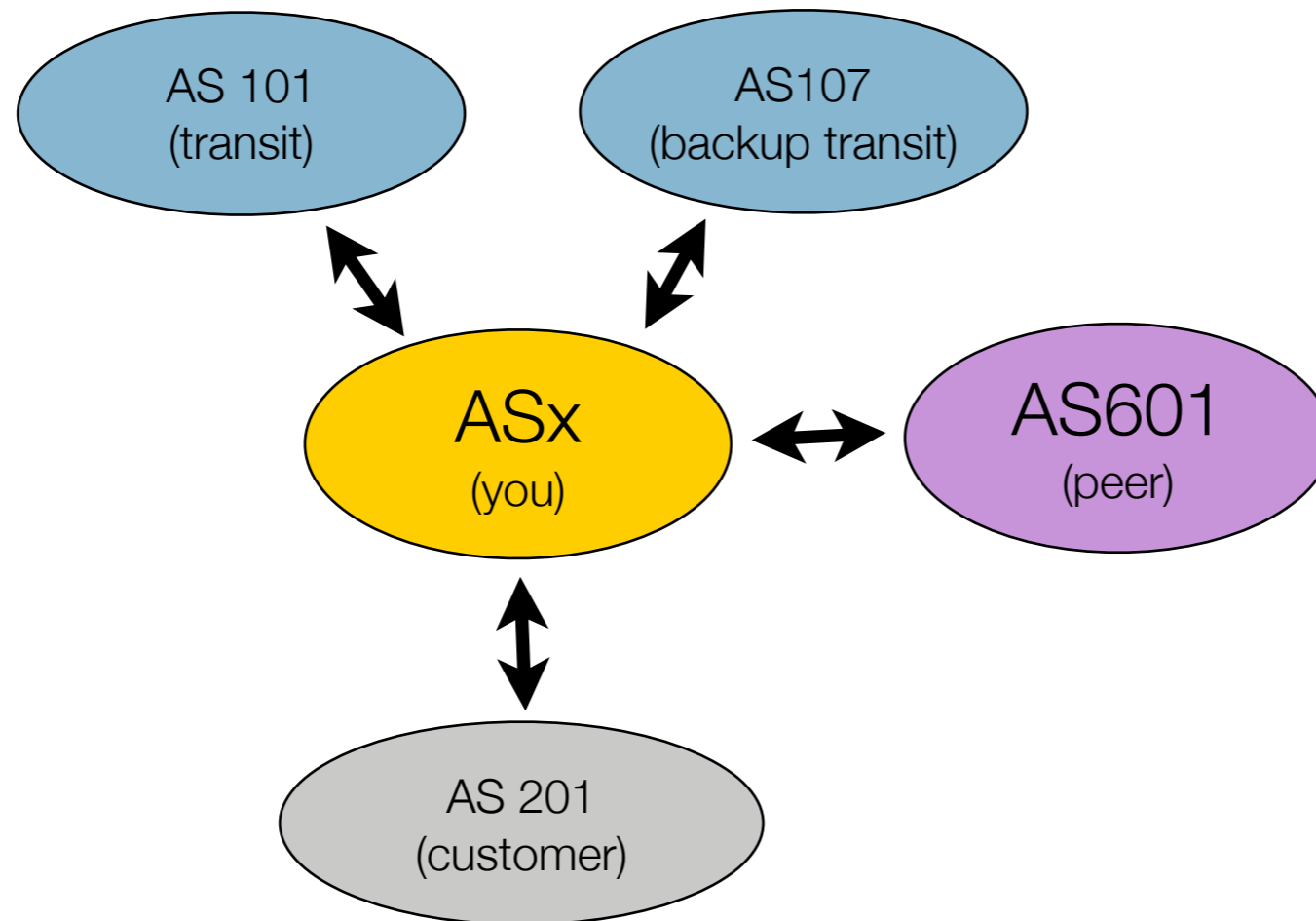


Exercise: Describing Your Policy

7



- Take the scenario as presented:



