

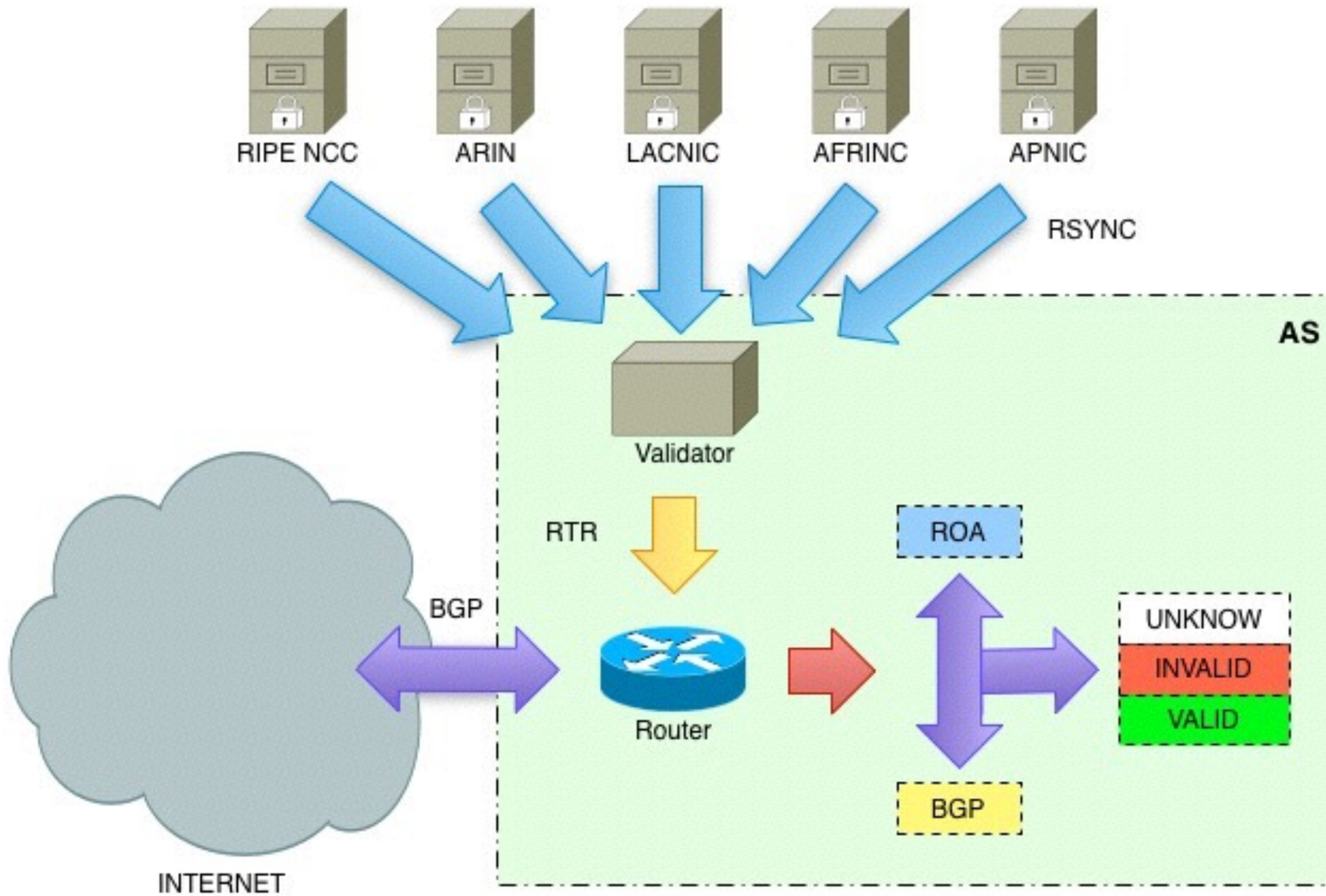


RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RPKI

A quick configuration intro

RPKI Overview

