Routing Security Training Course

Exercise Booklet

November 2015

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Introduction

Your database objects

For your convenience we have **already created some objects in the RIPE TEST Database**. You can use these objects during the practical exercises today. During the exercises, you can modify these or use them to update or create other objects.

We have created a **maintainer**, **person** and **organisation** object for you. There are also an IPv4 and IPv6 allocations and an AS assignment for your personal use.

To identify your objects, please look up your number in the attendees' list and substitute that in the placeholders. As an example, if your number on the list is **3**, your person object will be **TP3-TEST**. On the next pages you will find the list of all your objects that are in the TEST Database.

Passwords

All your objects are protected by your own **maintainer** object. In order to modify any of them, you will need the password for this maintainer.

This password is "secret" + your number, so the password for attendee **1** will be **secret1**, the password for attendee **2** will be **secret2,** and so on.

All pre-created objects

Fill in all ◯ placeholders with your number on the list

person:	**Training Course Participant ◯**
remarks:	RIPE NCC training courses - Participant ◯ Person
address:	Singel 258
address:	1016 AB Amsterdam
phone:	+312053544444
e-mail:	participant@example.com
nic-hdl:	TP◯-TEST
mnt-by:	CM◯-MNT
changed:	participant@example.com
source:	TEST

mntner:	**CM◯-MNT**
descr:	RIPE NCC training courses - Participant ◯ Maintainer
admin-c:	TP◯-TEST
mnt-by:	CM◯-MNT
referral-by:	CM◯-MNT
auth:	MD5-PW # Filtered
changed:	participant@example.com
upd-to:	participant@example.com
notify:	participant@example.com
source:	TEST

organisation:	**ORG-TCP-TEST**
org-name:	RIPE NCC training courses - Participant Organisation
org-type:	LIR
address:	Singel 258, 1016 AB Amsterdam
phone:	+31205354444
fax-no:	+31205354444
e-mail:	participant@example.com
admin-c:	TP-TEST
tech-c:	TP-TEST
ref-nfy:	auto@example.com
notify:	notify@example.com
mnt-ref:	TEST-NCC-HM-MNT"
mnt-by:	TEST-NCC-HM-MNT"
changed:	trainer@example.com
source:	TEST

The following Internet resources are available for you to be used in the exercises:

inetnum:	**192..0.0 - 192..3.255**
netname:	NL-RIPENCC-TCP-20140626
org:	ORG-TCP-TEST
descr:	RIPE NCC training courses - Participant Allocation
country:	EU
admin-c:	TP-TEST
tech-c:	TP-TEST
status:	ALLOCATED PA
mnt-by:	TEST-NCC-HM-MNT
mnt-lower:	CM-MNT
mnt-routes:	CM-MNT
changed:	hostmaster@example.com
source:	TEST

For **inet6num** and **aut-num** fill in ⬭ placeholders with your number on the list using two digits (i.e. 01, 02 , 03…25).

inet6num:	**2001:ff⬭::/32**
netname:	NL-RIPENCC-TCP⬭-20140625
org:	ORG-TCP⬭-TEST
descr:	RIPE NCC training courses - Participant ⬭ Allocation
country:	EU
admin-c:	TP⬭-TEST
tech-c:	TP⬭-TEST
status:	ALLOCATED-BY-RIR
mnt-by:	TEST-NCC-HM-MNT
mnt-lower:	CM⬭-MNT
mnt-routes:	CM⬭-MNT
changed:	hostmaster@example.com
source:	TEST

aut-num:	**AS1⬭**
as-name:	RIPE NCC training courses - Participant ⬭ ASN
org:	ORG-TCP⬭-TEST
admin-c:	TP⬭-TEST
tech-c:	TP⬭-TEST
mnt-by:	TEST-DBM-MNT
mnt-by:	CM⬭-MNT
changed:	hostmaster@ripe.net
source:	TEST

Test database

In the exercises, we will make use of the RIPE TEST Database. This is a public system that acts and responds in exactly the same way as the RIPE Database would do.

