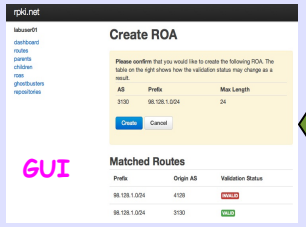
RPKI-Based Origin Validation Lab

Creative Commons: Attribution-NonCommercial-ShareAlike

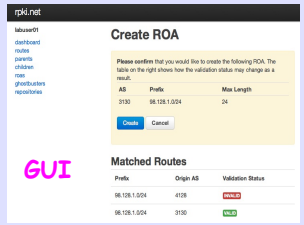
Issuing Parties

Relying Parties



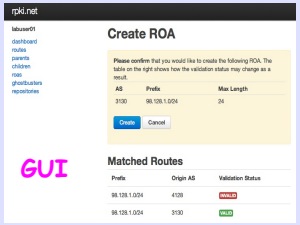
altCA

Up
Down



JPNIC

Up
Down



IIJ

Publication Protocol

Publication Protocol

Publication Protocol

Trust Anchor

Resource PKI

Resource PKI

Resource PKI

SIA Pointers

SIA Pointers

RCynic Gatherer

Validated Cache

Pseudo IRR

```
route:    147.28.0.0/16
descr:    147.28.0.0/16-16
origin:   AS3130
notify:   irr-hack@rpki.net
mnt-by:   MAINT-RPKI
changed:  irr-hack@rpki.net 20110606
source:   RPKI
```

NOC Tools

BGP Decision Process

Our Focus Today

Creative Commons: Attribution-NonCommercial-ShareAlike

Today

- Register Our Prefixes in CA
- Issue ROAs Using CA's Web Portal
- Configure Routers to get ROAs from Caches

Creative Commons: Attribution-NonCommercial-ShareAlike

Get Copy of This Preso

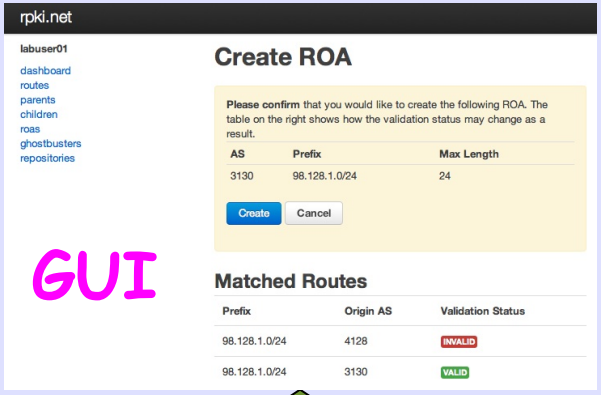
https://github.com/randyqx/apricot-sec2019

