Origin Validation in the infraestructure of RENATA
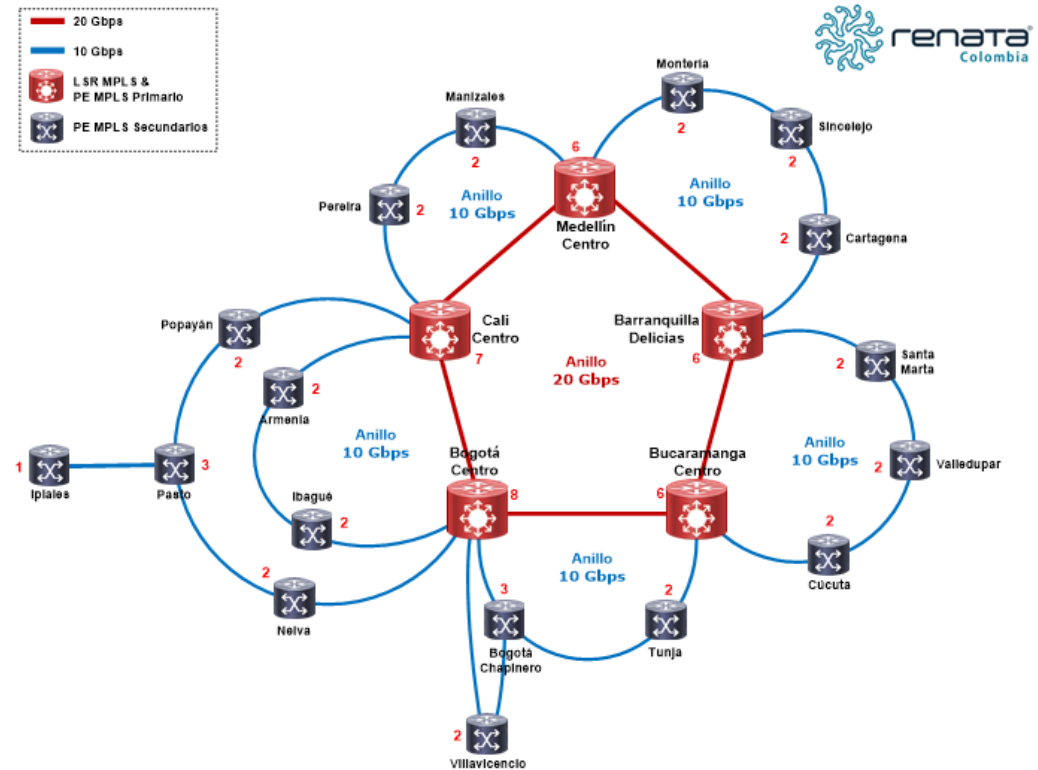
Erika Vega
Erika.vega@renata.edu.co

Infraestructure of RENATA

- Transmission Network of 19,000 km of optical fiber through the national territory.

- Backbone of 22 nodes, interconnected by 100 Gbps lambdas.

- Alcatel Lucent IP / MPLS network based on the high technology that supports 100 Gbps, 200 Gbps, 400 Gbps and 1 Tbit / s

