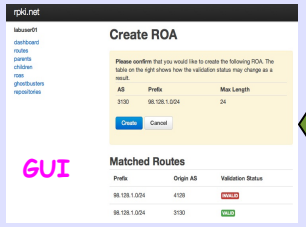
RPKI-Based Origin Validation Lab

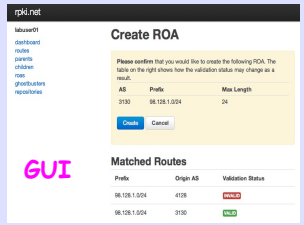
Issuing Parties

Relying Parties



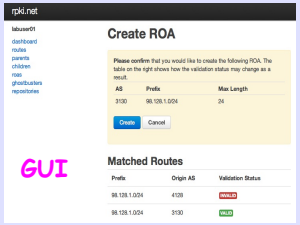
altCA

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

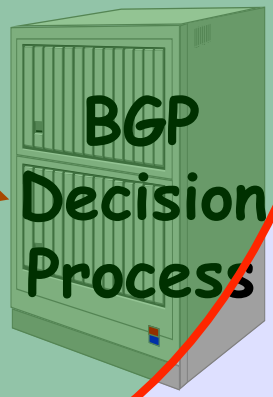
Validated Cache

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



Today

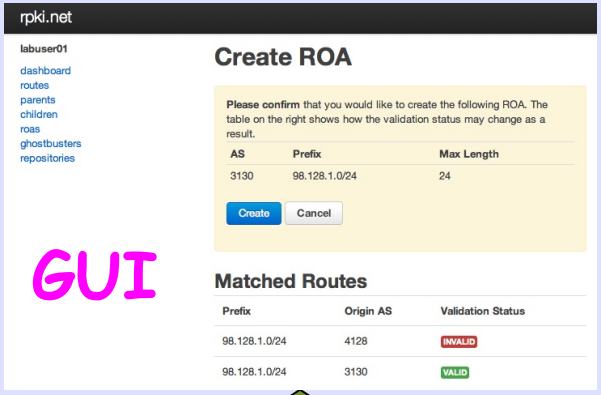
- Register Our Prefixes in CA
- Issue ROAs Using CA's Web Portal
- Configure Routers to get ROAs from Caches