So You Can

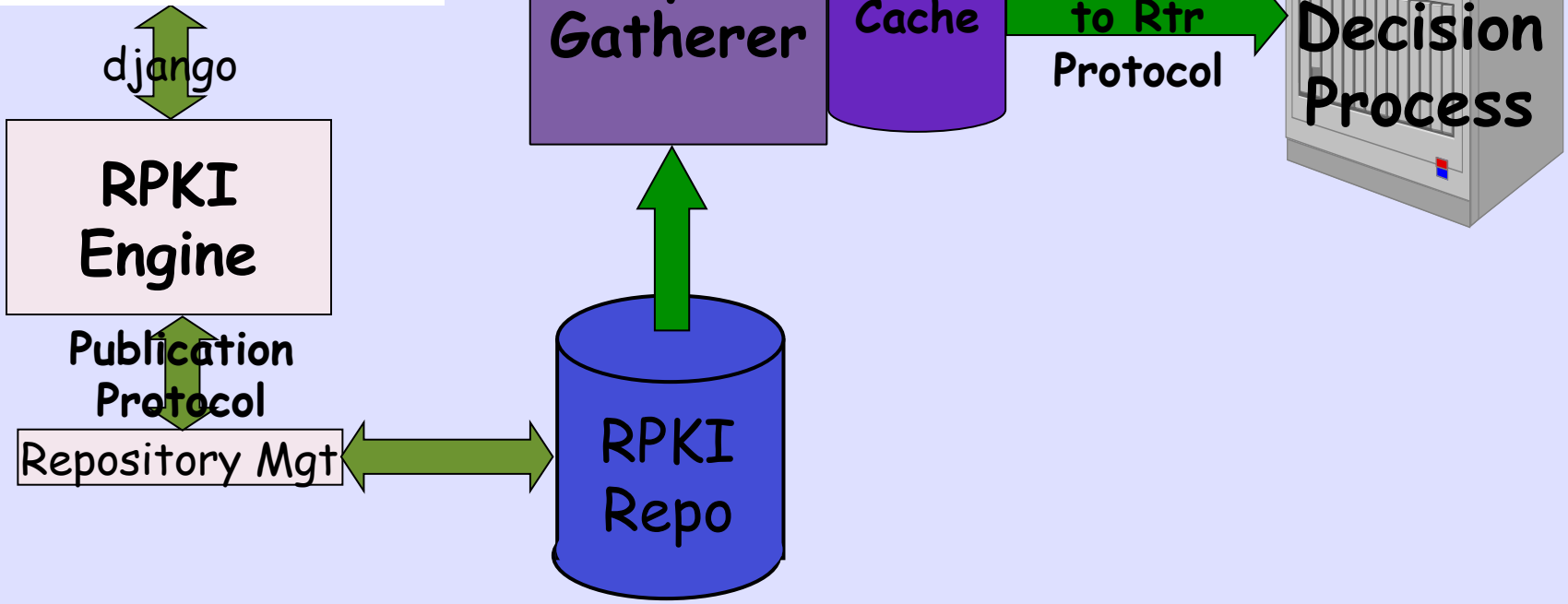
Copy and Paste

Creative Commons: Attribution-NonCommercial-ShareAlike

Lab Overview



GUI



Creative Commons: Attribution-NonCommercial-ShareAlike

Lab Environment

ubu01

ubu02

ubu03

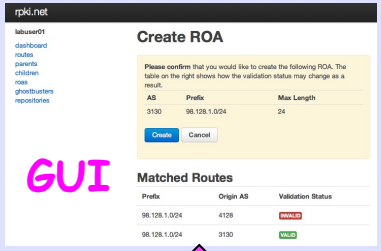
ubu04

ubu05

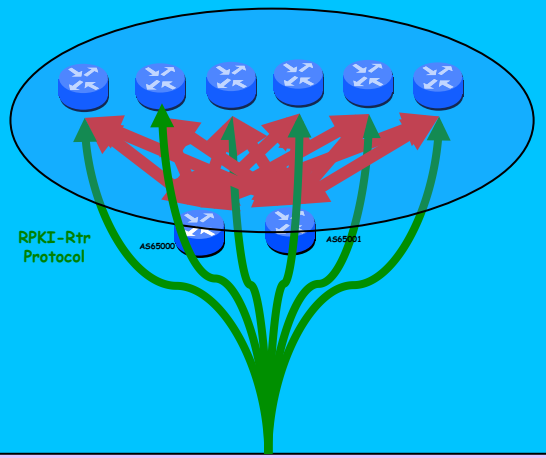
⋮

ubu16

Ubuntu/KVM Server in Ashburn



GUI

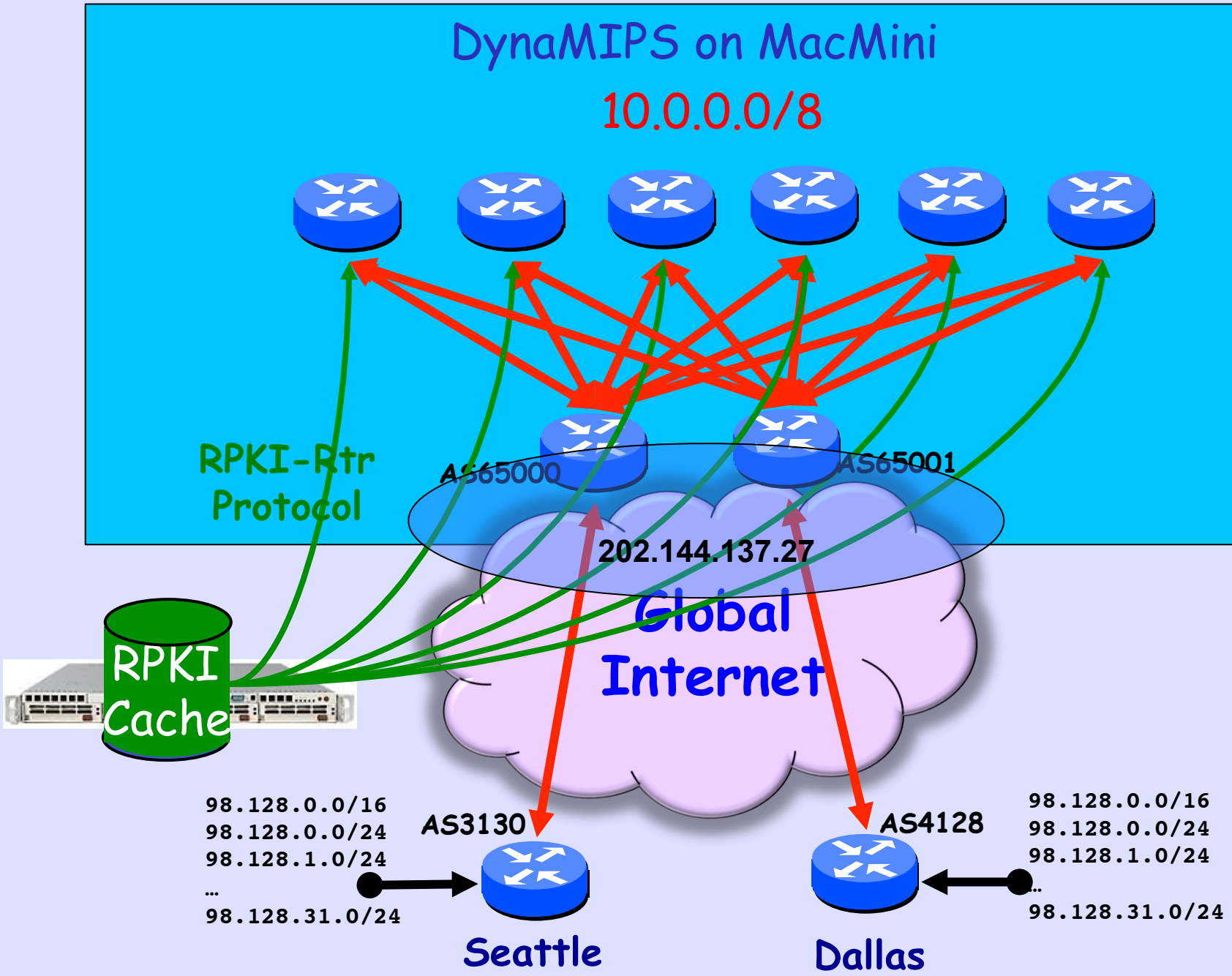


RP - cache0.vmini

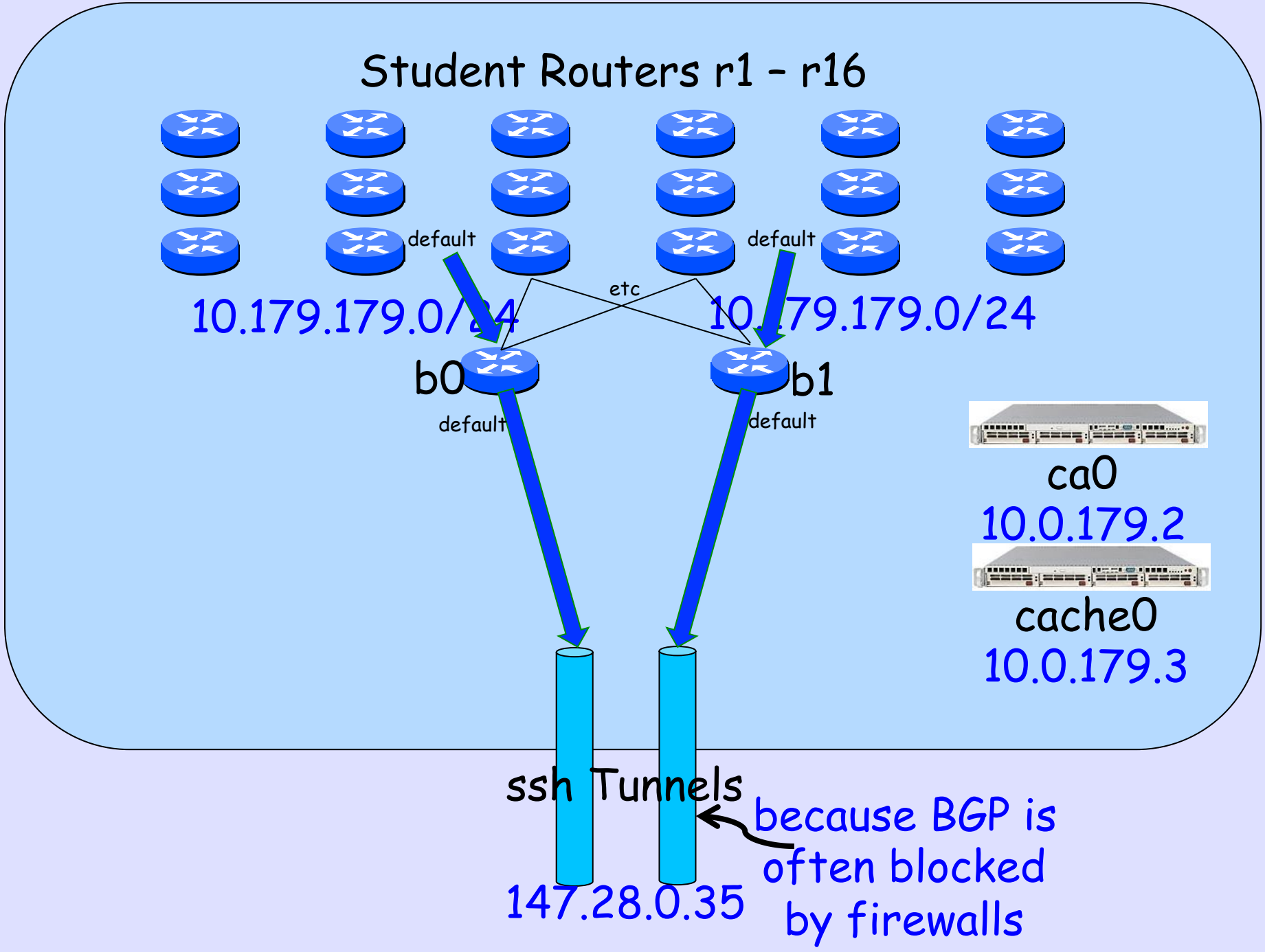
CA - ca0.vmini

Mac Mini running Ubuntu KVM

Creative Commons: Attribution-NonCommercial-ShareAlike

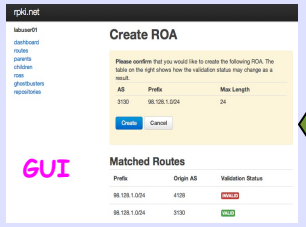


Creative Commons: Attribution-NonCommercial-ShareAlike


Student Routers r1 – r16
default
default