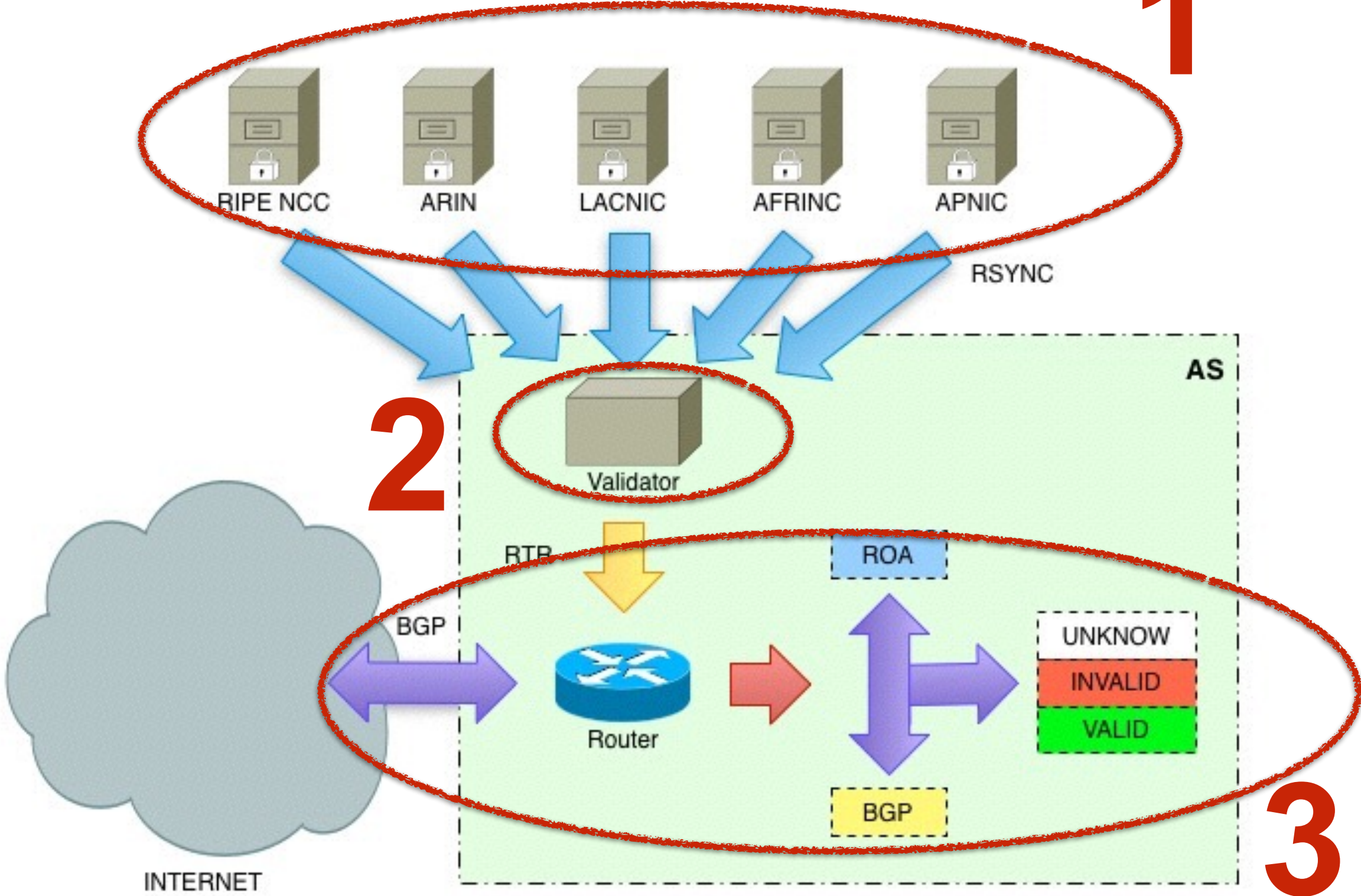


Simply put



- 3 parts
 - Create certificates
 - Install/run validator
 - Validate certificates (router configuration)