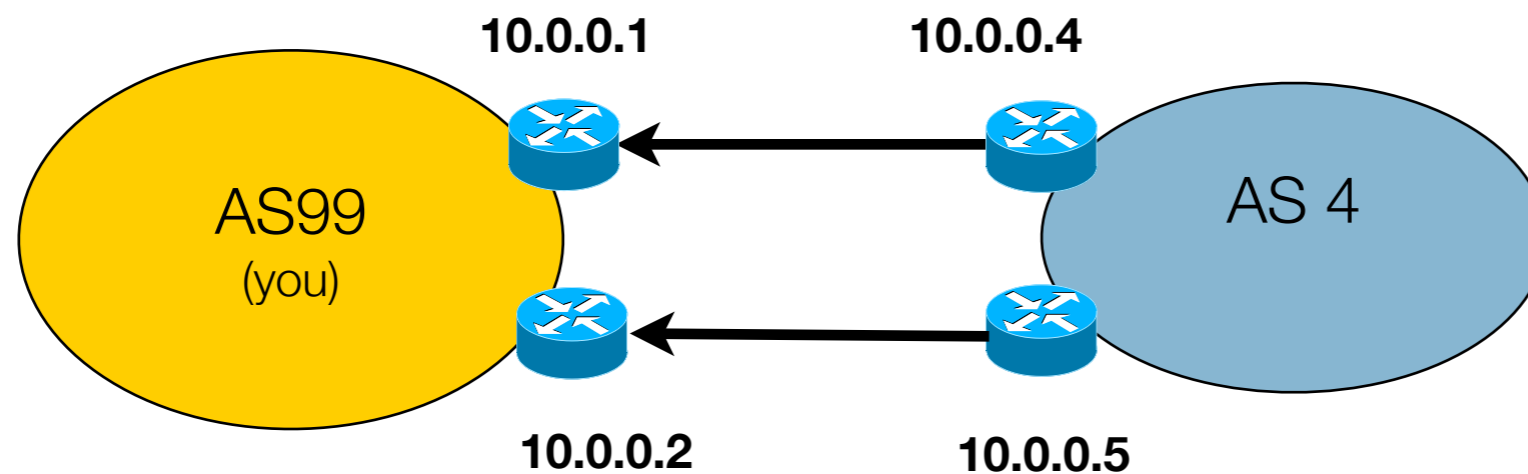
- In the TEST database update your AS, adding import and export attributes to describe your policy towards these neighbors



- Multiple Exit Discriminator
 - differentiates connections to same peer
 - “which inbound connection do I prefer?”
 - doesn’t go beyond neighbour
- Local Pref has precedence over MED
 - to honor your neighbor’s MED:
 - don’t set different prefs

```
export:    to AS4
           10.0.0.4 at 10.0.0.1
           action med=1000;
           announce AS99

export:    to AS4
           10.0.0.5 at 10.0.0.2
           action med=2000;
           announce AS99
```



- Optional tags
 - Can go through many peers
- Can be used for advanced filtering
- Not a routing parameter
- Enables customers to control their own routing policy
 - Publish your communities, and what you do with them
 - Filter incoming announcements accordingly

- Set a community:

```
import:      from AS6
             action community = { 99:100 };
             accept AS6
```

- Append a community:

```
import:      from AS7
             action community.append(99:51);
             accept AS7
```

```
export:      to AS3
             action community .= { 99:100 };
             announce ANY
```

- Delete a community:

```
import:      from AS201 action community.delete
             (99:100); accept AS201
```

```
import:      from AS21
             accept AS6 AND
             community.contains = (21:32)
```

```
import:      from AS17
             accept community(68:2)
```

```
import:      from AS1:AS-CUSTOMERS
             accept PeerAS AND
             community.contains (202:3)
```

```
export:      to AS3
             announce AS1:AS-CUST AND
             community == {1:113}
```

```
export:      to AS1:AS-PEERS
             announce ANY AND
             community.contains (1:75)
```



- You can use regular expressions in your filters
 - They are always enclosed in “< >”

```
import:      from AS201 accept <^AS201+$>
```