Get Copy of This Preso

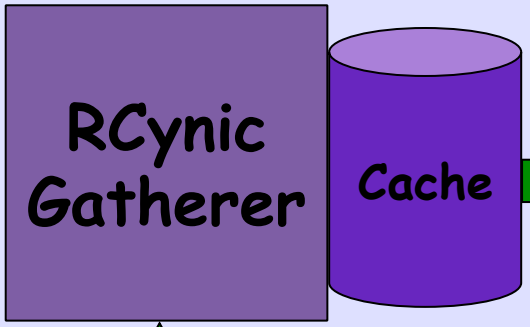
https://psg.com/140118.pdf

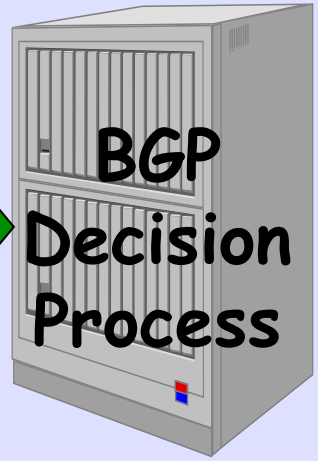
So You Can
Copy and Paste

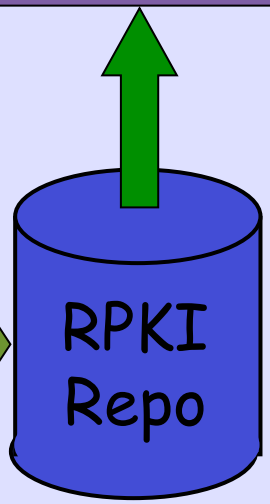
Lab Overview



GUI







Lab Environment

ubu01

ubu02

ubu03

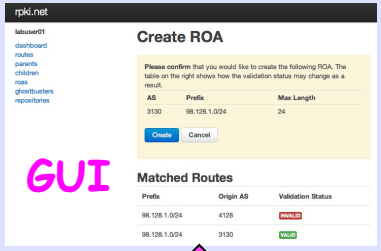
ubu04

ubu05

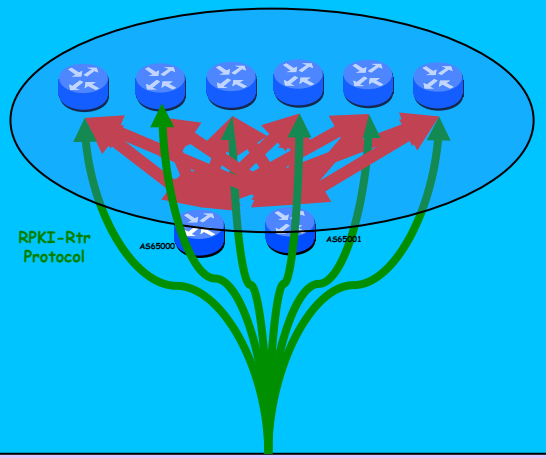
⋮

ubu16

Ubuntu/KVM Server in Ashburn



