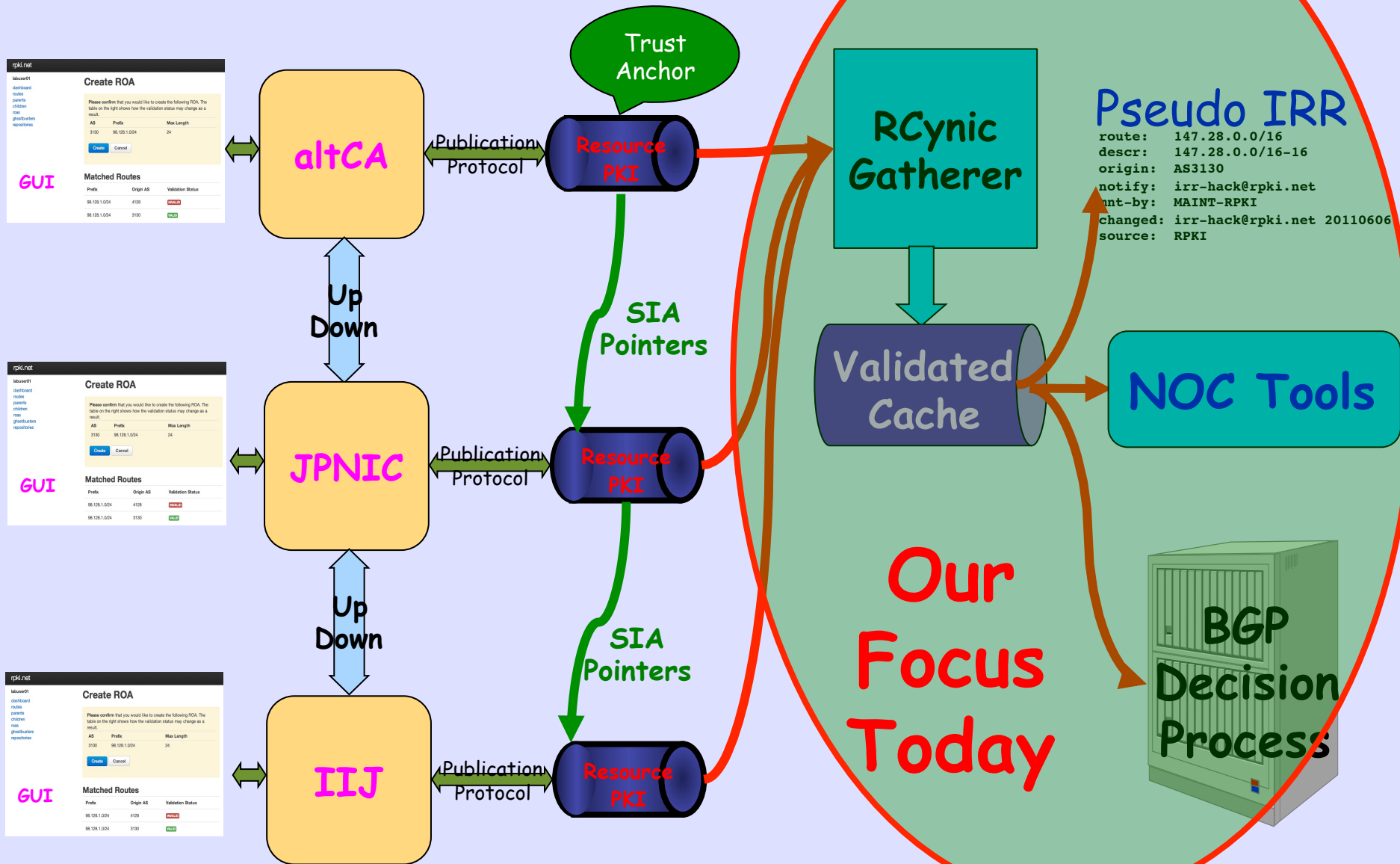


RPKI-Based Origin Validation Lab

Issuing Parties

Relying Parties



Our
Focus
Today

BGP
Decision
Process

Today

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

Get Copy of This Preso

<https://psg.com/1.pdf>

So You Can Copy and Paste

Lab Overview

rpki.net

labuser01
dashboard
routes
parents
children
roas
ghostbusters
repositories

Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

AS	Prefix	Max Length
3130	98.128.1.0/24	24

Create Cancel

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID

GUI

django

RPKI
Engine

Publication
Protocol

Repository Mgt

RCynic
Gatherer

Cache

RPKI
to Rtr
Protocol

BGP
Decision
Process

RPKI
Repo

Lab Environment

ubu01

ubu02

ubu03

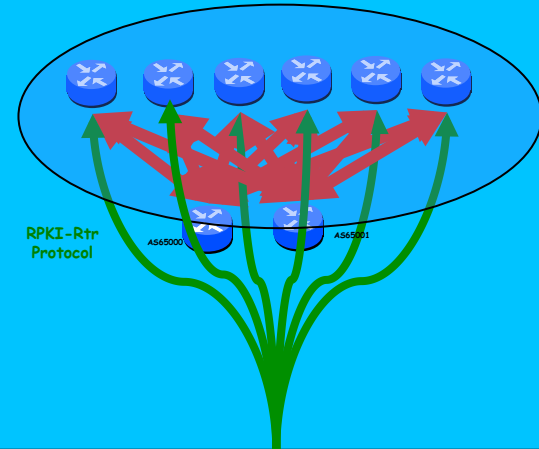
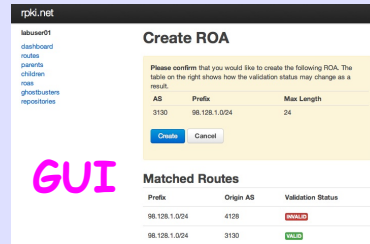
ubu04