RPKI Overview



1. Creating ROAs



RPKI Dashboard 9 CERTIFIED RESOURCES NO ALERT EMAIL CONFIGURED

41 BGP Announcements **4 ROAs**

4 Valid 1 Invalid 36 Unknown 3 OK 1 Causing problems

BGP Announcements **Route Origin Authorisations (ROAs)** History

Create ROAs for selected BGP Announcements Valid Invalid Unknown

<input type="checkbox"/>	Origin AS	Prefix	Current Status	
<input type="checkbox"/>	AS12654	2001:7fb:fe01::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:fe0c::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:fe0f::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:ff00::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:ff01::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:ff02::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	AS12654	2001:7fb:ff03::/48	UNKNOWN	<input type="checkbox"/> <input type="checkbox"/>

2. Validator



- Download from RIPE NCC
 - <https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources>
- Requires Java, rsync
- Runs standalone

- `./rpki-validator.sh start`

3. Validate prefixes



- Take routing decisions based on results of validation
 - Valid
 - Invalid
 - Unknown

Support in Routers



- **Cisco:**
 - XR 4.2.1 (CRS-x, ASR9000, c12K) / XR 5.1.1 (NCS6000, XRv)
 - XE 3.5 (C7200, c7600, ASR1K, CSR1Kv, ASR9k, ME3600...)
 - IOS15.2(1)S
- **Juniper** has support since version 12.2
- **Alcatel Lucent** has support since SR-OS 12.0 R4
- **Quagga** has support through BGP-SRX
- **BIRD** has support for ROA but does not do RPKI-RTR

Cisco config - 1



```
route-map rpki-loc-pref permit 10  
match rpki invalid ←  
set local-preference 90
```

!

```
route-map rpki-loc-pref permit 20  
match rpki not-found ←  
set local-preference 100
```

!

```
route-map rpki-loc-pref permit 30  
match rpki valid ←  
set local-preference 110
```

Cisco config - 2



```
router bgp 64500
  bgp log-neighbor-changes
  bgp rpki server tcp 10.1.1.6 port 8282 refresh 5
  network 192.0.2.0
  neighbor 10.1.1.2 remote-as 64510
  neighbor 10.1.1.2 route-map rpki-loc-pref in
```

Juniper config - 1



```
policy-options {  
  policy-statement validation {  
    term valid { ←  
      from {  
        protocol bgp;  
        validation-database valid;  
      }  
      then {  
        validation-state valid;  
        community add origin-validation-state-valid;  
        next policy;  
      }  
    }  
  }  
}
```

Juniper config - 2



```
policy-options {
  policy-statement validation {
    term invalid { ←
      from {
        protocol bgp;
        validation-database invalid;
      }
      then {
        validation-state invalid;
        community add origin-validation-state-invalid;
        next policy;
      }
    }
  }
}
```

Juniper config - 3



```
policy-options {  
  policy-statement validation {  
    term unknown { ←  
      from protocol bgp;  
      then {  
        validation-state unknown;  
        community add origin-validation-state-  
unknown;  
        next policy;  
      }  
    }  
  }  
}
```