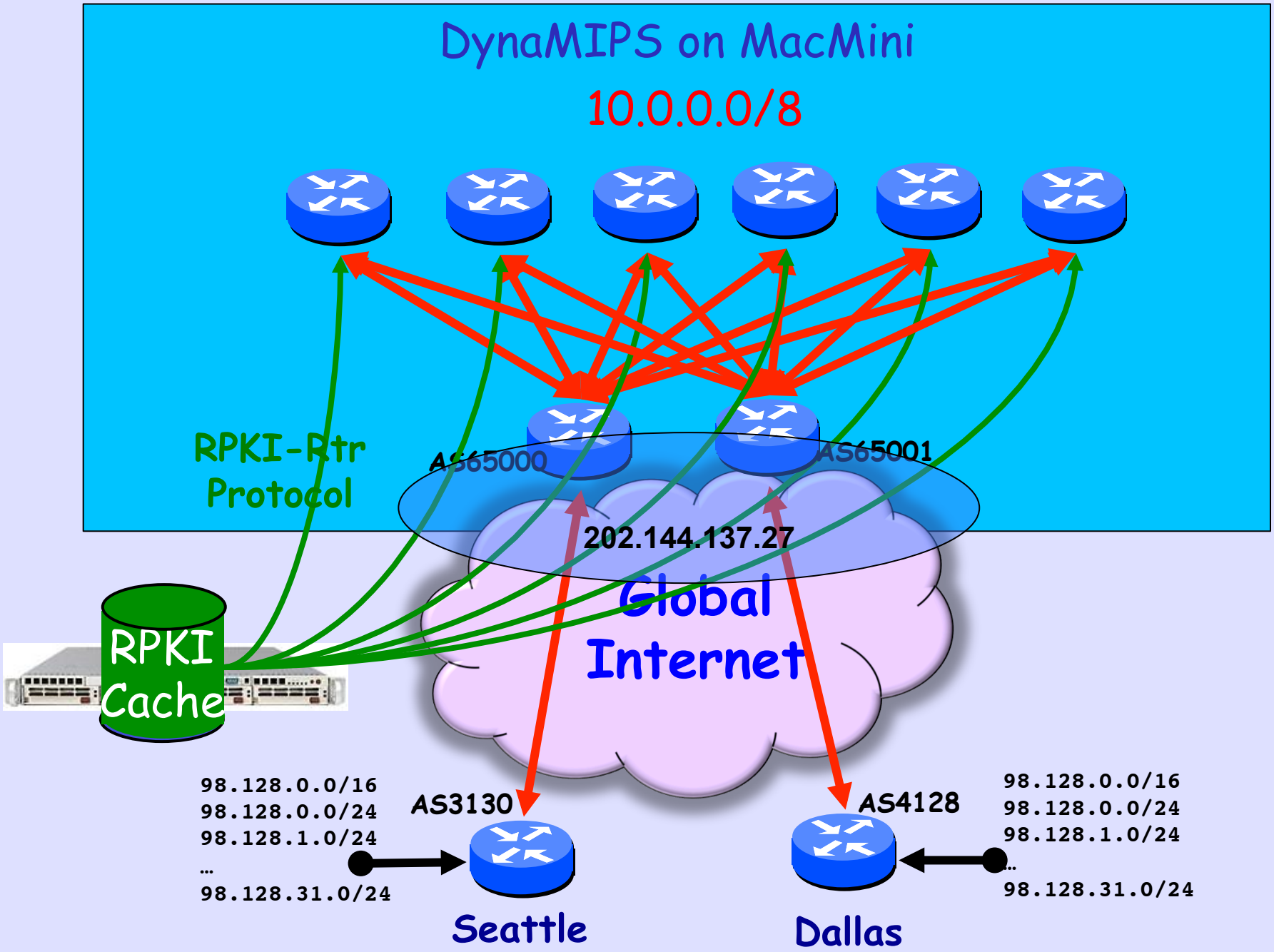
GUI

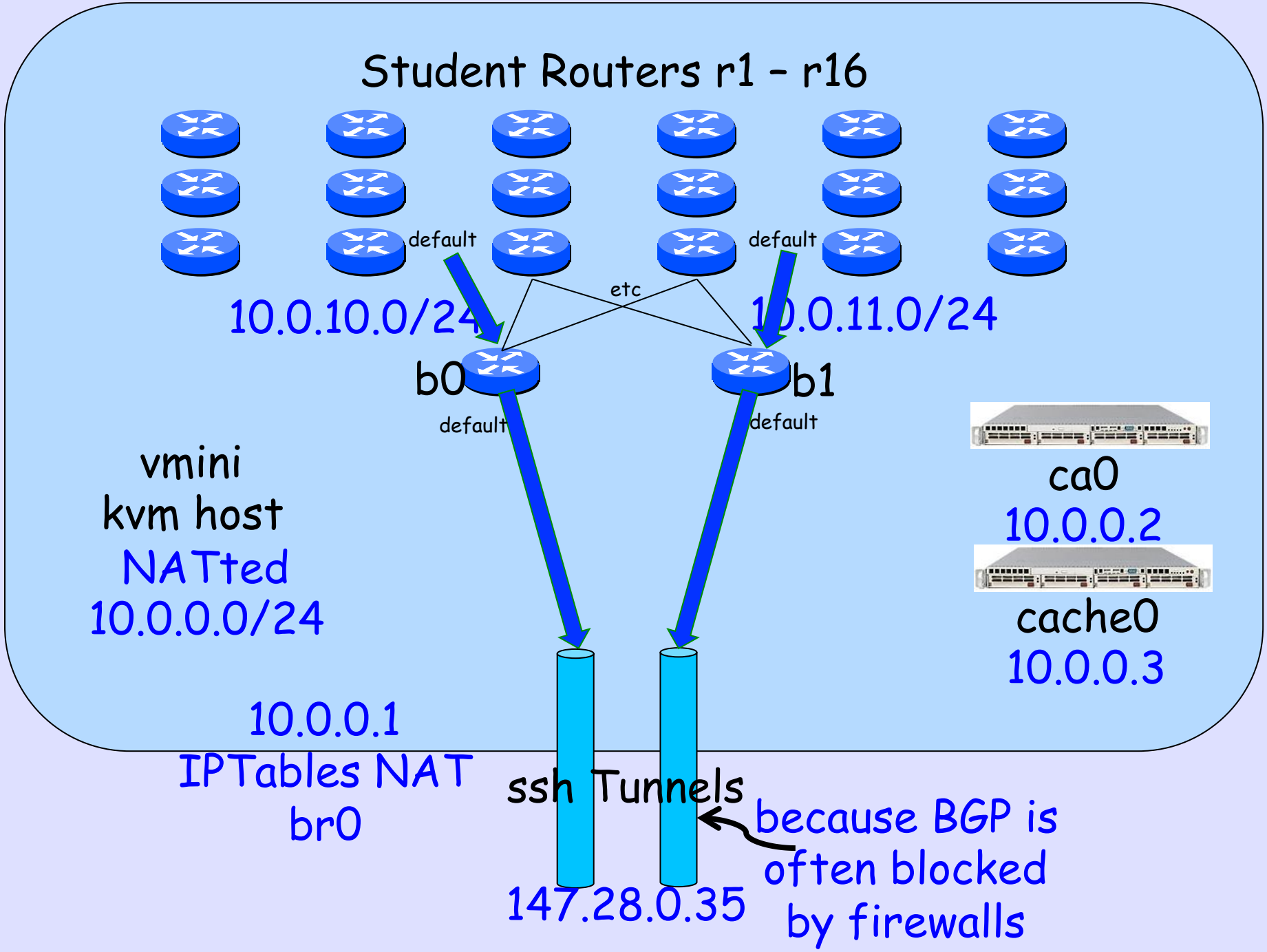


RP - cache0.vmini

CA - ca0.vmini

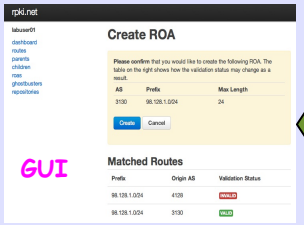
Mac Mini running Ubuntu KVM




Student Routers r1 – r16
default
default
etc
10.0.10.0/24
10.0.11.0/24
b0
b1
default
default
vmini
kvm host
NATted
10.0.0.0/24
ca0
10.0.0.2
cache0
10.0.0.3
10.0.0.1
IPTables NAT
br0
ssh Tunnels
because BGP is
often blocked
by firewalls
147.28.0.35

