Routing Policy System WG

Cengiz Alaettinoglu (ISI)

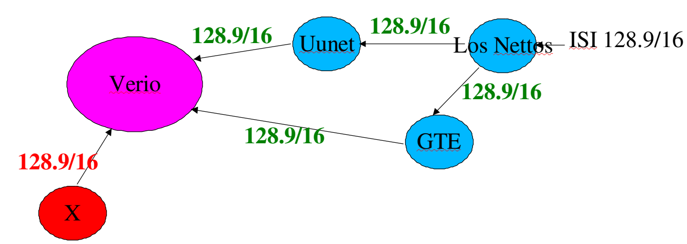
Main Work Items

- Routing Policy Specification Language
  - completed
- Routing Policy System Security
  - maturing
  - user feedback needed
- Distributed Routing Policy System
  - ongoing
  - mostly interesting to implementors

Routing Policy Specification Language (RPSL)

- Proposed standard
  - RFC 2280 (to be obsoleted next week)
- Tutorials
  - RIPE
  - APRICOT
  - NANOG
- Implementations
  - RAToolSet/BIRD — 100% completed
  - IRRd — ongoing
  - the new RIPE Server — ongoing
  - old perl Server — exists

Routing Policy System Security



- is UUNet/GTE/X authorized to announce 128.9/16?
- is Los Nettos authorized to originate 128.9/16?

Problem is real

- daily, someone's leaking someone else's prefix
- BGP–>RIP–>BGP injection
- UUNET's 128/7 leak
- bogon 0/0, 10/8 leaks

RPS Security

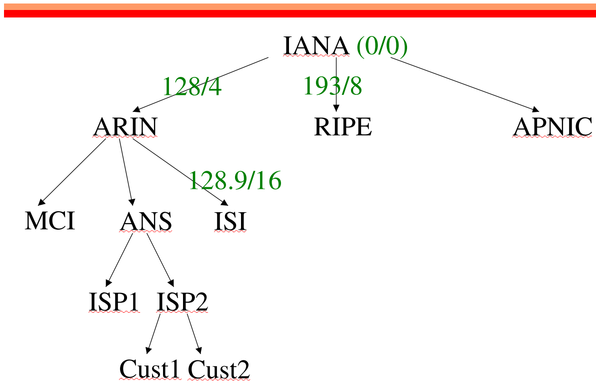
- Authentication model
  - who
  - are we talking to X or MCI?
  - draft–ietf–rps–dbsec–pgp–authent–01
- Authorization model
  - what
  - can Los Nettos originate ISI's route?
  - draft–ietf–rps–auth–03

Authorization Model

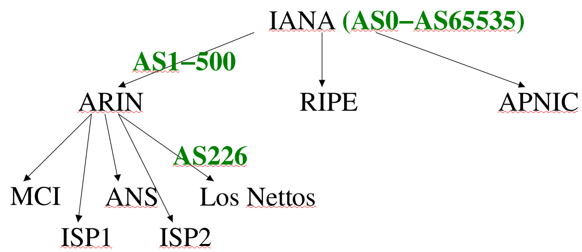
```
aut-num:  AS226
descr:    los nettos ISP in LA
mnt-by:   mnt-losnettos

inetnum:  128.9.0.0 - 128.9.255.255
descr:    USC Information Sci. Inst.
mnt-by:   mnt-isi

route:    128.9.0.0/16
origin:   AS226
```

Who has the authority?

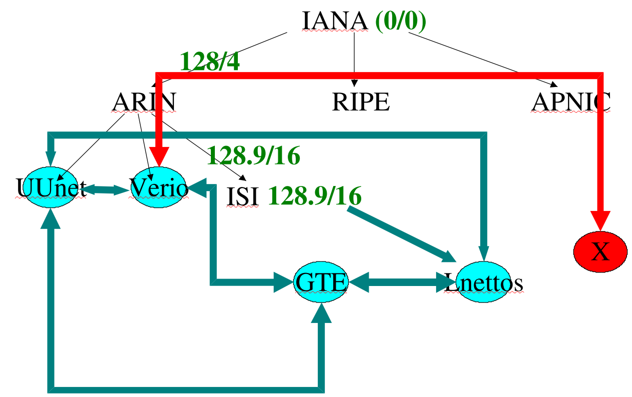
Address Assignment



AS# Assignment



Routing



route Objects

```
aut-num: AS226
mnt-by:  mnt-losnettos

inetnum: 128.9.0.0 - 128.9.255.255
mnt-by:  mnt-isi

route:   128.9.0.0/16
origin:  AS226
```

Who has the authority?

Los Nettos and ISI

```
aut-num:    AS226
mnt-by:     mnt-losnettos

inetnum:    128.9.0.0 - 128.9.255.255
mnt-by:     mnt-isi

route:      128.9.0.0/16
origin:     AS226
mnt-by:     mnt-isi, mnt-losnettos
```

Can be created if both parties sign.

Los Nettos

```
inetnum:     128.9.0.0 - 128.9.255.255
mnt-by:      mnt-isi
mnt-routes:  mnt-losnettos

aut-num:     AS226
mnt-by:      mnt-losnettos

route:       128.9.0.0/16
origin:      AS226
mnt-by:      mnt-losnettos
```

Can be created by mnt–losnettos.

ISI

```
Inetnum:     128.9.0.0 - 128.9.255.255
mnt-by:      mnt-isi

aut-num:     AS226
mnt-by:      mnt-losnettos
mnt-routes:  mnt-isi

route:       128.9.0.0/16
origin:      AS226
mnt-by:      mnt-isi
```

Can be created by mnt–isi.

Los Nettos or ISI

```
inetnum:     128.9.0.0 - 128.9.255.255
mnt-by:      mnt-isi
mnt-routes:  mnt-isi, mnt-losnettos

aut-num:     AS226
mnt-by:      mnt-losnettos
mnt-routes:  mnt-isi, mnt-losnettos

route:       128.9.0.0/16
origin:      AS226
mnt-by:      mnt-isi
```

Can be created by mnt–isi.

Rules

- Rules for object creation
  - aut–num, inetnum, as–block, route, mntner, person, role, ...
- Rules for updates and deletions
  - Maintainer of the object can update/delete
  - reclain/no–reclaim
  - auth–override
- draft–ietf–rps–auth–03

Distributed Routing Policy System

- draft–ietf–rps–dist–01
- Protocol for replication
  - flooding based
  - both pull and push of data
  - automatic discovery of registries
  - light–weight option
- Rules for ensuring
  - delegation
  - authorization
  - consistency
  - grand fathering legacy objects