ubu05

⋮

ubu16

**Ubuntu/KVM
Server in
Ashburn**



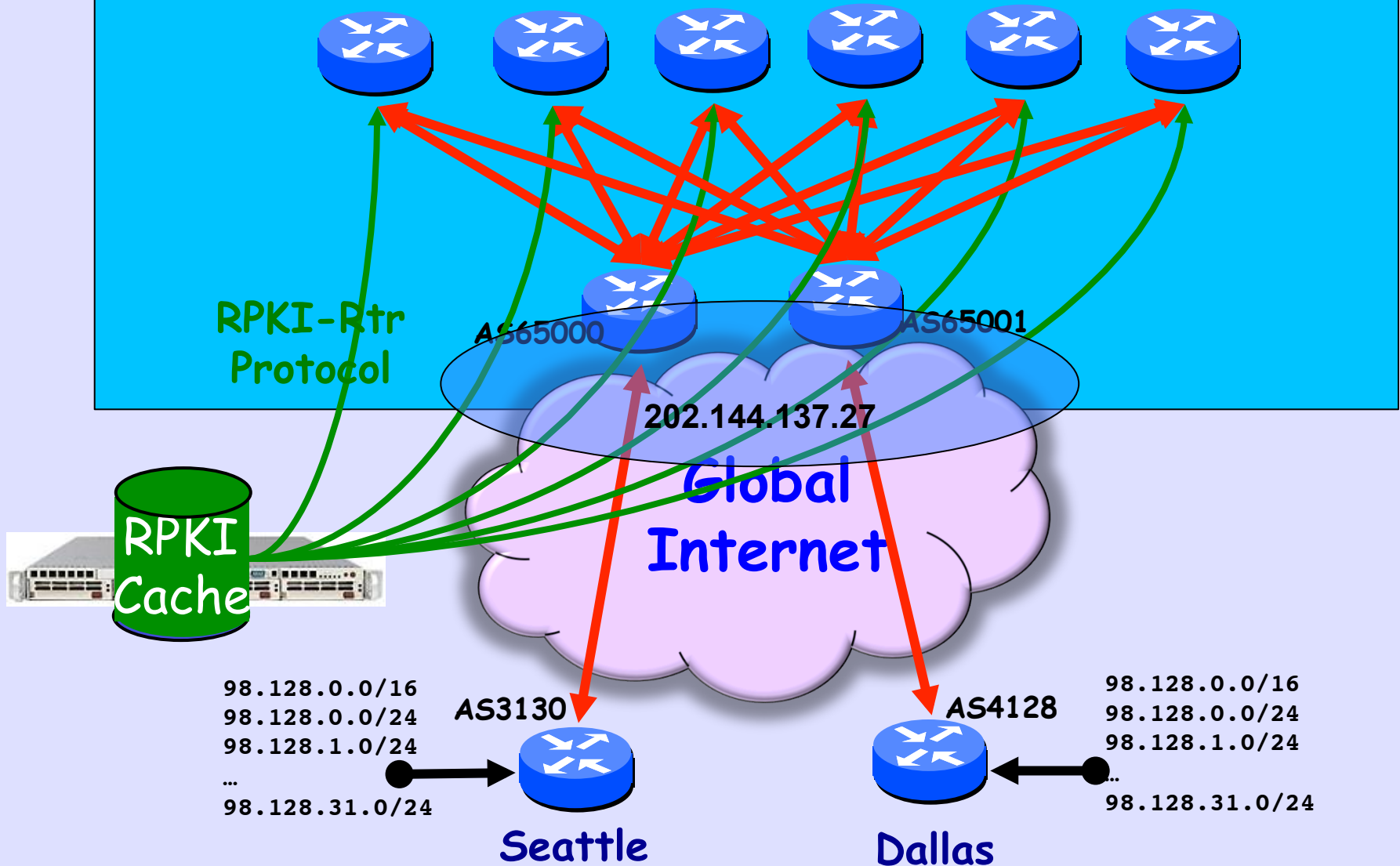
RP - cache0.vmini

CA - ca0.vmini

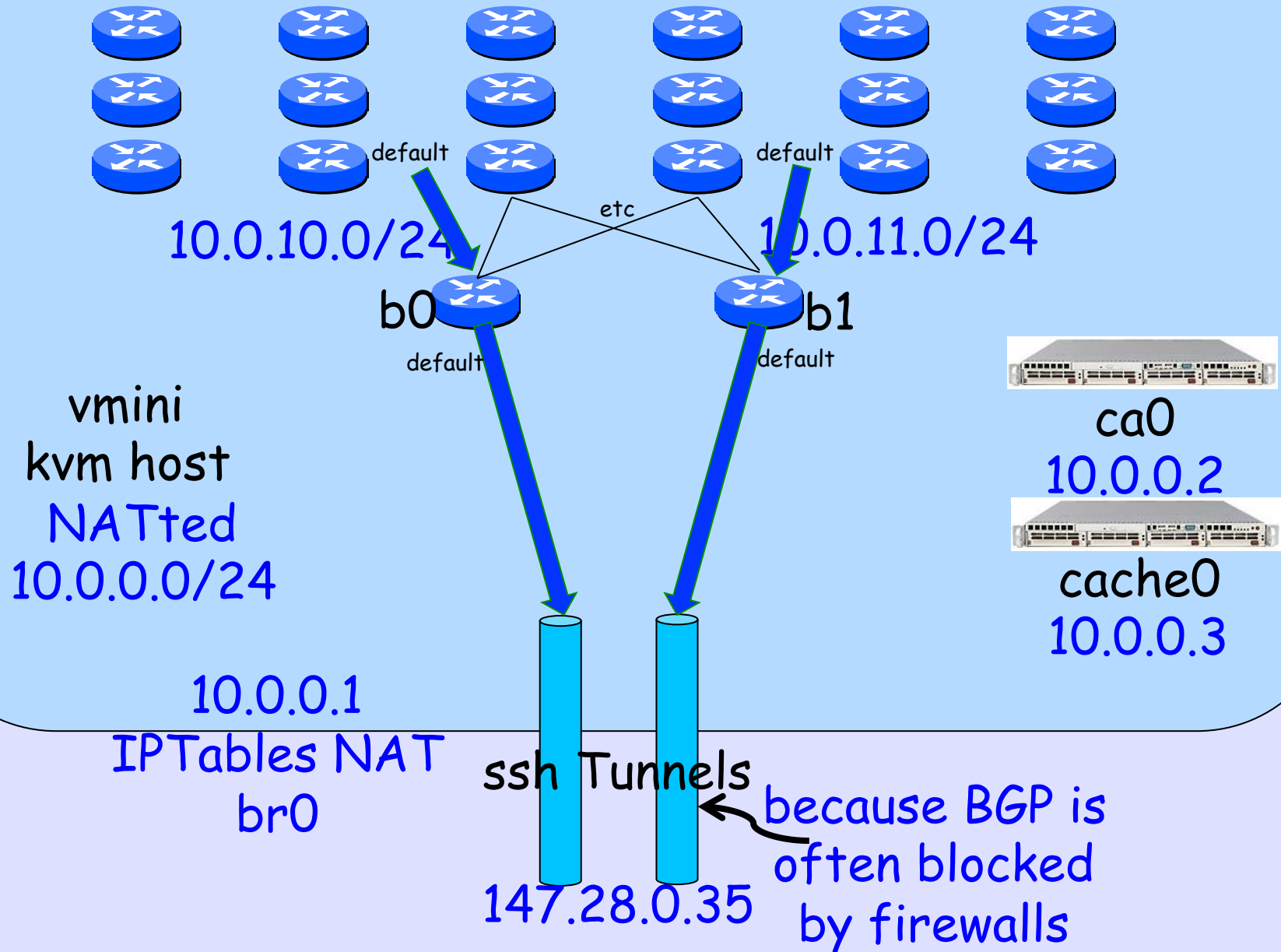
**Mac Mini running
Ubuntu KVM**

DynaMIPS on MacMini

10.0.0.0/8

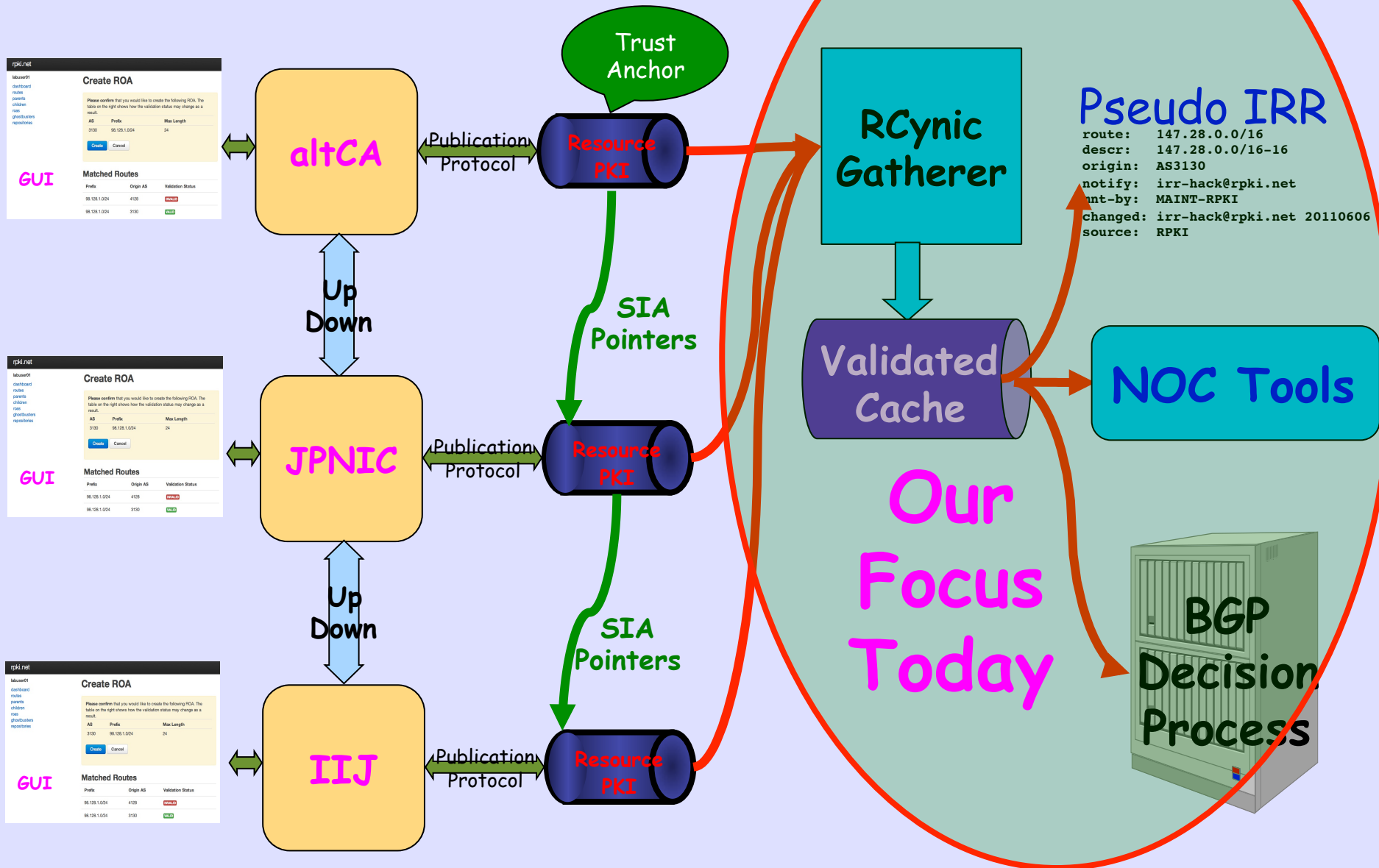


Student Routers r1 - r16