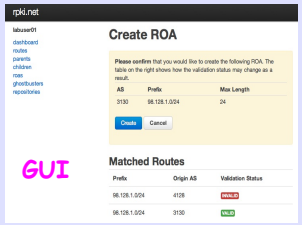
Issuing Parties

Relying Parties



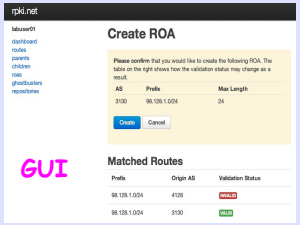
altCA

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

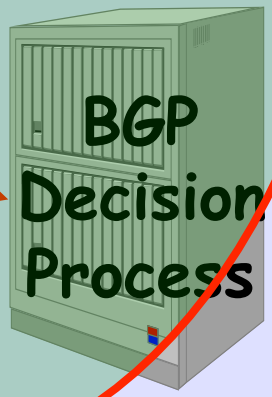
Validated Cache

Pseudo IRR

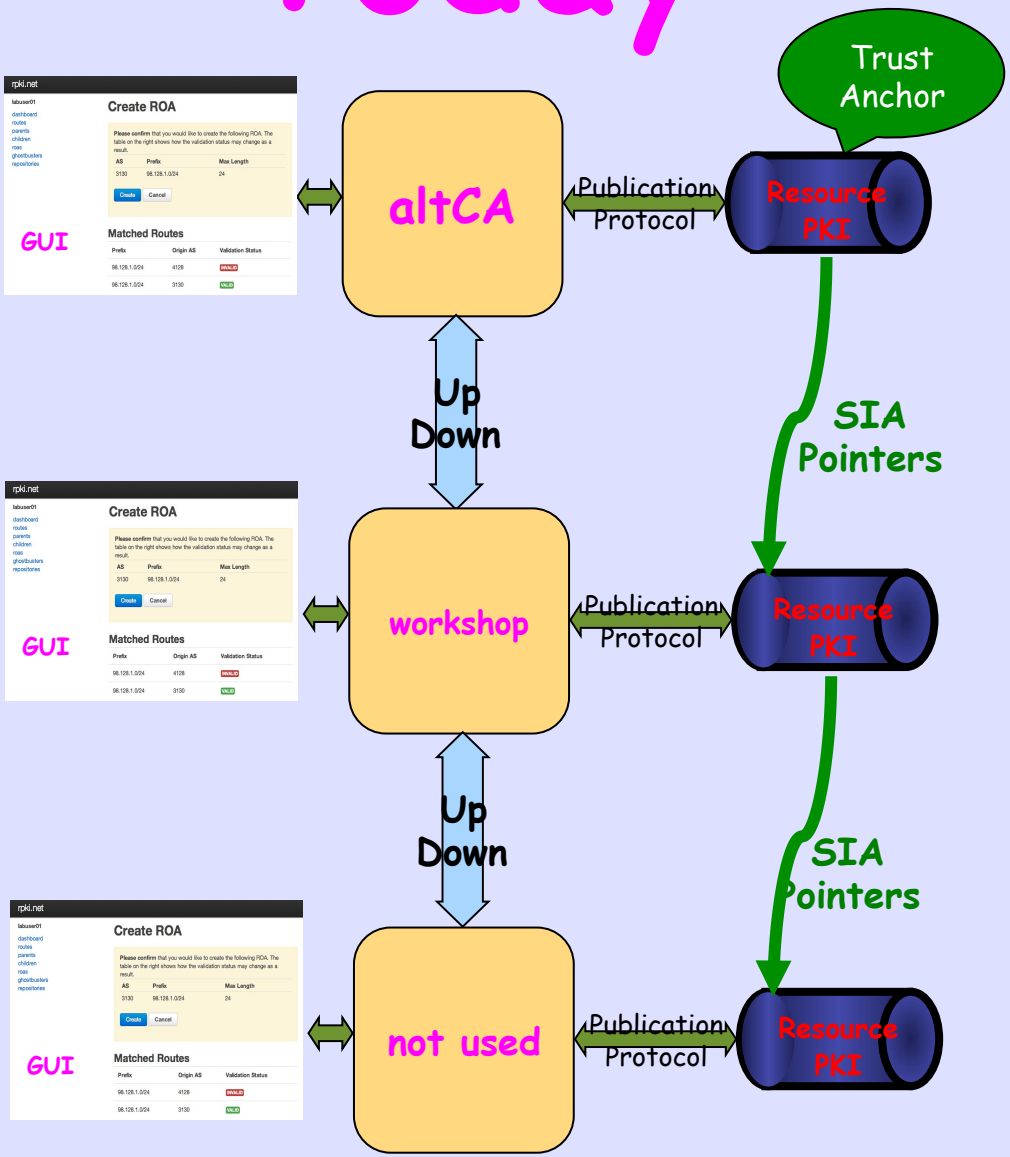
```
route:    147.28.0.0/16
descr:    147.28.0.0/16-16
origin:   AS3130
notify:   irr-hack@rpki.net
mnt-by:   MAINT-RPKI
changed:  irr-hack@rpki.net 20110606
source:   RPKI
```

NOC Tools

Our Focus Today



Today



IP Address Allocation

98.128.0.0/16 ARIN Experimental Allocation

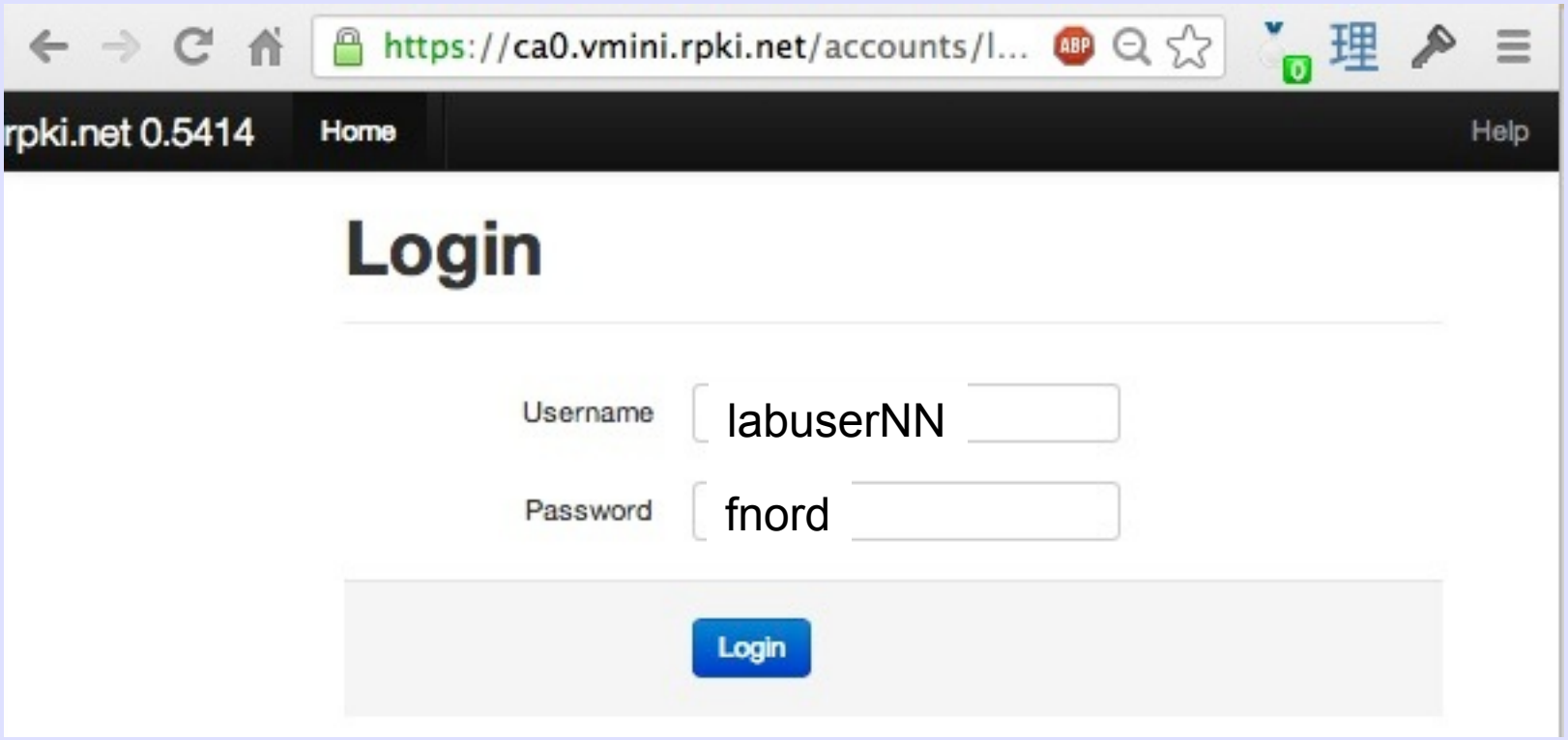
98.128.0.0/24 Instructors Play
98.128.1.0/24 labuser01
98.128.2.0/24 labuser02
…
98.128.32.0/24 labuser32