- Uses the standard posix notation:
 - “^” start of path
 - “\$” end of path
 - “*” zero or more
 - “+” one or more
 - “?” zero or one

- Instead of AS Numbers you can use prefixes:

```
import:    from AS2121 accept {193.0.24.0/21}
```

- Operators can be used to define ranges:
 - “ \wedge_- ” all more specifics excluding the prefix itself
 - “ \wedge_+ ” all more specifics including the prefix itself
 - “ \wedge_n ” all routes of length n in this prefix
 - “ \wedge_{n-m} ” all routes of length n to length m

- Groups literal prefixes
- Can include other route-sets and even ASNs

```
route-set: rs-bar  
descr:      All ASNs of a small ISP  
members:   5.0.0.0/8^+, 30.0.0.0/8^24-32  
members:   rs-foo^+  
members:   AS2
```

- And use that to describe/simplify your policy

```
export:     to AS101 announce RS-BAR
```

- Next to import and export there can also be a default line to describe your default policy

```
export:    to AS99 announce AS201
import:    from AS202 accept AS202
export:    to AS202 announce AS201
default:   to AS99 action pref=150
```

- Instead of all routes, you can also announce a default route

```
export:    to AS201 announce {0.0.0.0/0}
```

```
aut-num:      AS99
as-name:      SMALL-ISP-EU
descr:        My network
remark:       *** Announcements are grouped ***
import:       from AS101 accept ANY
export:       to AS101 announce AS-SMALLISP
import:       from AS102 accept ANY
export:       to AS102 announce AS-SMALLISP
remark:       *** My Customers are grouped ***
import:       from AS99:Customers accept PEERAS
export:       to AS99:Customers announce ANY
```







Exercise: Retrieving information from the Routing Registry

8



- Have a look at AS3333 in the RIPE Database
 - Find out if they have any “customer” ASNs
 - Which prefixes would you accept from AS3333 if it was your customer?
- Remember to use the real database!
- Optionally: verify the results using the tools at **<http://stat.ripe.net>**