Interconnection points
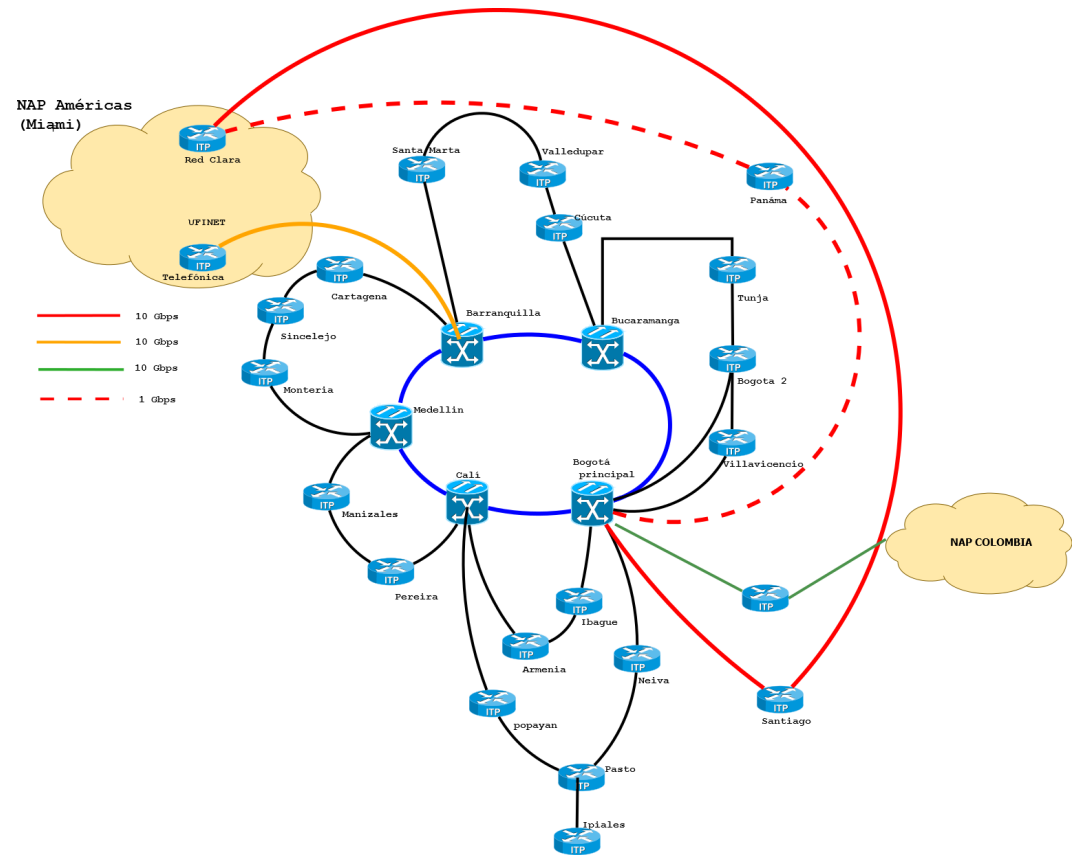
Academic network– CLARA
- A 1 Gb link Panama – Miami.
- A 10 Gb link Santiago –Miami.

Internet access
- A 10 Gb link.

NAP Colombia
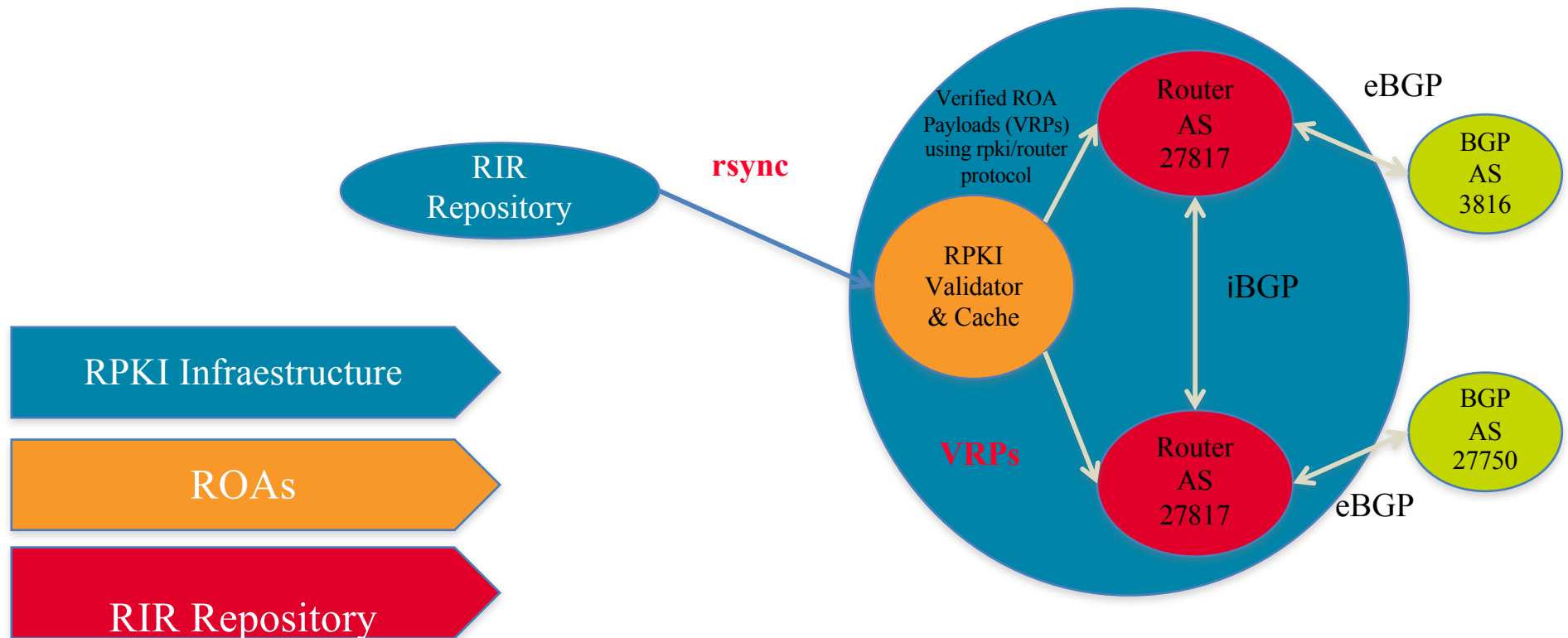- A 10 Gb link.