GUI Accounts

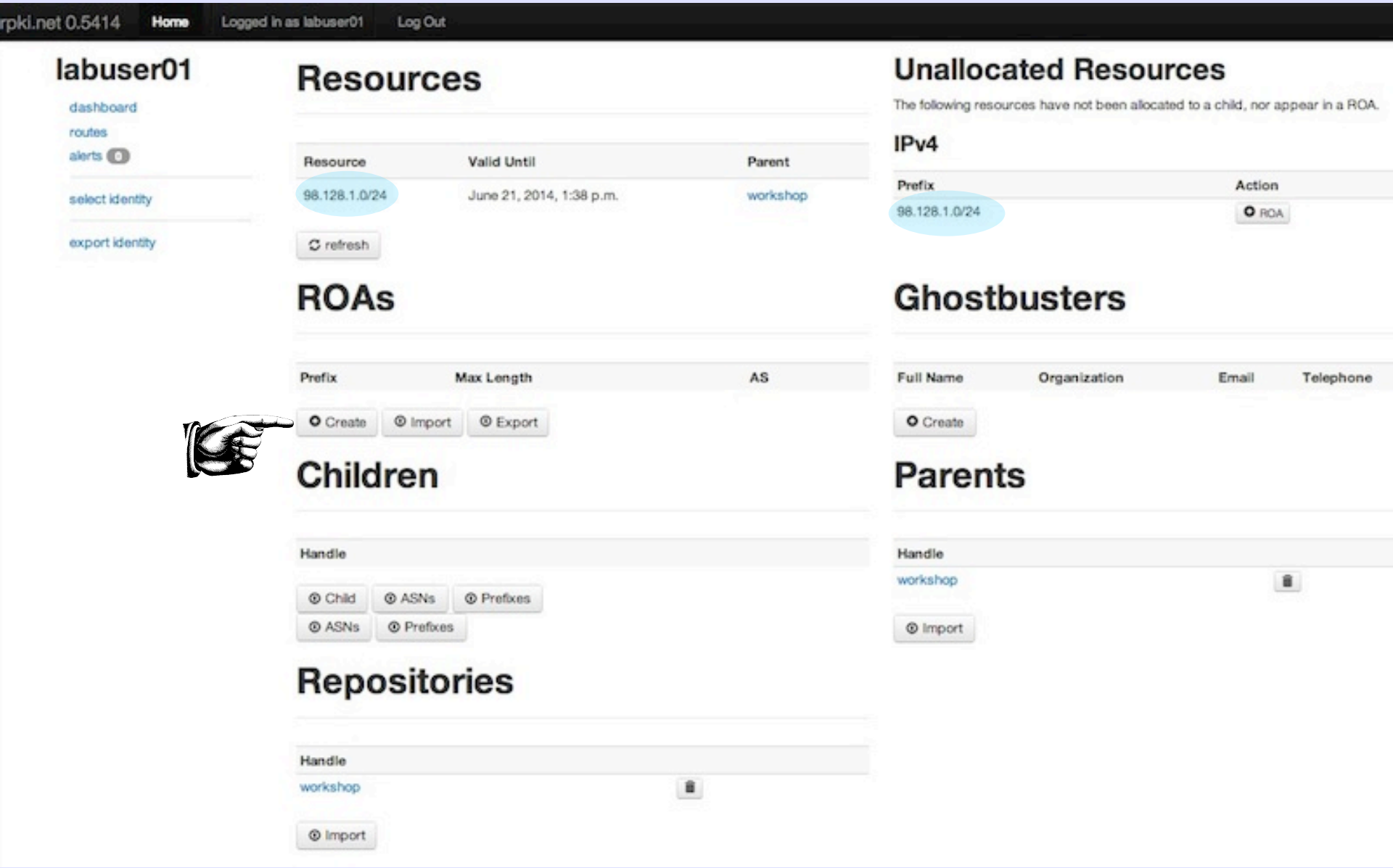
https://ca0.vmini.rpki.net/

UserID	Password
labuser01	fnord
labuser02	fnord
labuser03	fnord
…	
labuser16	fnord