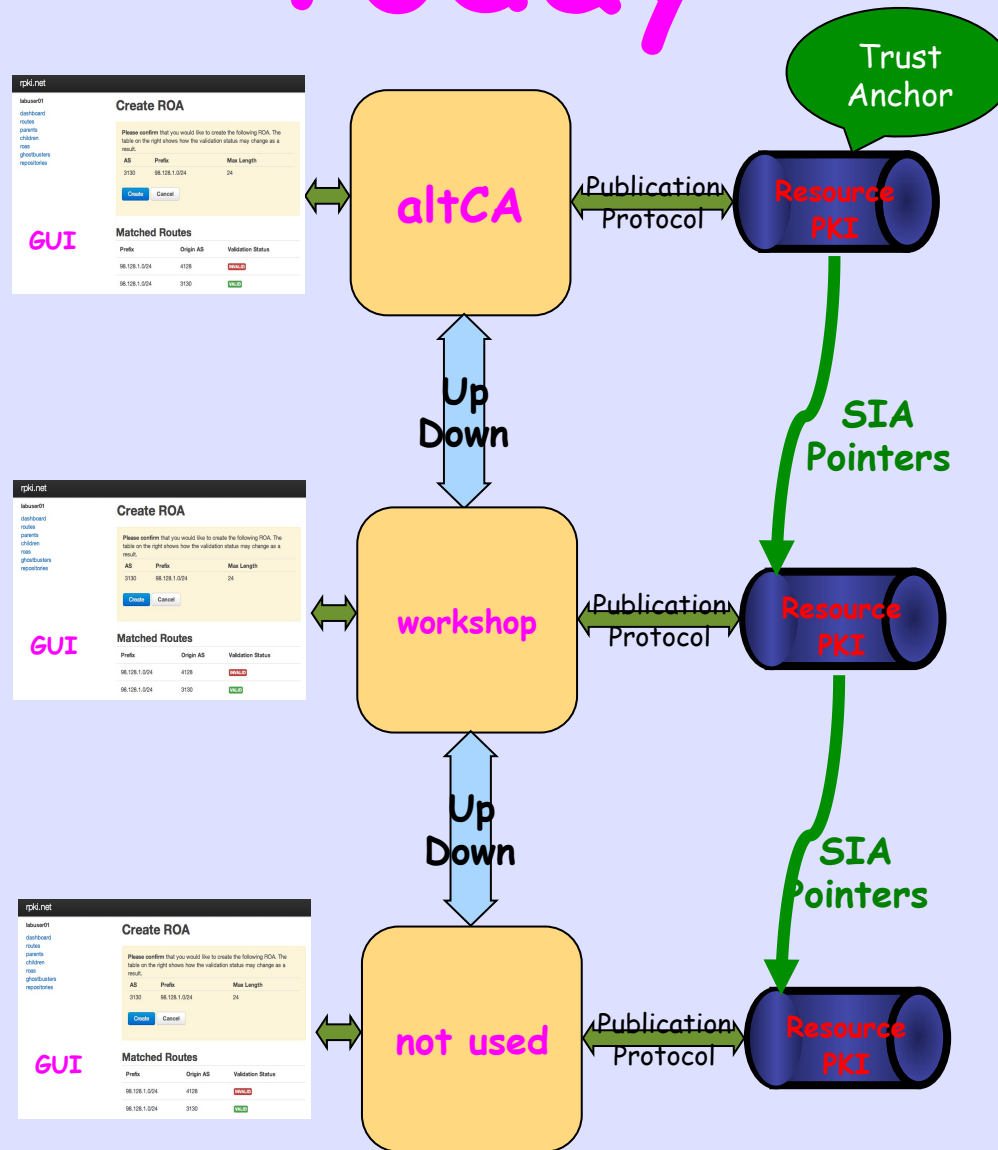


Issuing Parties

Relying Parties



Today



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

GUI Accounts

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

<u>UserID</u>	<u>Password</u>
labuser01	fnord
labuser02	fnord
labuser03	fnord
...	
labuser16	fnord

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

rpki.net 0.5414 Home Help

Login

Username

Password

Login

The Dashboard

rpki.net 0.5414

Home

Logged in as labuser01

Log Out

labuser01

[dashboard](#)
[routes](#)
[alerts](#) 0
[select identity](#)
[export identity](#)

Resources

Resource	Valid Until	Parent
98.128.1.0/24	June 21, 2014, 1:38 p.m.	workshop

refresh

ROAs

Prefix	Max Length	AS
--------	------------	----

Create Import Export

Children

Handle

Child ASNs Prefixes
ASNs Prefixes

Repositories

Handle

workshop

Import

Unallocated Resources

The following resources have not been allocated to a child, nor appear in a ROA.