About the project

The focus will be on the point of exchange at Bogotá node that facilitates connectivity with CLARA Network and NAP Colombia

Goals

1. To validate the content of advertisements at BGP routes that transit through RENATA network.

2. To achieve assurance of critical internet infrastructure and academic networks.

3. To provide new practices to the academic and research community of the country in order to get results and value experiences.

4. To provide information which can be verified independently of the BGP packets.

Technological process

RIR Repository

rsync

Verified ROA Payloads (VRPs) using rpki/router protocol

RPKI Validator & Cache

Router AS 27817

eBGP

BGP AS 3816

iBGP

VRPs

Router AS 27817

BGP AS 27750

eBGP

RPKI Infraestructure

ROAs

RIR Repository

Development

1 Communication and dissemination of the project

2 Training and resources signature

3 Initial configuration and trials

4 Correcting Configurations and Validating Invalid Networks

Training and Resources Signature

How it was made

1. Theoretical and practical virtual seminars
2. Training to different institutions connected to RENATA and to service providers that are part of the NAP Colombia

Training and Resources Signature

Results

- 328 professionals trained at virtual seminars
- 69 professionals trained at seminars
- Telefónica generated the signature for 1109 resources. (From **Not Found** to **Valid**)
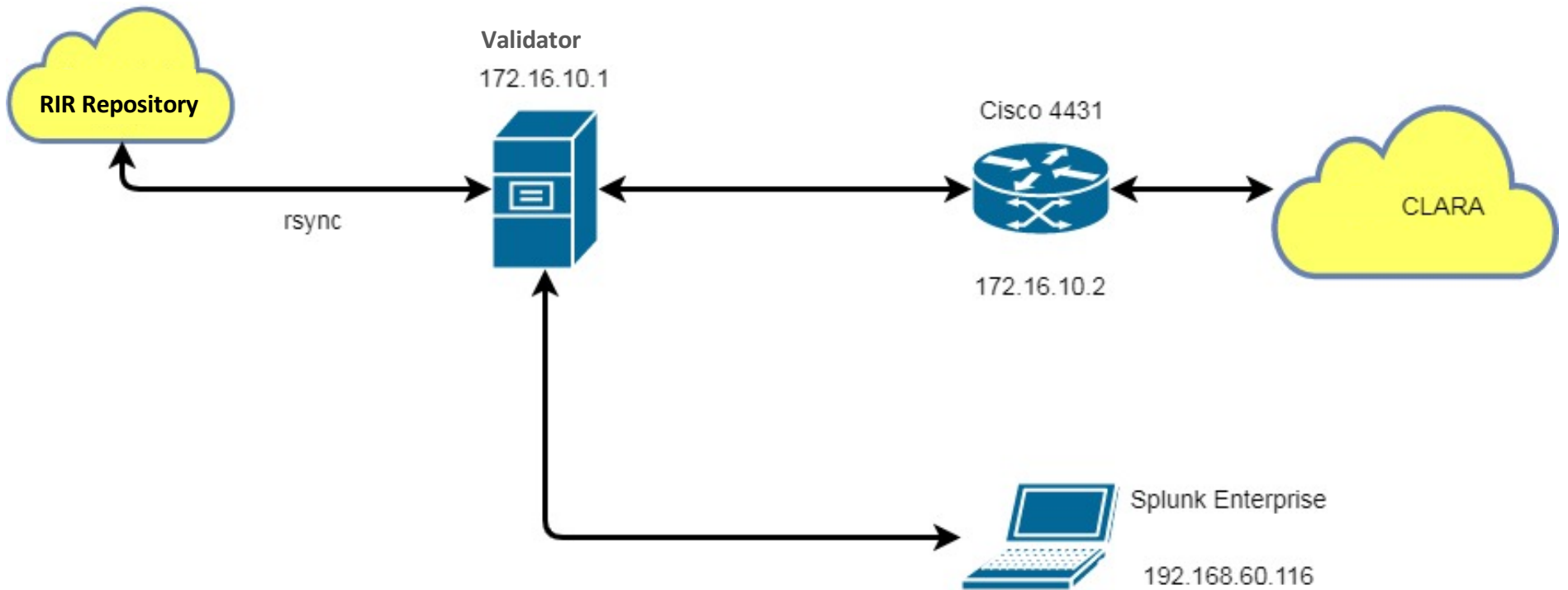
Initial configuration and trials