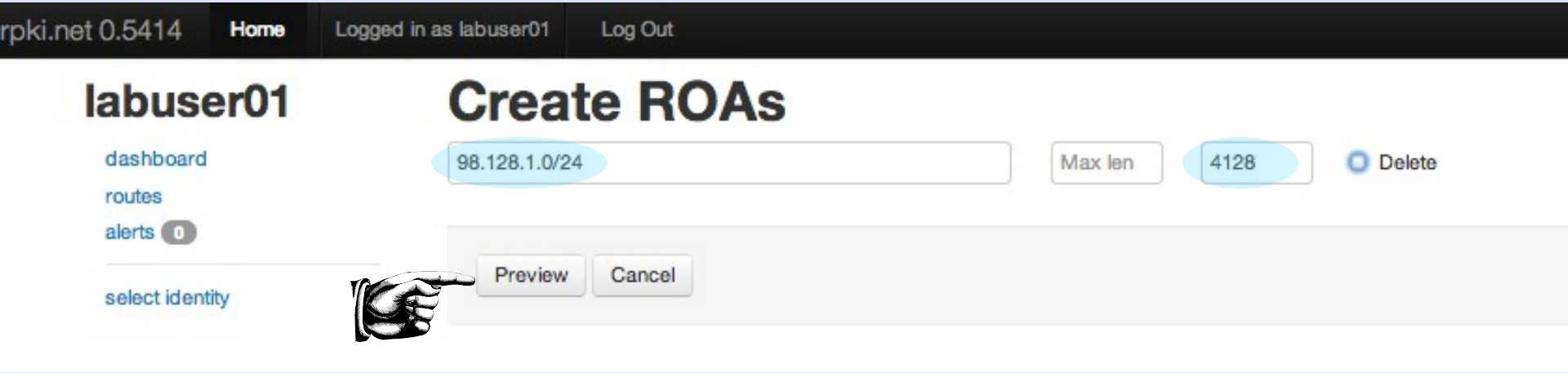
https://ca0.vmini.rpki.net/



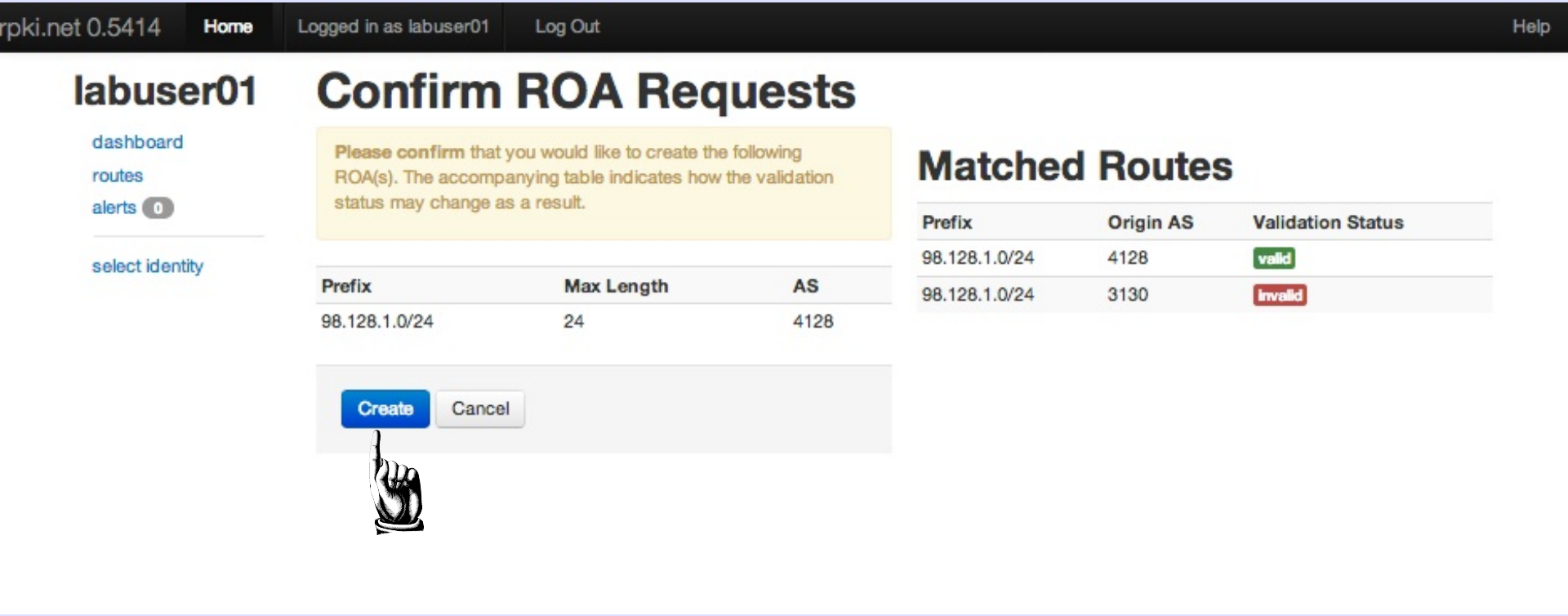
The Dashboard



Create a ROA



What Will Happen?