IPv4

Prefix	Action
98.128.1.0/24	ROA

Ghostbusters

Full Name	Organization	Email	Telephone
-----------	--------------	-------	-----------

Create

Parents

Handle

workshop

Import



Create a ROA

rpki.net 0.5414

Home

Logged in as labuser01

Log Out

labuser01

[dashboard](#)

[routes](#)

[alerts](#) 0

[select identity](#)

Create ROAs

98.128.1.0/24

Max len

4128

☐ Delete

Preview

Cancel



What Will Happen?

rpki.net 0.5414

Home

Logged in as labuser01

Log Out

Help

labuser01

[dashboard](#)
[routes](#)
[alerts](#) 0
[select identity](#)

Confirm ROA Requests

Please confirm that you would like to create the following ROA(s). The accompanying table indicates how the validation status may change as a result.

Prefix	Max Length	AS
98.128.1.0/24	24	4128

Create

Cancel



Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	valid
98.128.1.0/24	3130	invalid

Routers

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

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

In-Lab Router Accounts

ssh rN@vmini.rpki.net (N is your user number)

rN@vmini's password: *fnord*

user: *isplab*

password: *lab-PW*

enable

password: *lab-PW*

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 10.0.0.3 port \  
43779 refresh 60
```

```
rN(config-router)#end
```

That's All

Cisco Adventure

rN#show ip bgp rpki ?

servers Display RPKI cache server information

table Display RPKI table entries

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
```

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

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

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
```

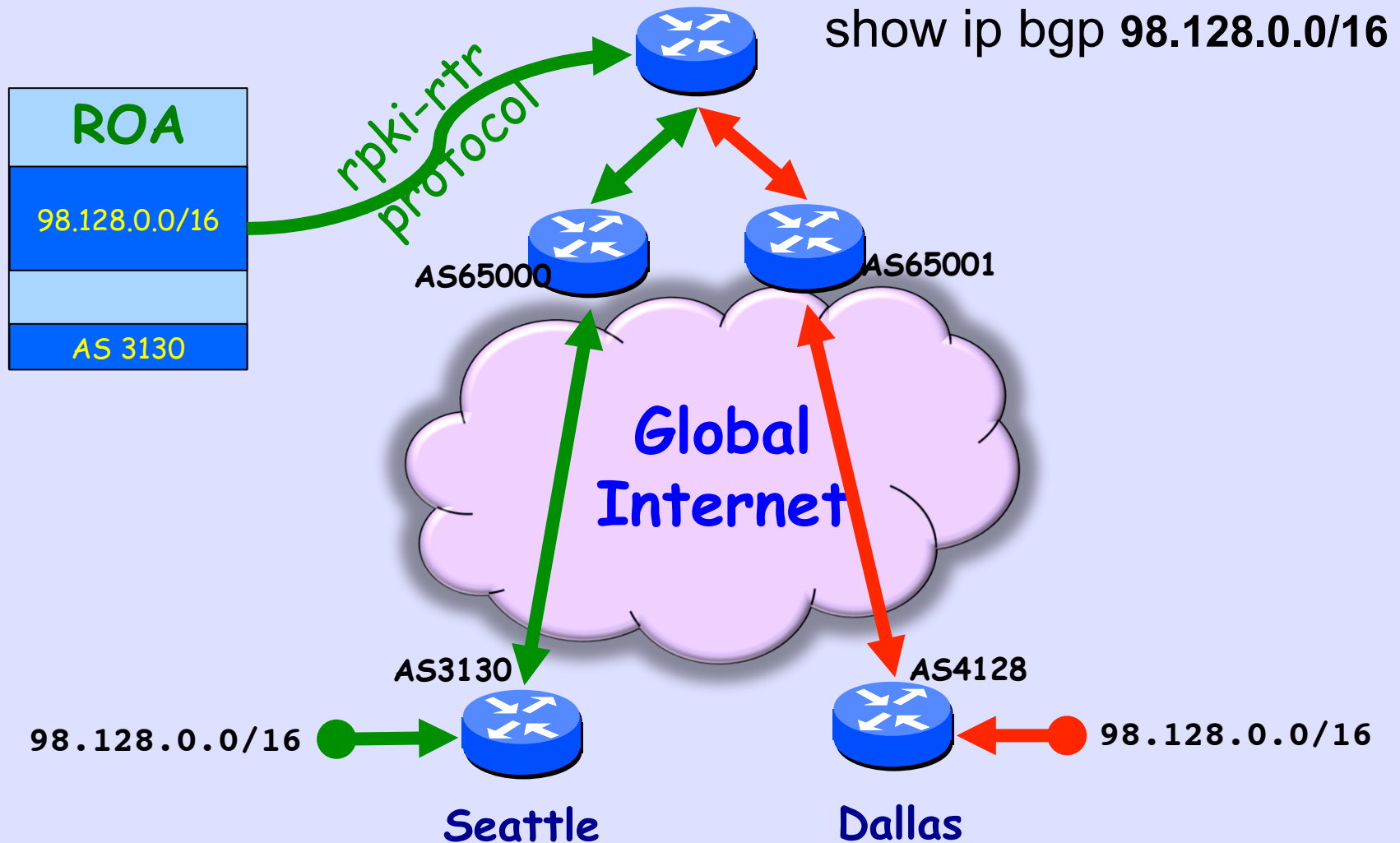
```
65001 4128
```