How it was made

1. Supports in Cisco and Nokia devices were analysed for origin validation. (NOKIA 7750 SR-12, SR-7 and Cisco ISR 9001)

Nokia 7750 SR12 and SR-7	Cisco ASR 9001
TIMOS −C-14.0R3	IOS XR 5.3.3

Topology

RIR Repository

Validator
172.16.10.1

rsync

Cisco 4431

172.16.10.2

CLARA

Splunk Enterprise

192.168.60.116

renata
Colombia

Initial configuration and trials

Results

28713 prefixes going to Red CLARA were validated. Percentages are as follow:

Valid	Invalid	Not Found
28,95%	3,55%	67,50%

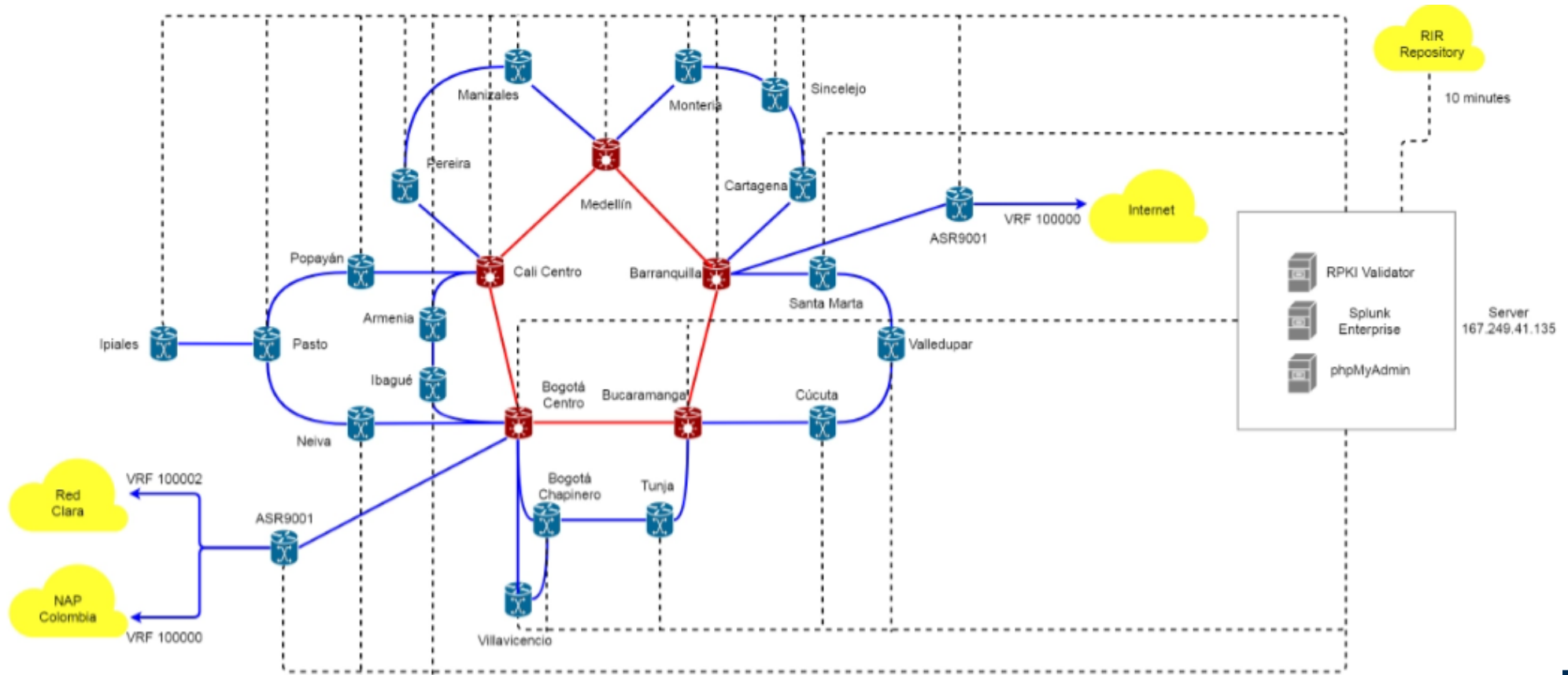# Correcting Configurations and Validating Invalid Networks