etc
10.179.179.0/24
10.179.179.0/24
b0
b1
default
default
ca0
10.0.179.2
cache0
10.0.179.3
ssh Tunnels
147.28.0.35
because BGP is often blocked by firewalls

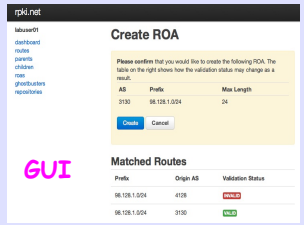
Issuing Parties

Relying Parties



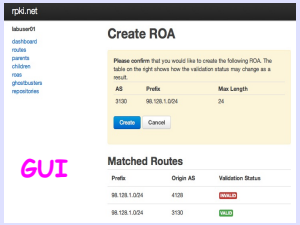
altCA

Up
Down



JPNIC

Up
Down



IIJ

Publication Protocol

Publication Protocol

Publication Protocol

Trust Anchor

Resource PKI

Resource PKI

Resource PKI

SIA Pointers

SIA Pointers

RCynic Gatherer

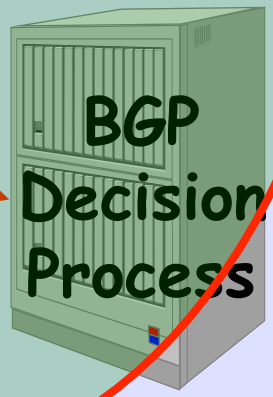
Validated Cache

Pseudo IRR

```
route:    147.28.0.0/16
descr:    147.28.0.0/16-16
origin:   AS3130
notify:   irr-hack@rpki.net
mnt-by:   MAINT-RPKI
changed:  irr-hack@rpki.net 20110606
source:   RPKI
```