Tools and Automation

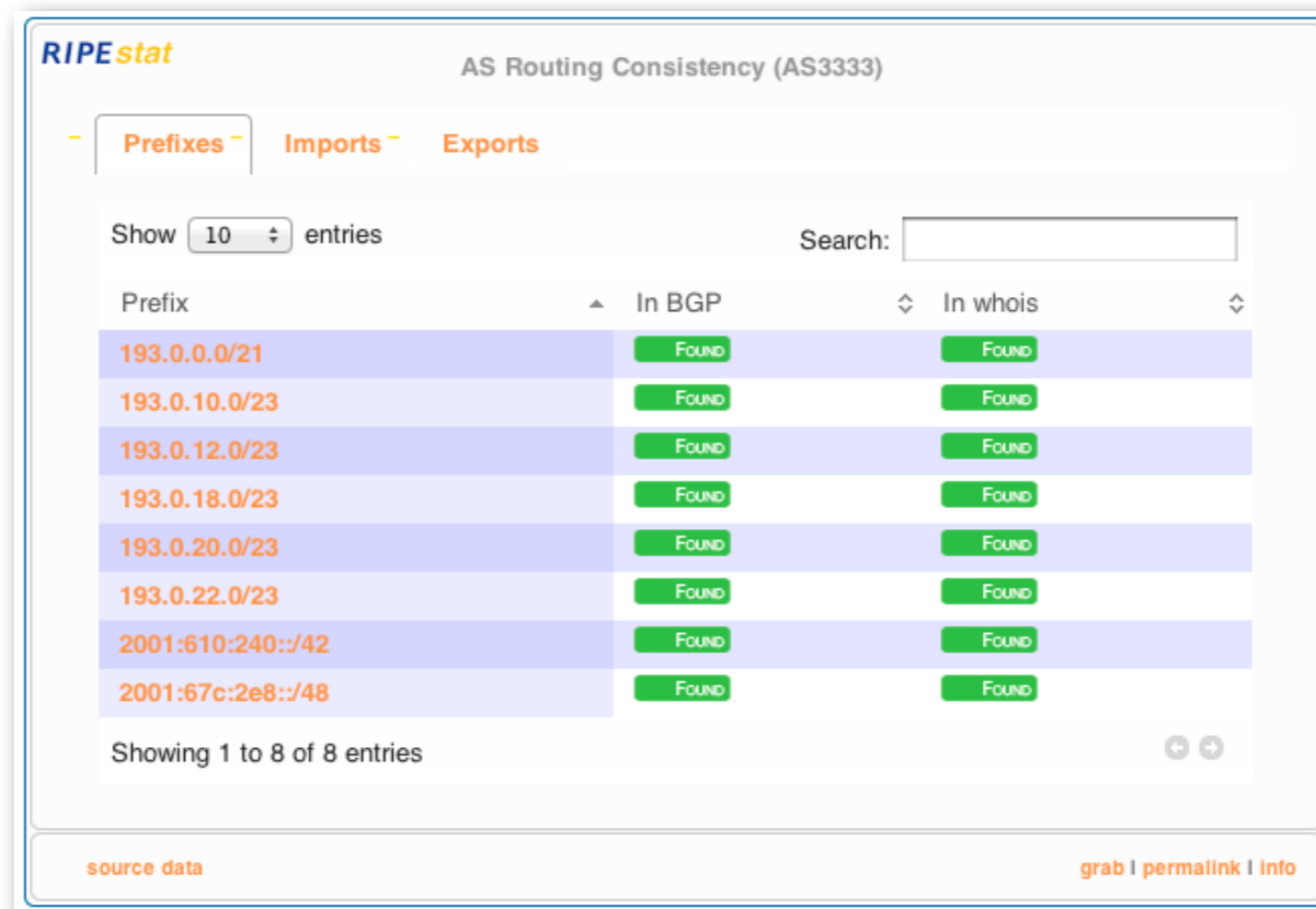
9



- There are a lot of tools around that use information in the Routing Registry
- Some can generate “complete” router configurations like the IRRToolset
- Most are open source tools
 - You can modify them to your needs
 - Some are not very well maintained

- Automation relies on the IRR being complete
 - Not all resources are registered in an IRR
 - Not all information is correct
- Check your output before using it
 - Be prepared to make manual overrides
- Tools:
 - IRRToolkit (in C++)
 - RPSLtool (perl)
 - `whois -h filtergen.level3.net RIPE::ASxxxx`

- You can compare the Routing Registry and the internet routing table using <http://stat.ripe.net>



The screenshot shows the RIPEstat interface for AS Routing Consistency (AS3333). It features three tabs: 'Prefixes' (selected), 'Imports', and 'Exports'. Below the tabs, there is a 'Show 10 entries' dropdown and a 'Search:' input field. The main content is a table with columns for 'Prefix', 'In BGP', and 'In whois'. The table lists eight prefixes, all of which are marked as 'FOUND' in both columns. At the bottom of the table, it says 'Showing 1 to 8 of 8 entries'. Below the table, there are links for 'source data', 'grab', 'permalink', and 'info'.

Prefix	In BGP	In whois
193.0.0.0/21	FOUND	FOUND
193.0.10.0/23	FOUND	FOUND
193.0.12.0/23	FOUND	FOUND
193.0.18.0/23	FOUND	FOUND
193.0.20.0/23	FOUND	FOUND
193.0.22.0/23	FOUND	FOUND
2001:610:240::/42	FOUND	FOUND
2001:67c:2e8::/48	FOUND	FOUND





Resource Certification

10



- To be able to answer the question:
 - Is that ASN authorised to originate that address range?