You can access the TEST Database by selecting the correct source in the Webupdates or whois tools:

Exercise 1

route and route6 object creation

Task: Create a **route** and **route6** object

Preparations:

- Using your number on the attendee list, identify your **IPv4 and IPv6 allocations**
- Find out your AS Number using the same method
- Find out the name and password of your **maintainer** object

Instructions:

- Go to the Webupdates tool
- Select “create object” and choose **route**
- Add your **IPv4 allocation** prefix to your **route** object
- Add your AS Number as the **origin** AS for your prefix
- Add the correct password and submit the update

- Go back to the Webupdates tool
- Select “create object” and choose **route6**
- Add your **IPv6 allocation** prefix to your **route6** object
- Add your AS Number as the **origin** AS for your prefix
- Add the correct password and submit the update

Alternative additional task:

- Take your **IPv6 allocation**
- Create second **route6** object for it
- Add your **neighbour’s** AS as the **origin**
- Which password(s) do you need to create this object?
- What is the alternative approach?
- Add a **mnt-routes** attribute to solve the issue

Exercise 2

Retrieving information from the Routing Registry

Task: Lookup AS 3333 and find out which prefixes they announce

For this task we are going to use the production RIPE Database. AS 3333, which is the RIPE NCC, is registered in there. Use the whois interface to retrieve the object and answer the following questions.

If AS 3333 was your customer and you needed to build a filter, which prefixes would you accept from them?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

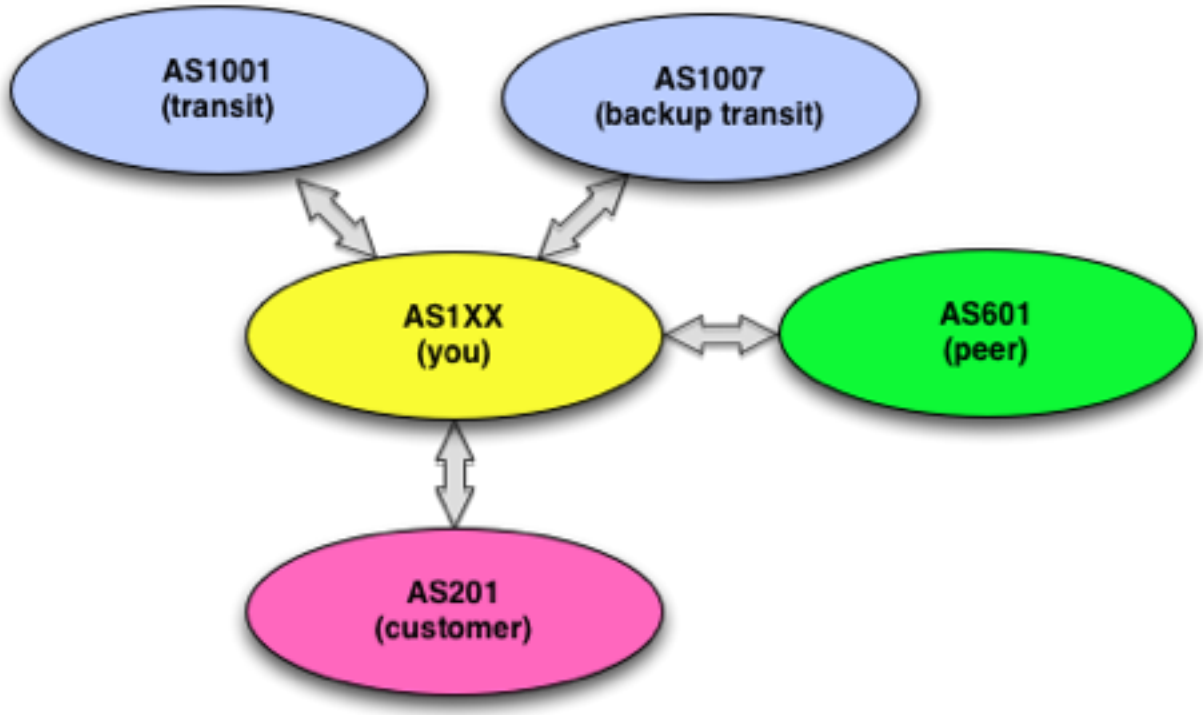
If you have time to spare, browse to http://stat.ripe.net and look them up.

Looking at RIPEstat, do the announcements from AS 3333 match the entries in the routing registry?

_____

Exercise 3

Routing policy in your aut-num



Task: Update your aut-num object to show your routing policy

Your AS is the middle one in the diagram above. You have two upstreams, (one preferred, one backup), one customer and one peer AS. Update your **aut-num** object and add **import, export, mp-import and mp-export** attributes to describe the peering with these networks.