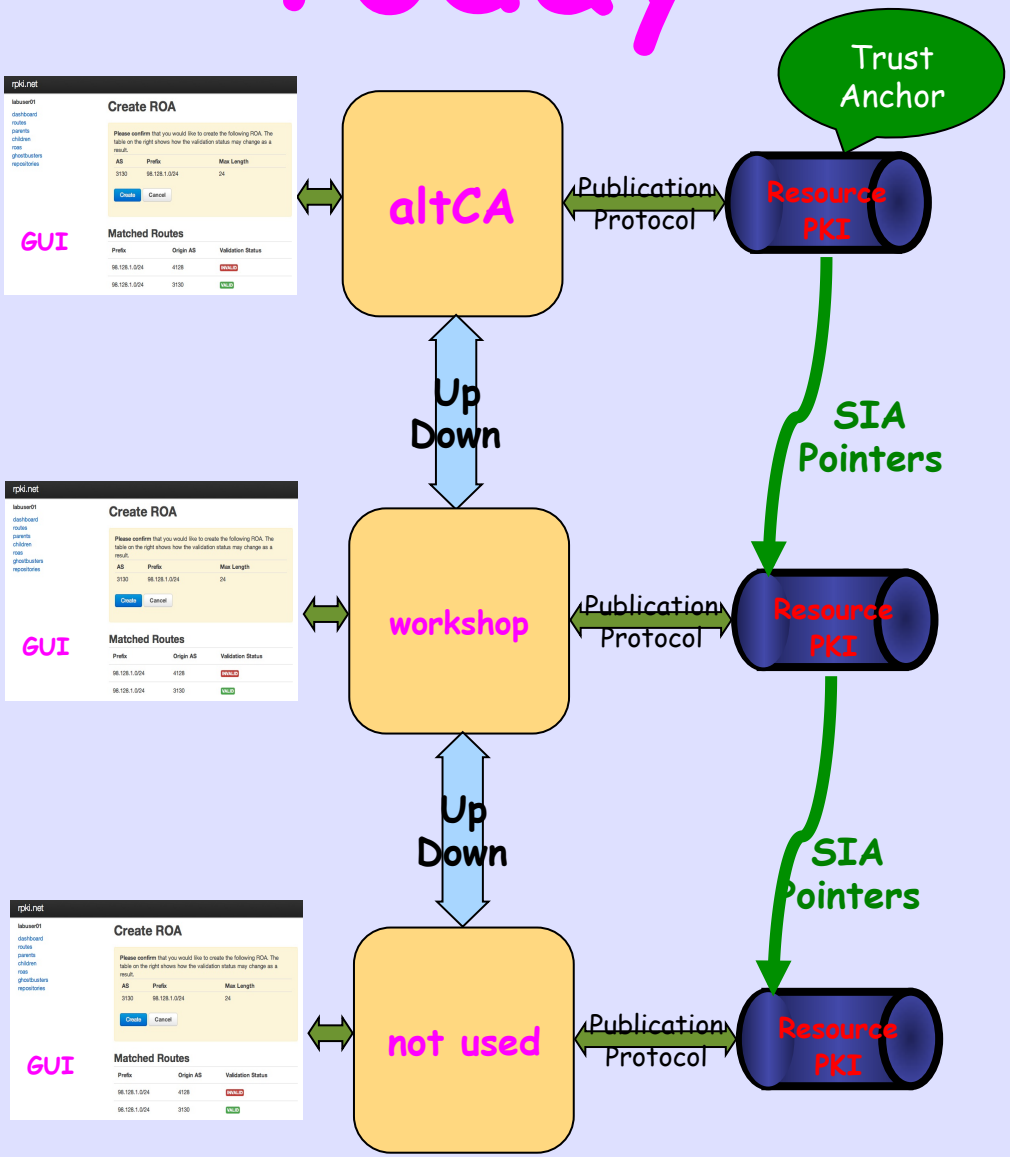
NOC Tools

Our Focus Today



Creative Commons: Attribution-NonCommercial-ShareAlike

Today



Creative Commons: Attribution-NonCommercial-ShareAlike

IP Address Allocation

98.128.0.0/16 ARIN Experimental Allocation

98.128.0.0/24	Instructors Play
98.128.1.0/24	labuser01
98.128.2.0/24	labuser02
…	
98.128.32.0/24	labuser32

Creative Commons: Attribution-NonCommercial-ShareAlike

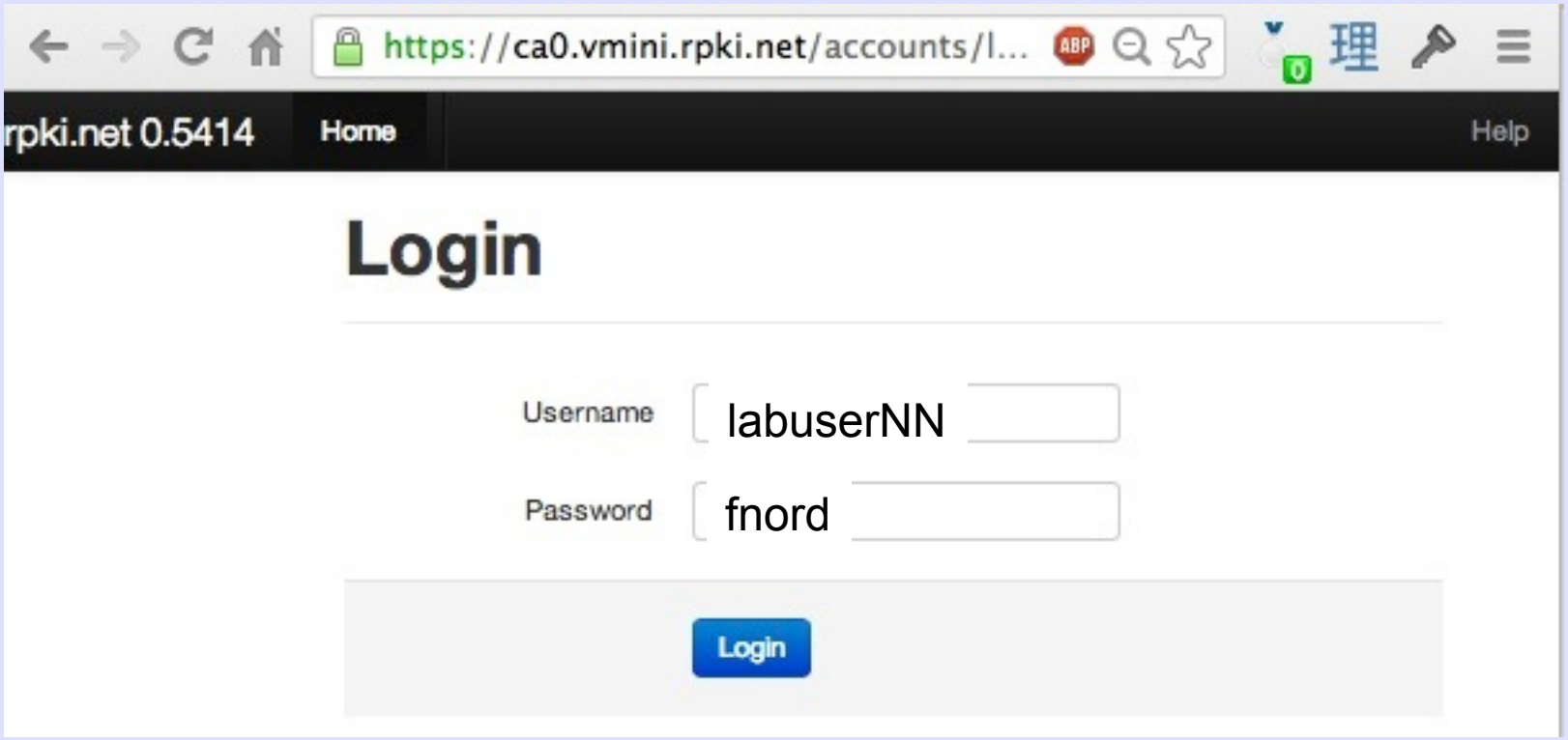
GUI Accounts

https://rpki-ca.workshop/

UserID	Password
labuser01	fnord
labuser02	fnord
labuser03	fnord
…	
labuser16	fnord