- Why yet another system?
 - Lots of Routing Registries
 - Not all mirroring each other
 - Different levels of trustworthiness and authentication
- RPKI replaces RR or lives side by side?
 - Side by side: different advantages
 - Security, almost real time, simple interface: RPKI
 - More information in: RR

- Usable toolset
 - No installation required
 - Easy to configure manual overrides
- Tight integration with routers
 - Supported routers have awareness of RPKI validity states

- RIPE NCC issues digital certificates
 - To LIRs only (more info coming soon!)
 - Upon request
- Certificate lists all resources held by the member

- Everything for which we are 100% sure who the owner is:
- Provider Aggregatable (PA) IP addresses
- Provider Independent (PI) IP addresses marked as “infrastructure” of the LIR

- Other resources will be added soon!
 - PI addresses for which we have a contract
 - ERX resources

- RPKI system:
- RIPE NCC holds self-signed root certificate for all resources they have in the registry
 - Signed by the root's private key
- The root certificate is used to sign all certificates for members listing their resources
 - Signed by the root's private key

- Route Origin Authorisation
- LIRs can use their certificate to create a ROA for each of their resources (address ranges)
- ROA states:
 - Address range
 - Which AS number this is announced from (freely chosen)
 - Maximum length (freely chosen)
- You can have multiple ROAs for an IP range
- ROAs can overlap

ROA

193.0.24.0/21

AS2121

Max Length: _

193.0.24.0/21 

193.0.24.0/22 

193.0.30.0/23 

ROA

193.0.24.0/21

AS2121

Max Length: /23

193.0.24.0/21 ✓

193.0.24.0/22 ✓

193.0.28.0/22 ✓

193.0.24.0/23 ✓

193.0.26.0/23 ✓

193.0.28.0/23 ✓

193.0.30.6/23 ✓



Examples with ROAs (3)

ROA

193.0.24.0/21
AS2121
Max Length: _

193.0.24.0/21 ✓

193.0.24.0/22

193.0.28.0/22 ✗

ROA

193.0.24.0/23
AS2121
Max Length: /24

ROA

193.0.30.0/23
AS2121
Max Length: _

/23

/23

/23

/23 ✓

/24 /24 ✓

/24 /24

/24 /24

/24 /24







Demonstration: Setting up Certification

11



My LIR

- Home >
- LIR Contacts >
- Communication Preferences >
- Manage Users >
- Add Users >

Tools

- LIR Locator >
- Training >

Edit John Smith (john@smith.name)

Title

As an admin, you can grant and revoke access to and from your LIR.

Groups billing certification general resources ticketing

Assign admin privileges to this user

UPDATE USER

My LIR

- Home >
- LIR Contacts >
- Communication Preferences >
- Manage Users >
- Add Users >

Resource Certification

- Dashboard >
- ROA Configuration >
- History >

Tools

- LIR Locator >
- Training >

Certificate Authority Setup

You currently do not have a Certificate Authority for your registry *fi.notexist42*.
Would you like to create your Certificate Authority?

RIPE NCC Certification Service Terms and Conditions

Introduction

This document will stipulate the Terms and Conditions for the RIPE NCC Certification Service. The RIPE NCC Certification Service is based on Internet Engineering Task Force (IETF) standards, in particular RFC3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC3779, "X.509 Extensions for IP Addresses and AS Identifiers", and the "Certificate Policy (CP) for the Resource PKI (RPKI)".

By clicking on 'I accept' below you confirm that that you have read, understood and agree to the [RIPE NCC Certification Service Terms and Conditions](#).

I accept. Create my Certificate Authority

My LIR

Home >
LIR Contacts >
Communication Preferences >

Resource Certification

Dashboard >
ROA Configuration >
History >

Tools

LIR Locator >
Training >
E-Learning >
Glossary >
Events >
RIPE Atlas >
RIPEstat >
Other Tools >

BGP Route Validity

All Valid Invalid Unknown Suppressed

Items per page 10

Search by AS or IP...

<input type="checkbox"/>	Origin AS	Prefix	Route Validity
<input type="checkbox"/>	AS2121	2001:67c:64::/48	Valid
<input type="checkbox"/>	AS2121	193.0.24.0/21	Valid

Suggest ROAs

Suppress Alerts

Re-enable Alerts

Showing 1 to 2 of 2 entries

Go to page: < 1 of 1 >

Alerts

You currently have 0 invalid and 0 unknown BGP announcements (0 are suppressed).

