



# **JUNOS implementation of BGP Route Origin validation**

Hannes Gredler <[hannes@juniper.net](mailto:hannes@juniper.net)>



---

## IMPLEMENTED DRAFTS & FUNCTIONALITY

---

### draft-ietf-sidr-rpki-rtr-11

No SSH support, raw TCP only, IPv4 and IPv6 transport static entries

### draft-ietf-sidr-origin-validation-signaling-00

No change of BGP path selection logic  
Has to be implemented using policy

### draft-ietf-sidr-pfx-validate-01

JUNOS RV-DB caches withdraws as well, this requires slight change in the eval logic to only consider “Positive” updates

Full Policy support

Non-Stop routing, graceful restart support

Routing instance (vrf) and Logical System support

---

# Client configuration

---

```
routing-options {
  route-validation {
    group in-POP {
      max-sessions 2; ## how many sessions per group
      session 192.168.1.100 {
        refresh-time 300; ## query for serial each N seconds
        hold-time 900; ## after N seconds of inactivity drop session
        record-lifetime 900; ## keep validation state for N seconds
        preference 200;
        port 4711;
      }
      server 192.168.1.101;
      server 192.168.1.102;
      server 192.168.1.103;
    }
    group public-RIPE {
      server abcd::1234:1;
    }
    static {
      route 208.65.152.0/22 {
        maximum-length 24;
        origin-autonomous-system 17557;
        validation-state invalid; ## negative update
      }
    }
  }
}
```

# Policy language extensions

```
policy-options {
  term check-valid-state-and-tag-stuff {
    from {
      validation-state valid;
    }
    then {
      accept;
      local-preference 110;
      community origin-validation add;
      validation-state valid;
    }
  }
  term check-invalid-state-and-reject {
    from {
      validation-state state invalid;
    }
    then {
      reject;
    }
  }
}
```

- From **validation-state** qualifier triggers evaluation in the RV database.
- RTM\_Metric6 is the new home for validation state
  - Caching Logic: Presence of RTM\_Metric6 does not cause re-evaluation
- Community value is built **on the fly** from RTM\_Metric6 state

---

# UI output

---

```
root@R2> show route-validation database <prefix> session <session-ip> mismatch
RV database for instance master
  Total IPv4 records: 551
  Total IPv6 records: 191

Prefix          Origin-AS Session      State  Mismatch
1.2.3.0/24-32   45163 1.1.5.2    valid
1.4.0.0/24-32   45163 1.1.5.2    valid
1.10.10.0/24-32 45163 1.1.5.2    valid
49.238.32.0/19-32 17771 1.1.5.2    invalid *
49.238.32.0/19-32 17772 13.2.4.46  valid  *
49.244.0.0/16-32 23752 1.1.5.2    valid
218.100.59.0/24-32 45482 1.1.5.2    valid
[ ... ]
2001:de8:9::/48-128 45482 1.1.5.2    valid

root@R2> show route 91/10 detail [validation-state valid | invalid | unknown]

inet.0: 345789 destinations, 345789 routes (345754 active, 0 holddown, 35 hidden)
91.0.0.0/10 (1 entry, 1 announced)
  *BGP      Preference: 170/-111
            Next hop type: Indirect
            Next-hop reference count: 1037192
            Source: 192.168.69.71
            Next hop type: Router, Next hop index: 516
            Next hop: 10.94.175.254 via em0.0, selected
            Protocol next hop: 192.168.69.71
            Indirect next hop: 15324000 131070
            State: <Active Ext>
            Local AS: 65435 Peer AS: 10458
            Age: 1d 4:46:55      Metric2: 0
            Task: BGP_10458_69.192.168.69.71+179
            Announcement bits (2): 0-KRT 5-Resolve tree 1
            Validation State: <valid>
            AS path: 10458 14203 2914 3320 I
            Communities: 2914:420 2914:2000 2914:3000
            Accepted
            Localpref: 110
            Router ID: 207.17.136.192
```



everywhere

---

## Local Cache configuration (test-only)

---

```
routing-options {
  route-validation {
    group local-cache {
      session 192.168.1.100 {
        local-cache;
      }
    }
  }
}
```