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
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

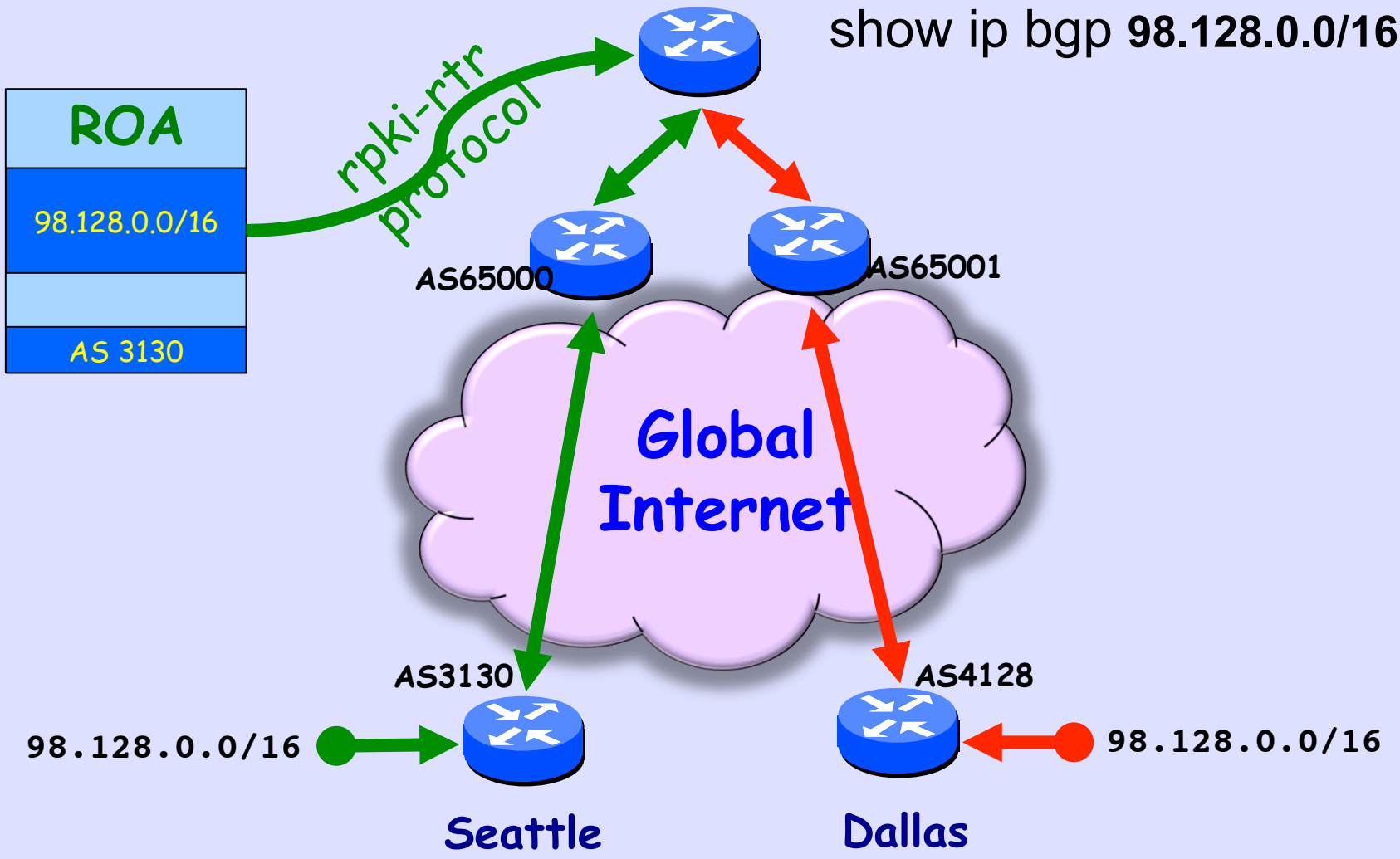
Look at BGP Table

```
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
```

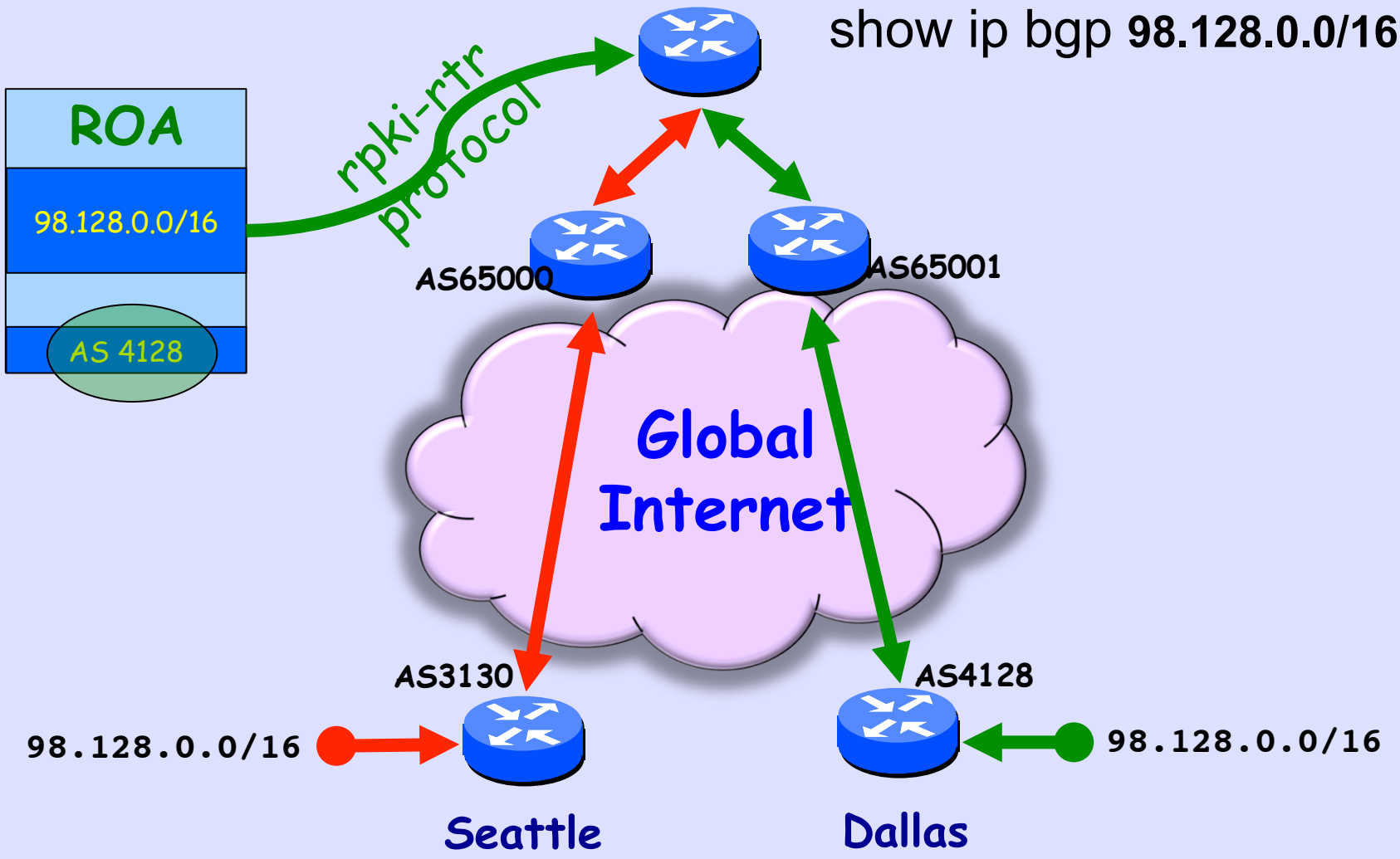
Mis-Origination Caught

```
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
```