You are currently not subscribed to ROA alerts.

Configure

Certified Resources

193.0.24.0/21

2001:67c:64::/48

ROA Configuration

Items per page 10

Search by AS or IP...

AS number	Prefix	Maximum length
AS2121	2001:67c:64::/48	48
AS2121	193.0.24.0/21	21

Configure

Showing 1 to 2 of 2 entries

Go to page: < 1 of 1 >

RIPE NCC RPKI Validator

Download the RPKI Validator toolset to use RPKI data in your BGP decision making workflow. [Learn more...](#)





Demonstration: Creating a ROA

12



My LIR

Home >
LIR Contacts >
Communication Preferences >

Resource Certification

Dashboard >
ROA Configuration >
History >

Tools

LIR Locator >
Training >
E-Learning >
Glossary >
Events >
RIPE Atlas >
RIPEstat >
Other Tools >

BGP Route Validity

All Valid Invalid Unknown Suppressed

Items per page 10

Search by AS or IP...

<input type="checkbox"/>	Origin AS	Prefix	Route Validity
<input type="checkbox"/>	AS2121	2001:67c:64::/48	Valid
<input type="checkbox"/>	AS2121	193.0.24.0/21	Valid

Suggest ROAs

Suppress Alerts

Re-enable Alerts

Showing 1 to 2 of 2 entries

Go to page: < 1 of 1 >

Alerts

You currently have 0 invalid and 0 unknown BGP announcements (0 are suppressed).

You are currently not subscribed to ROA alerts.

Configure

Certified Resources

193.0.24.0/21

2001:67c:64::/48

ROA Configuration

Items per page 10

Search by AS or IP...

AS number	Prefix	Maximum length
AS2121	2001:67c:64::/48	48
AS2121	193.0.24.0/21	21

Configure

Showing 1 to 2 of 2 entries

Go to page: < 1 of 1 >

RIPE NCC RPKI Validator

Download the **RPKI Validator toolset** to use RPKI data in your BGP decision making workflow. [Learn more...](#)



My LIR

- Home >
- LIR Contacts >
- Communication Preferences >

Resource Certification

- Dashboard >
- ROA Configuration >
- History >

Tools

- LIR Locator >
- Training >
- E-Learning >
- Glossary >
- Events >
- RIPE Atlas >
- RIPEstat >
- Other Tools >

Change ROA Configuration

AS Number Prefix Maximum Length

All Changes Items per page Search by AS or IP...

AS number	Prefix	Maximum length	
AS2121	2001:67c:64::/48	48	
AS2121	193.0.24.0/21	21	

Showing 1 to 2 of 2 entries
Go to page: < of 1 >

BGP Route Validity

All Valid Invalid Unknown Suppressed Items per page Search by AS or IP...

<input type="checkbox"/>	Origin AS	Prefix	Route Validity
<input type="checkbox"/>	AS2121	2001:67c:64::/48	Valid
<input type="checkbox"/>	AS2121	193.0.24.0/21	Valid

Showing 1 to 2 of 2 entries
Go to page: < of 1 >

My LIR

- Home >
- LIR Contacts >
- Communication Preferences >

Resource Certification

- Dashboard >
- ROA Configuration >
- History >

Tools

- LIR Locator >
- Training >
- E-Learning >
- Glossary >
- Events >
- RIPE Atlas >
- RIPEstat >
- Other Tools >

Change ROA Configuration

AS Number Prefix Maximum Length

All Changes Items per page 10 Search by AS or IP...