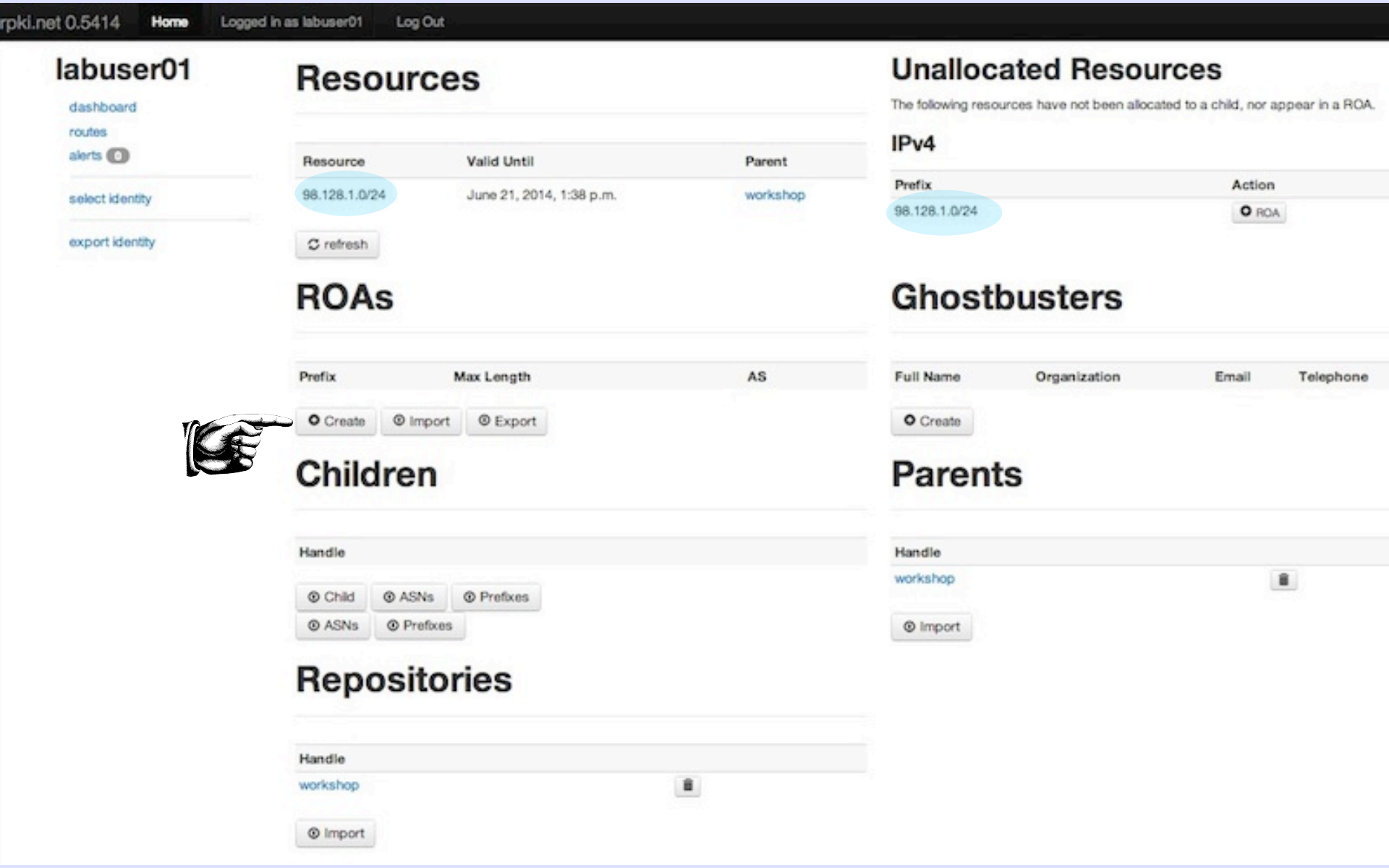
Creative Commons: Attribution-NonCommercial-ShareAlike

https://ca0.vmini.rpki.net/



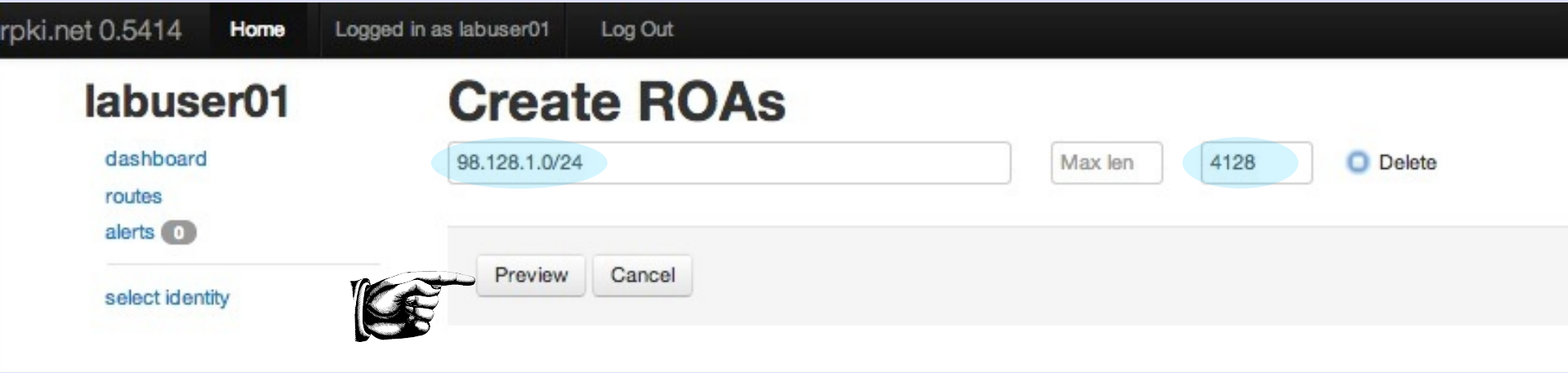
Creative Commons: Attribution-NonCommercial-ShareAlike