```
  10.0.1.1 from 10.0.1.1 (65.38.193.13)
```

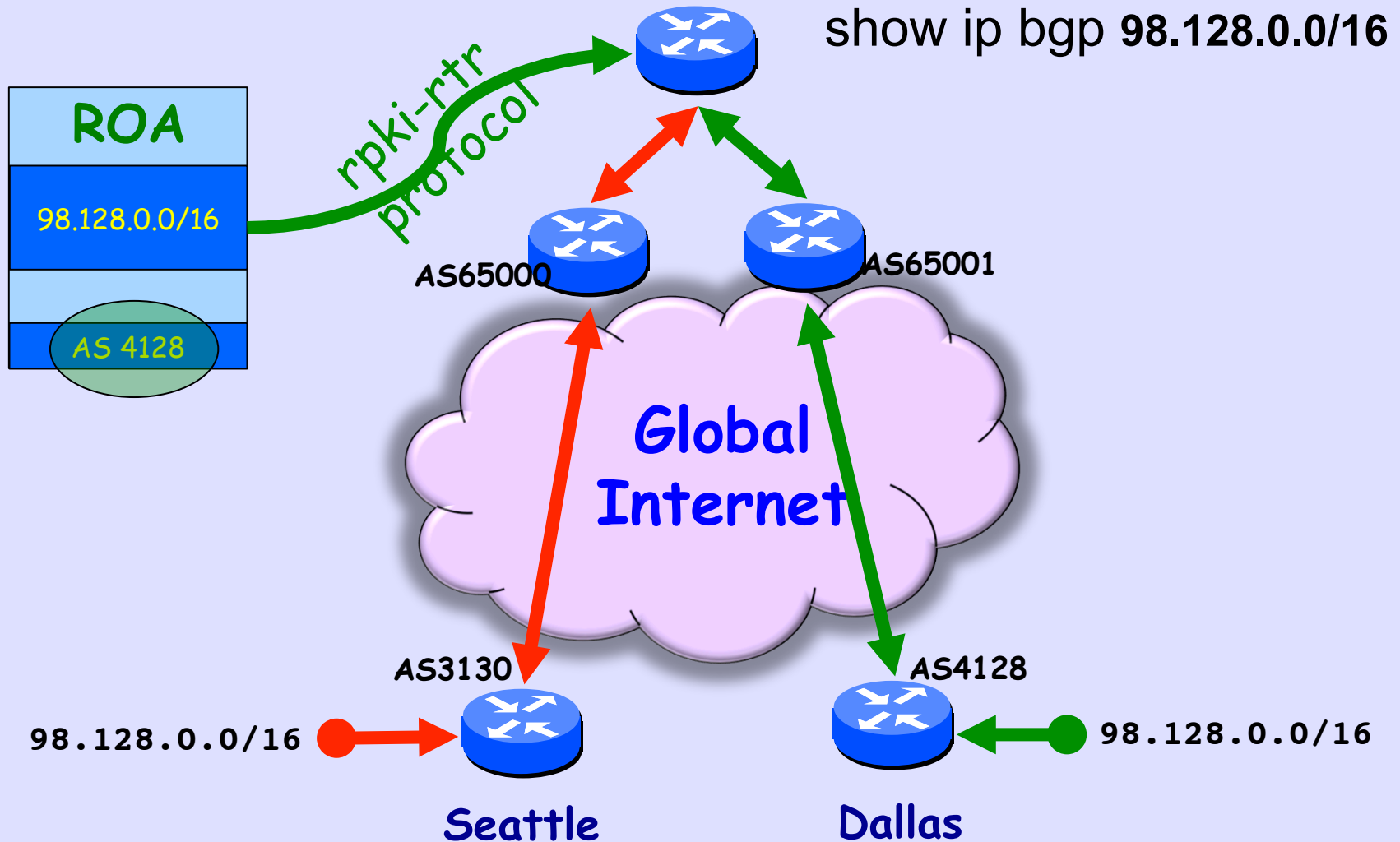
```
    Origin IGP, localpref 100, valid, external, best
```