How it was made

The validation stage in the production environment was built. See figure in slide 17.

The following platforms were installed:

- RIPE NCC RPKI Validator 2.23
- Splunk Enterprise
- phpMyAdmin

Topology

Correcting Configurations and Validating Invalid Networks

How it was made

The connection between ASR9001-Bogotá and ALU-Bogotá Centro routers with RPKI validator was made. Communication was established between them so origin validation was activated in both devices.

The script designed to consult the prefixes located in VRFs devices was executed

Correcting Configurations and Validating Invalid Networks

How it was made

The analysed routes are part of the VRFs used in RENATA. Those VRFs contain the following amount of prefixes:

	VRF100000	VRF100002
Number of prefixes	14922	17912

Correcting Configurations and Validating Invalid Networks

VRF100000 contains the prefixes directed to NAP Colombia and Internet. Meanwhile, VRF100002 contains prefixes for Red CLARA.

Red Clara			NAP Colombia e Internet		
Valid	Invalid	NotFound	Valid	Invalid	NotFound
5.828%	1.066%	93.104%	46.134%	2.453%	51.411%
5.828%	1.066%	93.104%	46.141%	2.467%	51.391%
5.828%	1.066%	93.104%	46.148%	2.460%	51.391%
5.828%	1.066%	93.104%	46.154%	2.453%	51.391%

Correcting Configurations and Validating Invalid Networks

The origin validation was activated in 24 nodes. It was necessary to generate and install a patch over the OS in the equipments of the MPLS, since the information in the BGP routes is not in the BGP global mode but inside the VRF (address-familly). So it was possible to activate the validation in the address-family in order to validate the known routes contained in the VRF in the following form:

Correcting Configurations and Validating Invalid Networks

Configuration

router bgp 27817
rpki server 10.201.1.2
transport tcp port 8282
refresh-time 600
!
vrf 100000
address-family ipv4 unicast
bgp origin-as validation enable
bgp bestpath origin-as use validity
bgp bestpath origin-as allow invalid

VALIDACIÓN

sh bgp vrf 100000 origin-as validity

Correcting Configurations and Validating Invalid Networks

```
RP/0/RSP0/CPU0:RI-BOG-CEN-1#sh bgp vrf 100000 origin-as validity
Fri Nov 10 14:46:44.256 COL
BGP VRF 100000, state: Active
BGP Route Distinguisher: 27817:100000
VRF ID: 0x60000007
BGP router identifier 10.4.10.25, local AS number 27817
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000016    RD version: 45251533
BGP main routing table version 45251559
BGP NSR Initial initsync version 56445 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
Origin-AS validation codes: V valid, I invalid, N not-found, D disabled
    Network              Next Hop             Metric LocPrf Weight Path
Route Distinguisher: 27817:100000 (default for vrf 100000)
```