The Dashboard



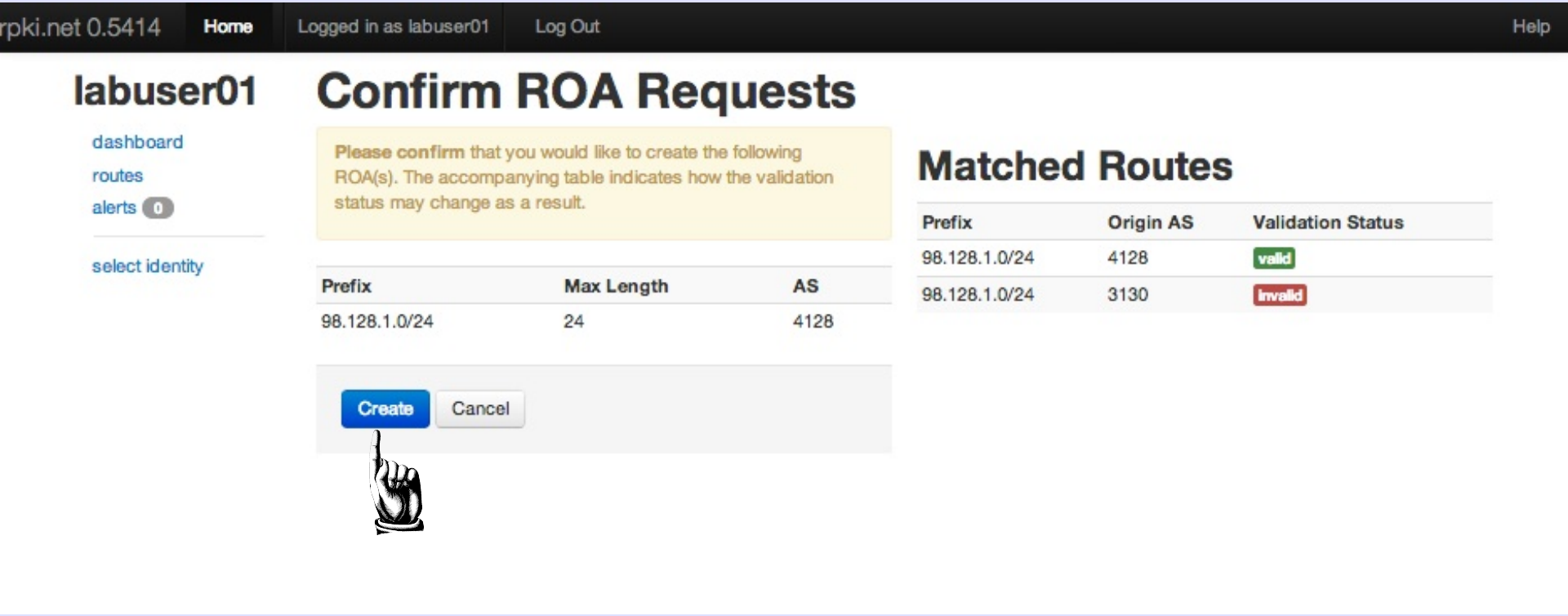
Creative Commons: Attribution-NonCommercial-ShareAlike

Create a ROA



Creative Commons: Attribution-NonCommercial-ShareAlike

What Will Happen?



Creative Commons: Attribution-NonCommercial-ShareAlike

Routers

- Use Your Own! (in production images from C&J)
- 16 DynaMIPS 7200s in Lab

Creative Commons: Attribution-NonCommercial-ShareAlike

Be Careful !

- Some Caches Have a LOT of ROAs
- Do Not Configure DynaMIPS to a Server With RIR TALs Because RIPE Data Has Thousands of ROAs
- dfw0, 198.180.152.11 Has Full BGP Table if you want to crash DynaMIPS

Creative Commons: Attribution-NonCommercial-ShareAlike

In-Lab Router Accounts

ssh isplab@10.179.179.**N** (**N** is your user number)

isplab@10.179.179.**N**'s password: *lab-PW*

enable

password: *lab-PW*

Creative Commons: Attribution-NonCommercial-ShareAlike

Basic bgp configuration

router bgp 651xx

distance bgp 200 200 200

neighbor 10.179.179.253 remote-as 65000

neighbor 10.179.179.254 remote-as 65001

network 98.128.N.0 255.255.255.0

no bgp default ipv4-unicast

Creative Commons: Attribution-NonCommercial-ShareAlike

Basic bgp configuration(2)

- This configuration does not work.
  - show ip bgp neighbor 10.179.179.253 advert
- How do we fix?

Creative Commons: Attribution-NonCommercial-ShareAlike

RPKI BGP Configuration

```
rN#conf t

Enter configuration commands, one per line.  End with
   CNTL/Z.

rN(config)#router bgp 651NN

rN(config-router)#bgp rpki server tcp 10.0.179.3 port
   43779 refresh 60

rN(config-router)#end
```

That's All

Creative Commons: Attribution-NonCommercial-ShareAlike

Cisco Adventure

```
rN#show ip bgp rpki ?
  servers  Display RPKI cache server information
  table    Display RPKI table entries
```


Creative Commons: Attribution-NonCommercial-ShareAlike

Check Server

```
rN#show ip bgp rpki servers
BGP SOVC neighbor is 10.0.0.3/43779 connected to port 43779
Flags 0, Refresh time is 600, Serial number is 1304239609
InQ has 0 messages, OutQ has 0 messages, formatted msg 345
Session IO flags 3, Session flags 4008
 Neighbor Statistics:
  Nets Processed 624

Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Mininum incoming TTL 0, Outgoing TTL 255
Local host: 199.238.113.10, Local port: 57932
Foreign host: 10.0.0.3, Foreign port: 43779
Connection tableid (VRF): 0
```


Creative Commons: Attribution-NonCommercial-ShareAlike

Look at Table

```
rN#show ip bgp rpki table | i ^98
76 BGP sovc network entries using 6688 bytes of memory
78 BGP sovc record entries using 1560 bytes of memory
Network                Maxlen  Origin-AS  Source  Neighbor
98.128.0.0/24          24      3130       0       10.0.0.3/43779
98.128.0.0/16          16      3130       0       10.0.0.3/43779
98.128.6.0/24          24      4128       0       10.0.0.3/43779
98.128.9.0/24          24      3130       0       10.0.0.3/43779
98.128.30.0/24         24      1234       0       10.0.0.3/43779
128.224.1.0/24         24      3130       0       10.0.0.3/43779
129.6.0.0/17           17      49         0       10.0.0.3/43779
129.6.112.0/24         24      10866      0       10.0.0.3/43779
129.6.128.0/17         17      49         0       10.0.0.3/43779
147.28.0.0/16          16      3130       0       10.0.0.3/43779
```


Creative Commons: Attribution-NonCommercial-ShareAlike

Look at BGP Table

```
rN#sh ip bgp
     Network          Next Hop            Metric LocPrf Weight Path
* i I198.180.150.0    144.232.9.61   100  0 1239 3927 i
*>  I                 199.238.113.9       0 2914 3927 i
*   I                 129.250.11.41       0 2914 3927 i
*>  V198.180.152.0    199.238.113.9       0 2914 4128 i
*   V                 129.250.11.41       0 2914 4128 i
*>  N198.180.155.0    199.238.113.9       0 2914 22773 i
*   N                 129.250.11.41       0 2914 22773 i
*>  N198.180.160.0    199.238.113.9       0 2914 23308 13408 5752 i
*   N                 129.250.11.41       0 2914 23308 13408 5752 i
```