Instructions:

- Select “modify or delete an object” and search for your AS number
- Click on a + sign to add a new attribute field
- Select first import, then export, mp-import, mp-export
- Continue adding fields until you covered all connections
  - There should be 4 import and 4 export attributes for IPv4 Policy
  - There should be 4 mp-import and 4 mp-export attributes for IPv6 Policy
- Submit the update, remembering to supply the correct password
- Did you consider adding remark lines to describe your policy?

Exercise 4

Using a tool

Task: Use the Level3 tool online to look up AS 3333

Level 3 has a tool online that queries the routing registry. This system is based on the whois protocol and uses the same syntax.

To access the tool, do a whois lookup from your computer and use the following syntax:

“whois -h filtergen.level3.net RIPE::AS3333”

This should return a list of prefixes. Do they match the results from the previous exercise?

The command uses the following syntax:

- -h filtergen.level3.net tells your whois client which server to use
- RIPE:: tells the whois server you want to query the RIPE Routing Registry
- AS 3333 finally tells which AS you want information about
-

Additional task:

- Try looking up RIPE::AS-RIPENCC
- Does it work?
- Do you get the same list of prefixes. If not, what is the difference?

Exercise 5

RPKI Quiz

In case multiple answers are possible, please circle all correct ones.

1. If a ROA is invalid, and there are no other valid ROAs for that range in the cache,what will be the result of the BGP verification for that prefix?

   A. valid
   B. invalid
   C. unknown
   D. not enough info to answer the question

2. If the ROA size =/22 MaxLength=empty
   What size prefixes can be announced?

   A. /22
   B. /22 and more specific
   C. not /22, but more specific
   D. anything less specific than /22

3. Referring to Question2, What will the BGP verification status be of all other prefixes?

   A. valid
   B. invalid
   C. unknown
   D. not enough info to answer the question

4. If the ROA size =/21 MaxLength=22
   How many different prefixes can be announced?

   A. 0
   B. 1
   C. 2
   D. 3

5. Can you have several prefixes in a ROA?

   A. yes
   B. no

6. Can you create a separate ROA for each of your prefixes?

   A. yes
   B. no

7. Can you have overlapping ROAs of the same size?

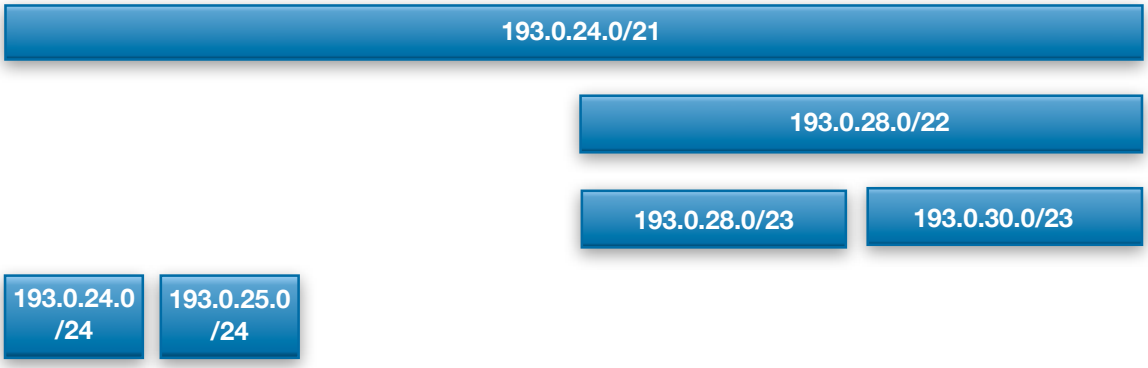
   A. yes

B. no

8. Can you have overlapping ROAs of the same size, with the same origin AS?

A. yes
B. no

9. You want to enable the following announcement from your AS333 (see diagram).
Which ROAs do you have to create? Fill out as many rows as needed in the table below.



ROA range	AS	max length
	AS333	
	AS333	
	AS333	
	AS333	
	AS333	
	AS333	

10.You have created the following ROAs. See table below.
Encircle in the diagram below all the BGP route announcements, that will have the verification value = **"valid"** as a result.

ROA range	AS	max length
193.0.0.0/21	AS333	/22
193.0.2.0/23	AS333	/24
193.0.4.0/23	AS333	empty
193.0.5.0/24	AS333	empty
193.0.6.0/24	AS333	empty