AS number	Prefix	Maximum length	
AS2121	2001:67c:64::/48	48	
AS2121	193.0.24.0/21	21	
AS2121	193.0.24.0/24	24	

Showing 1 to 3 of 3 entries
Go to page: < 1 of 1 >

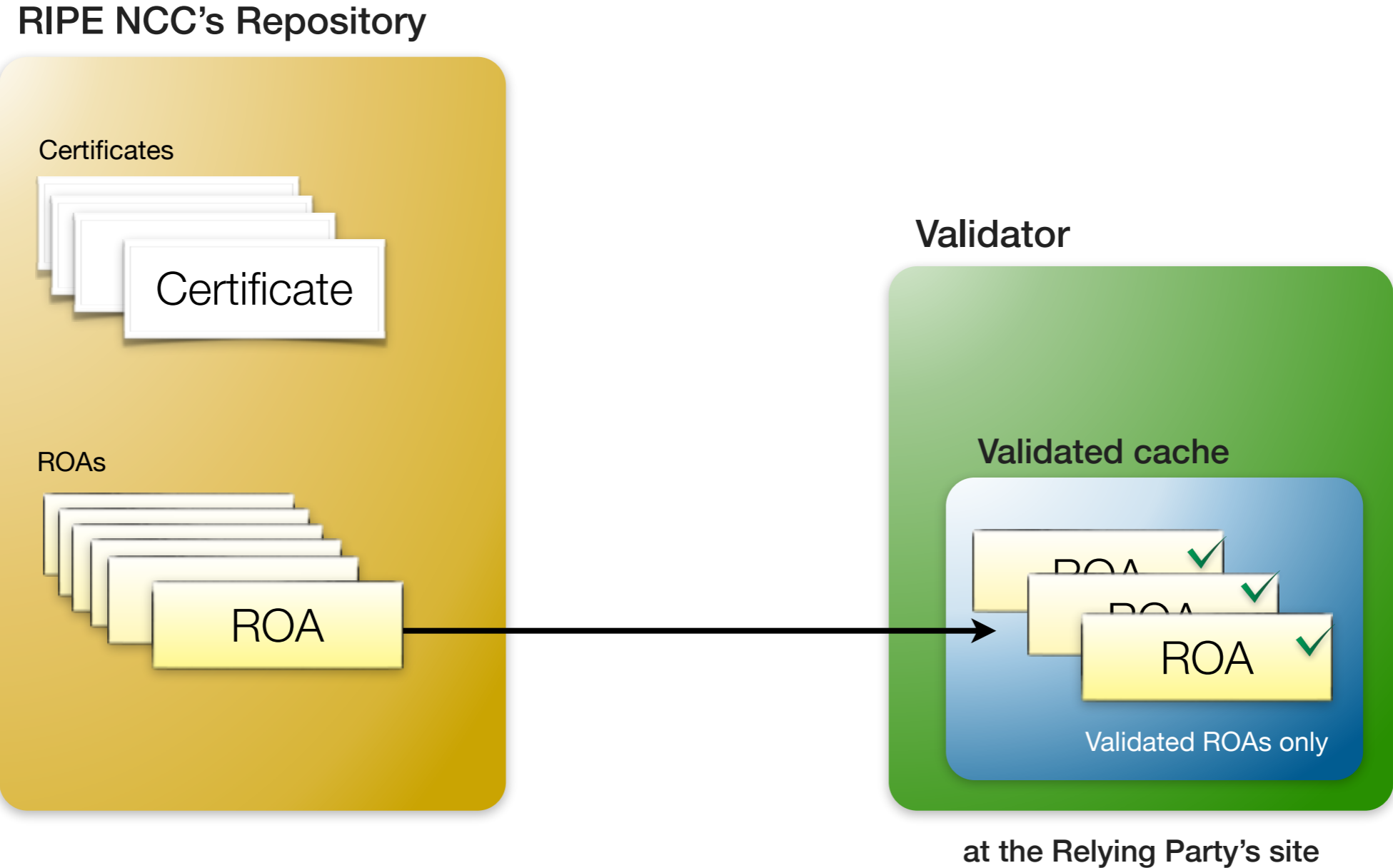
BGP Route Validity

All Valid Invalid Unknown Suppressed Items per page 10 Search by AS or IP...