Juniper config - 4

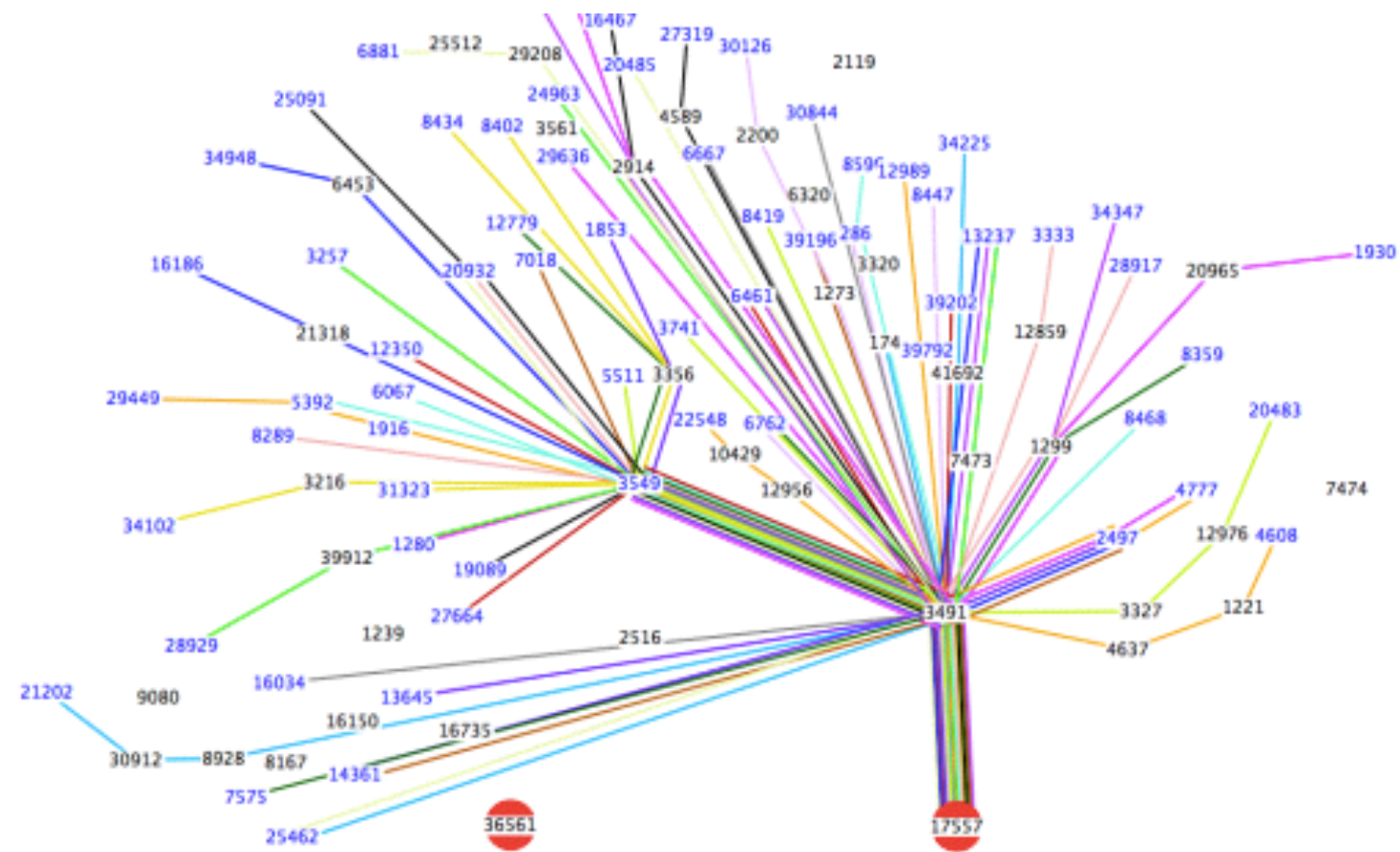


```
protocols {
  bgp {
    group mypeers {
      import route-validation;
      peer-as 200;
      neighbor 10.1.1.2;
    }
  }
}
```

Routing Incidents



- Misconfiguration
 - No malicious intentions
 - Software bugs
- Malicious
 - Competition
 - Claiming “unused” space
- Targeted Traffic Misdirection
 - Collect and/or tamper with data



BGPsec



- Still in draft state
- Secures route propagation by using signatures in AS-Path



Questions



mstucchi@ripe.net
@TrainingRIPENCC
<https://ripe.net/certification>