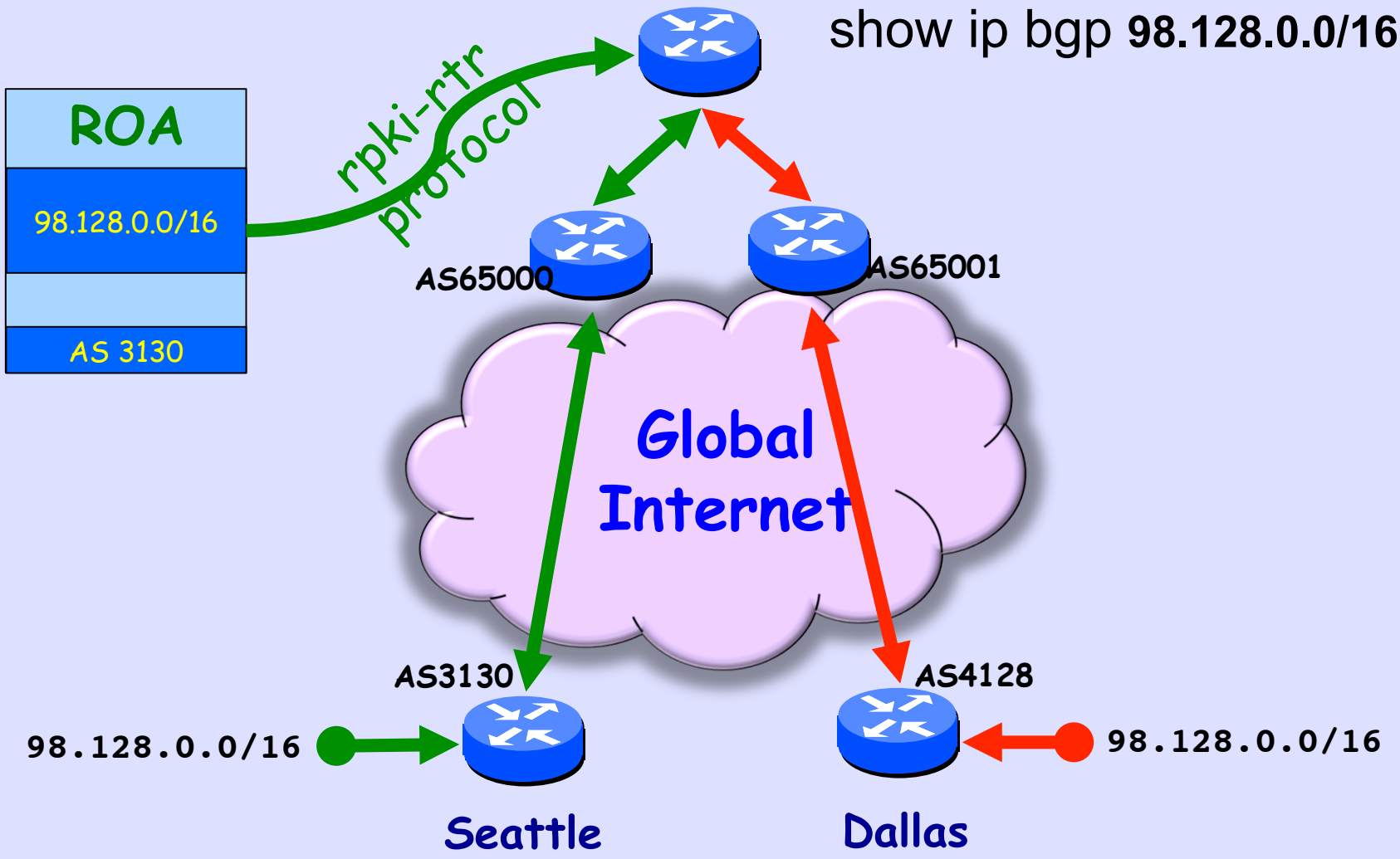

Creative Commons: Attribution-NonCommercial-ShareAlike

Mis-Origination Caught

```
RN#sh ip bgp 98.128.NN.0/24
BGP routing table entry for 98.128.0.0/24, version 94
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  65000 3130
    10.0.0.1 from 10.0.0.1 (65.38.193.12)
      Origin IGP, localpref 100, valid, external
      path 6802D4DC RPKI State invalid
  Refresh Epoch 1
  65001 4128
    10.0.1.1 from 10.0.1.1 (65.38.193.13)
      Origin IGP, localpref 100, valid, external, best
      path 6802D7C8 RPKI State valid
```