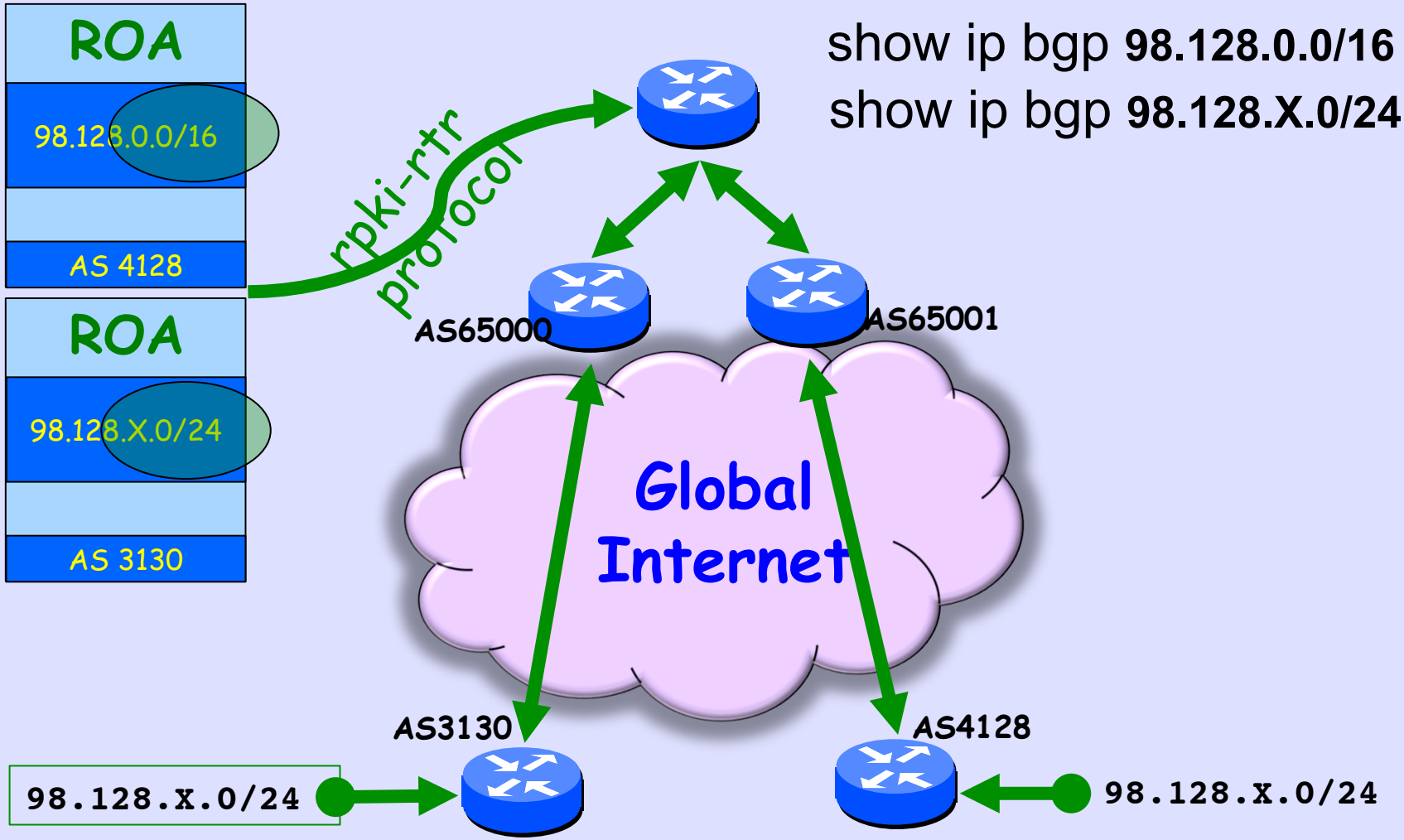
Fat-Finger Detected



ROA Controls Validity



Try Your Own /24



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

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

Please Do Try This At Home