```
    path 6802D7C8 RPKI State valid
```

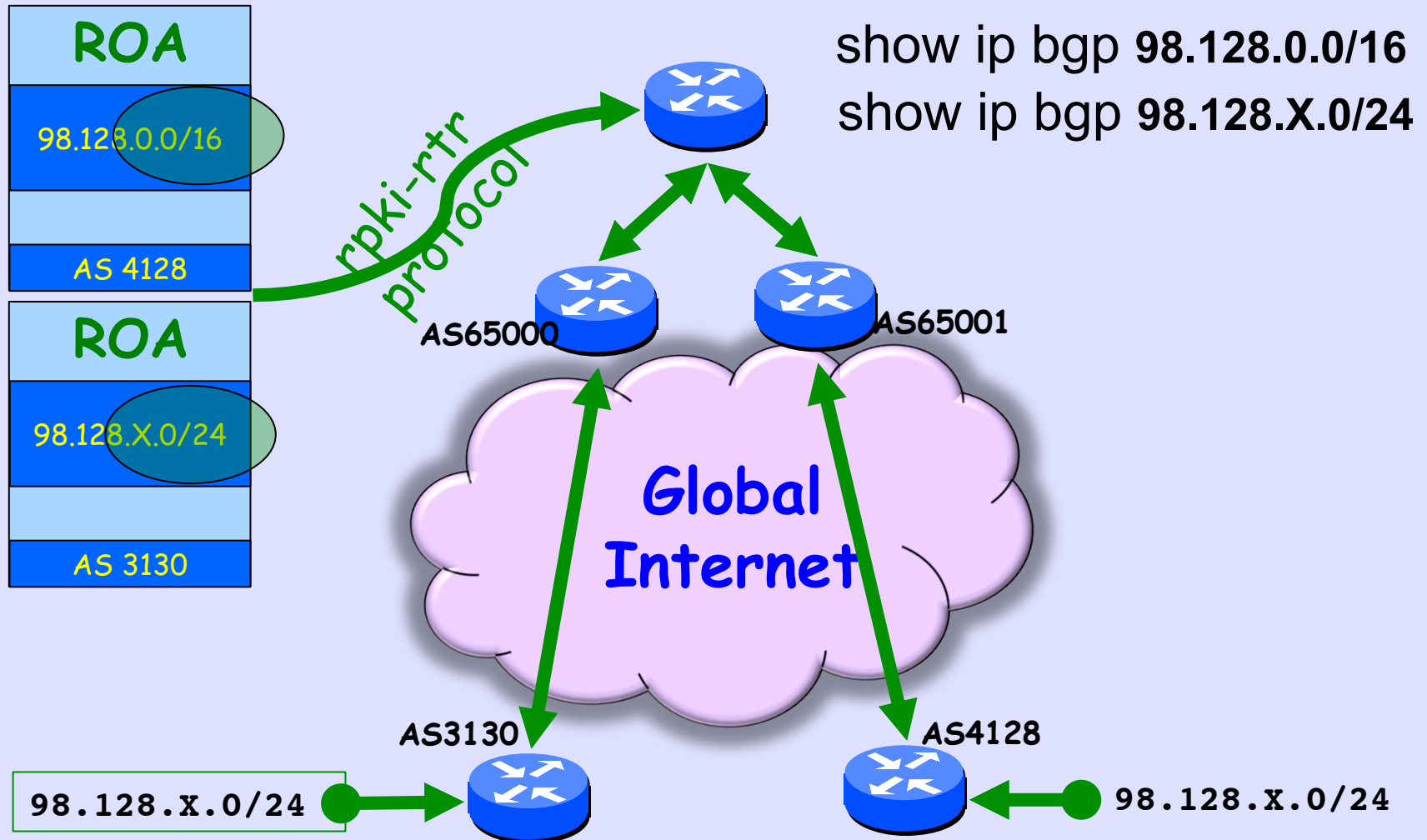
Fat-Finger Detected



ROA Controls Validity



Try Your Own /24



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>.0 255 255 255.0
ip route 98.128.<neighbor>.0 255.255.255.0 \
null0

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

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

Please Do
Try This
At Home