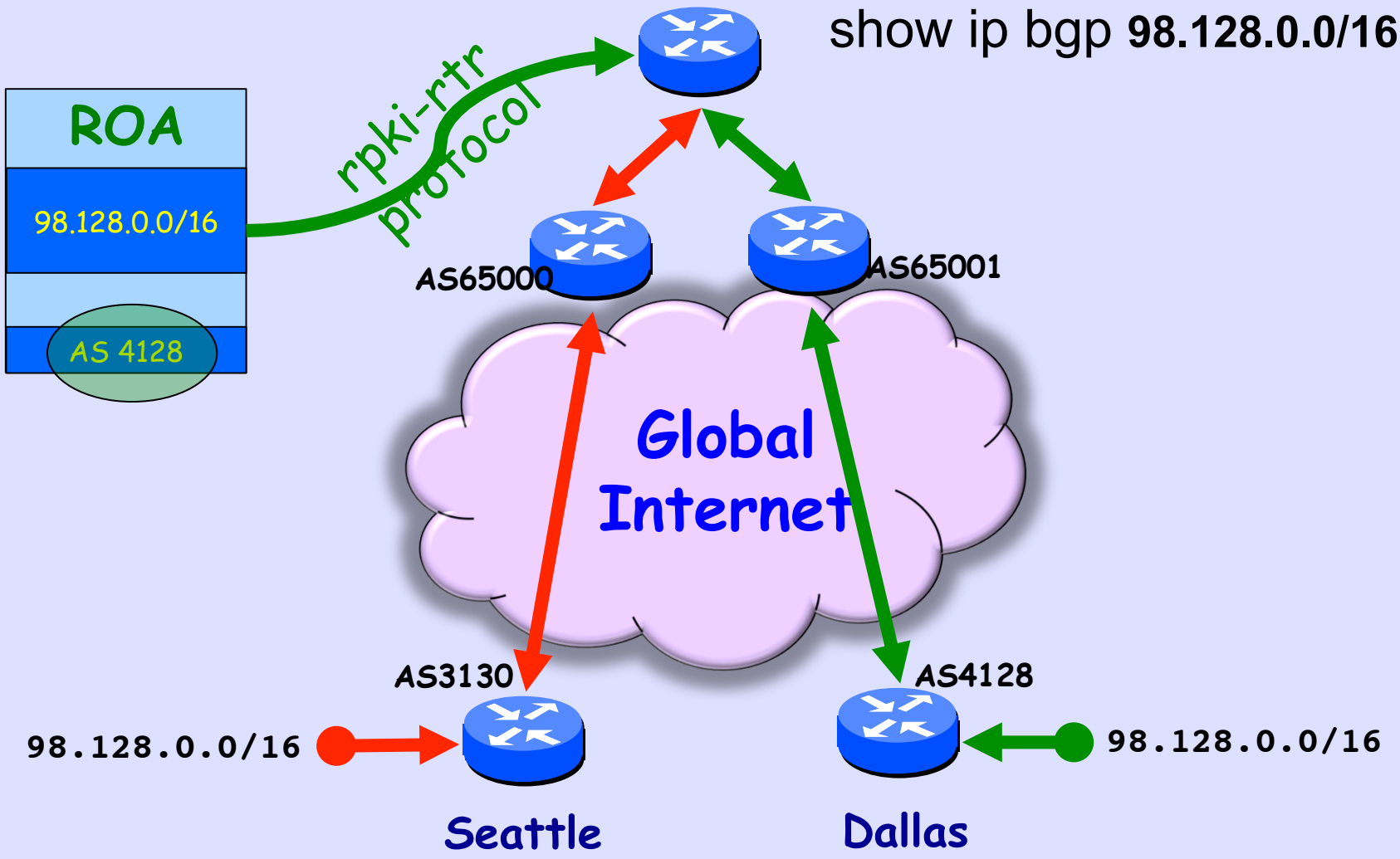

Creative Commons: Attribution-NonCommercial-ShareAlike

Fat-Finger Detected



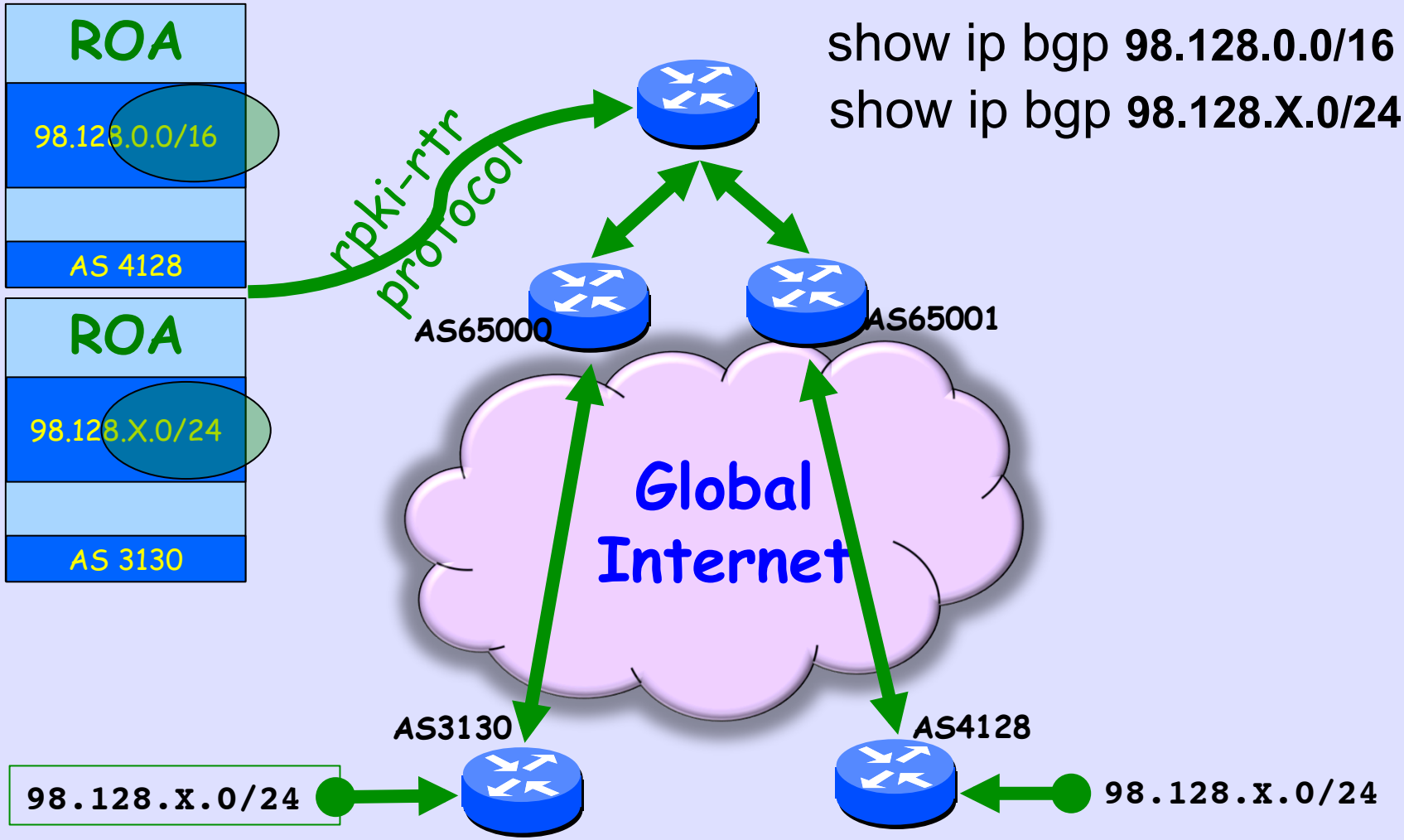
Creative Commons: Attribution-NonCommercial-ShareAlike

ROA Controls Validity



Creative Commons: Attribution-NonCommercial-ShareAlike

Try Your Own /24



show ip bgp **98.128.0.0/16**
show ip bgp **98.128.X.0/24**

Creative Commons: Attribution-NonCommercial-ShareAlike

Fun Things to Do

- Look at your neighbors' prefixes
- Use the GUI to change the ROA for your prefix, and wait for it to propagate
- Attack your neighbor's prefix by configuring your bgp to announce it

```
router bgp 651nn
 network 98.128.<neighbor>.0 mask 255 255 255.0
 ip route 98.128.<neighbor>.0 255.255.255.0
null0
```


Creative Commons: Attribution-NonCommercial-ShareAlike

Notice it Did Not Work

```
router bgp 651nn
  network 98.128.<neighbor>.0 mask 255 255 255.0
ip route 98.128.<neighbor>.0 255.255.255.0 null0

show ip bgp 98.128.<neighbor>.0
```

- **It is marked Invalid on your own router! It caught you injecting a bad prefix. To cheat you need to**

```
router bgp 651nn
  no bgp bestpath prefix-validate local
```

- **Now ask others to look for your announcement. They should see it as Invalid**

Creative Commons: Attribution-NonCommercial-ShareAlike

Now You Know How to Prevent YouTube Incident-2 And Stay Out of The Newspapers

Creative Commons: Attribution-NonCommercial-ShareAlike

Please Do Try This At Home

Creative Commons: Attribution-NonCommercial-ShareAlike