Correcting Configurations and Validating Invalid Networks

```
RP/0/RSP0/CPU0:RI-BOG-CEN-1#
RP/0/RSP0/CPU0:RI-BOG-CEN-1#sh bgp vrf 100000 origin-as validity | in  V
Fri Nov 10 14:46:03.233 COL
BGP VRF 100000, state: Active
VRF ID: 0x60000007
Origin-AS validation codes: V valid, I invalid, N not-found, D disabled
V*> 57.74.192.0/19     206.223.124.140         0           0 6505 51964 i
V*> 104.132.160.0/24   206.223.124.143                     0 7087 18747 41264 i
V*  131.0.136.0/22     206.223.124.147       2713          0 6140 3549 10753 61467 i
V*                     206.223.124.151       2703          0 6140 3549 10753 61467 i
V*>                    206.223.124.154                     0 18678 61467 i
V*> 131.108.168.0/22   206.223.124.133                     0 10299 i
V*                     206.223.124.134                     0 10299 i
V*                     206.223.124.147       2593          0 6140 3549 10299 10299 10299 10299 10299 10299 10299
10299 i
V*                     206.223.124.151       2583          0 6140 3549 10299 10299 10299 10299 10299 10299 10299
10299 i
V*> 131.161.232.0/24   206.223.124.154                     0 18678 262195 11664 11664 52327 52327 52327 52327 52327 i
V*> 131.161.233.0/24   206.223.124.154                     0 18678 262195 11664 11664 52327 52327 52327 52327 52327 i
V*> 131.161.234.0/24   206.223.124.154                     0 18678 262195 11664 11664 52327 52327 52327 52327 52327 ?
V*> 131.161.235.0/24   206.223.124.154                     0 18678 262195 11664 11664 52327 52327 52327 52327 52327 i
V*> 131.221.32.0/24    206.223.124.154                     0 18678 52368 263702 i
V*> 131.221.164.0/23   206.223.124.154                     0 18678 27901 i
V*> 131.221.166.0/23   206.223.124.154                     0 18678 27901 i
V*> 132.255.20.0/24    206.223.124.142                     0 27951 i
```

Correcting Configurations and Validating Invalid Networks

Results

- 1150 signed prefixes since the first training.

- 328 professionals trained.

- Increasing of valid routes in prefixes published in Internet and NAP Colombia.

- The patch was applied only in the two interconnection points since the patch for the TiMOS –C14.0.R3 is still under development.
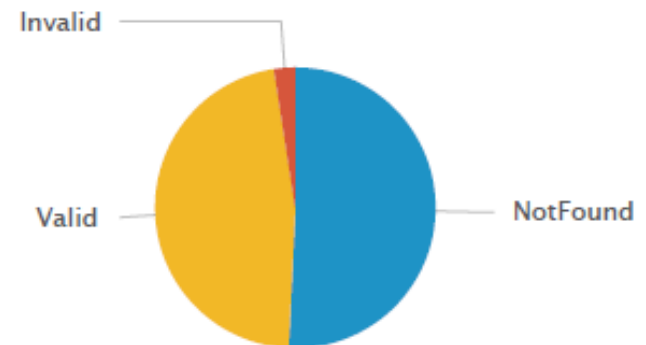
VRF 100000 report

Statistics of BGP prefixes of ALU-BOG (VRF 100000) - NAP Colombia and commercial Internet

Consulted on October 31

Validity Status ⇕	Number of Prefixes ⇕	Percent ⇕
NotFound	7572	50.767684
Valid	6982	46.811934
Invalid	361	2.420382

Graph of BGP prefixes of ALU-BOG (VRF 100000) - NAP Colombia and commercial Internet
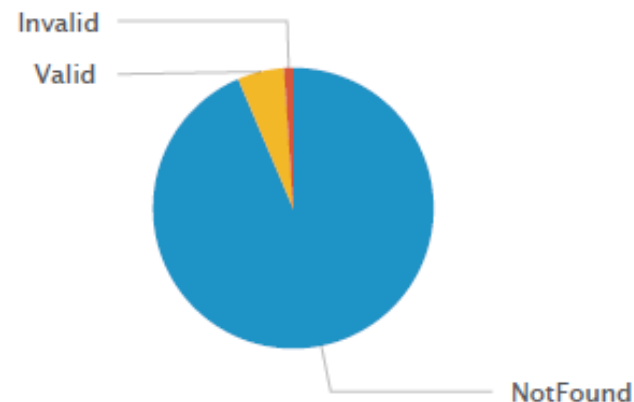
Consulted on October 31

VRF 100002 report

Statistics of BGP ads of the ASR9001-BOG (VRF 100002) - Red Clara

Consulted on October 31

Validity Status ⇕	Number of Prefixes ⇕	Percent ⇕
NotFound	16764	93.596114
Valid	961	5.365418
Invalid	186	1.038468

Graphic of BGP ads of the ASR9001-BOG (VRF 100002) - Red Clara

Consulted on October 31

Impact and innovation

- Worldwide this project is the first one in considering the implementation of the origin validation in a national network.

- Innovative achivement towards security in critical infrastructure of Internet and academic networks.

Next steps

- Activate the parch in the Nokia devices (devolopment)

- Expand the idea in the academics networks.(collaborative work with the CLARA network)

- Experiment with SLURM and whitelist and other validator extensions