<input type="checkbox"/>	Origin AS	Prefix	Route Validity
<input type="checkbox"/>	AS2121	2001:67c:64::/48	Valid
<input type="checkbox"/>	AS2121	193.0.24.0/21	Valid

Showing 1 to 2 of 2 entries
Go to page: < 1 of 1 >

- The validator of the client can access RIPE NCC's Repository with all the certificates, public keys, ROAs
- It downloads everything and then performs validation, checking whether the certificates and ROAs are valid
- Then it constructs a list of valid ROAs, which is its “validated cache”



- Invalid ROAs are simply not included in the list of valid ROAs when the validator of the client computes them
- Reasons for a ROA to be invalid
 - The signing certificate or key pair has expired or has been revoked
 - It does not validate back to a configured trust anchor
 - The LIR's resource has been returned to the RIPE NCC

- The RIPE NCC Validator allows you to manually override the validation process
- Adding an ignore filter will ignore all ROAs for a given prefix
 - The end result is the validation state will be “unknown”
- Creating a whitelist entry for a prefix and ASN will locally create a valid ROA
 - The end result is the validation state becomes “valid”

- **valid**
 - there is a ROA in the validated cache that matches the BGP announcement of the peer. Size matches too
- **unknown**
 - There is no ROA for that prefix in the cache
- **invalid**
 - There is a ROA for the prefix, but for a different AS
 - Or the size doesn't match

- Invalid ROA:
 - The ROA in the repository cannot be validated by the client (ISP) so it is not included in the validated cache
- Invalid BGP announcement:
 - There is a ROA in the validated cache for that prefix but for a different AS
 - Or the max. length doesn't match
- Remember: If no ROA in cache -> announcement unknown!

- The Relying Party's router can connect and download the cache from the validator
- Router can then compare any BGP announcements to the list of valid ROAs in the validated cache

- As an announcer/LIR:
 - You choose if you want certification
 - You choose if you want to create ROAs
 - You can choose max. length and AS
- As a Relying Party
 - You can choose if you use the validator
 - You can choose to make any routing decisions based on the results of the BGP Verification (valid/invalid/unknown)





Demonstration: Using the RIPE NCC Validator

13





Exercise: RPKI Quiz

14





Router Integration

15



- Router sessions
 - Validator listens on 8282 for RPKI-RTR Protocol
 - Routers can connect and download the cache
- Export function
 - Allows you to download a CSV with the cache
 - Can be integrated with your internal workflow
 - Use for statistics or spotting anomalies

- The RPKI-RTR Protocol is an IETF standard
- All router vendors can implement it
- Production Cisco support
 - ASR1000, 7600, ASR903, ASR901 in releases 15.2(1)S or X 3.5
- Cisco Early Field Trial (EFT)
 - ASR9000, CRS1, CRS3, c12K (IOS-XR)
- Juniper has support since version 12.2
- Quagga has support through BGP-ERX

- Cisco (hosted by the RIPE NCC):
 - Telnet to rpkirtr.ripe.net
 - User: ripe, no password
- Juniper (hosted by Kaia Global Networks)
 - Telnet to 193.34.50.25 or 193.34.50.26
 - User: rpki, password: testbed
- (<http://www.ripe.net/certification/tools-and-resources>)





IPv4 Transfers

16



- Only between RIPE NCC Members
- Allocation is allowed to be in use
- Minimum size is /22
- Must qualify for allocation
 - 80% usage criteria applies
- Evaluated by RIPE NCC

- PA between RIPE NCC members
- Due to merger or acquisition
- From legacy space

- IPv4 RIPE NCC Listing Service
 - Accessible from LIR Portal Account
- Brokers
 - Listed on RIPE NCC website
 - NOT endorsed by RIPE NCC
 - Signed an agreement to conform to RIPE policies



The End!

Край

Y Diwedd

النهاية

Соңы

ჟღერა

Fí

Finis

Ende

Finvezh

Liðugt

Кінець

Konec

Kraj

Ěnn

Fund

پایان

Lõpp

Beigas

Vége

Son

An Críoch

Kraj

הסוף

Fine

Endir

Sfârșit

Fin

Τέλος

Einde

Конец

Slut

Slutt

დასასრული

Pabaiga

Fim

Amaia

Loppu

Tmíem

Koniec

