Matthew Williams

From: Matthew Williams [matthew@ripe.net]
Sent: 11 February 2004 15:23
To: ris@ripe.net
Subject: Main Points - myASn Meeting - 04.02.2004 - Final

I'll stick it on iii too.
/Matthew
==========

Main Points - myASn Meeting - 04.02.2004

Action Plan:

We now have a mechanism in place that looks at all BGP events and tags the ones that meet certain criteria. The next step is to aggregate them and generate alarms:

1. Matthew to write down alarm mechanism.

+++

A. The Two Mechanisms that Trigger Alarms

The first mechanism, which is based on the alarm event counter, can be manipulated by the Hold-down Event (HDE), a threshold, and the Time-to-live (TTL), a monitoring period. When the counter exceeds the HDE within or equal to the TTL an alarm should be triggered by myASn. The second relates to the longevity of the alarm event's condition in 'active' state. A condition is 'active' until the peer that announced the 'offending' NLRI sends out a withdrawal for the exact match of that prefix. The Hold-down Time
(HDT) is the sole user-configurable setting that affects this mechanism. If the 'active' state continues for a longer duration than the specified HDT then an alarm should be triggered. The alarm consists of an entry for the 'offending' peer in an email summary, which is sent to the user at regular time intervals.

These processes operate independently of each other.

B. Definition of (Origin) Alarm Events and the Hold-down Event (HDE)

Alarm events are monitored and generated per peer for each RRC. A counter shall be incremented by one when a particular peer 'offends' the user configuration of 'what is expected' by forwarding to the RRC a BGP announcement with NLRI that is inconsistent with expectations. If the counter surpasses the user-configurable HDE value within or equal to the TTL, an alarm should be triggered by myASn.

In the case of Origin alarm events, we monitor ranges of IP addresses, ie 'address space'. This implies that 'offending' NLRI with both exact matches and more specific prefixes in regard to that address space shall increase the above mentioned counter, for
instance:

- 10.10.0.0/16 has been allocated to ASxxx by RIPE NCC, and is monitored by myASn.

- Assume peer A.B.C.D announces 10.10.0.0/16 and 10.10.192.0/18, while peer D.C.B.A announces 10.10.0.0/16, 10.10.0.0/17, 10.10.128.0/17 and 10.10.192.0/18 to RRCnn as originating from ASyyy.

- This scenario should increment the alarm event counter by two in the case of peer

A.B.C.D and four in the case of peer D.C.B.A.

The HDE does not take into account withdrawals.

+++

2. Desired Alarm Types (James and Alexis worked out regexps towards the end of meeting)

- 'Transit of Transit'
- 'Customer' with exceptions for multihoming
- 'Origin'
- 'Transit'

+++

Since changing the way the regexps behave (the entered regular expression now indicates the normal routing) these can be things (for a myASn user AS123; customers AS1001, AS1002 and AS1003; and transit providers AS10 and AS20)
like:

"Customer Alarm"

\b123 (1001|1002|1003)\b

generates an alarm if any of the three customer ASes appear through an AS other than AS123.

\b(123|999) 1001\b

An multi-homing exception - the alarm is generated if customer AS1001 is seen other than behind AS123 or AS999.

(If there are known to be no further ASes dowstream of the customer ASes then the second "\b" would be replaced by a "$")

"Origin Alarm"

\b123$

Generated an alarm if the configured address range originates from an AS other than AS123.

"Transit Alarm"

\b(10|20) 123\b

Generates an alarm if AS123 is seen other than through the two know transit providers AS10 and AS20.

"Transit of Transit"

Simply add additional ASes to the left of the normal "Transit" pattern.

+++

3. Install current software on Cherry (Alexis),
   Give accounts to internal users for testing (Matthew)

4. Build a WWW I/F that allows the user to easily create/modify/delete the
   real alarm conditions. (Alexis)

5. Implement code that takes the tagged events and generates alarms.

(Alexis)

6. Send email when an alarm occurs. (Alexis)

7. Interface WWW pages to the other RIS tools, similar to the hyperlinks elsewhere on the RIS pages. (Alexis).

8. Migrate existing users

9. Provide non-LIR workaround (?)

When we have this, then have the basic functionality: look at incoming BGP, tag relevant events, aggregate into alarms.

AOB:

- Provide D Knight with account for K-root monitoring
- Later issues: Migrating current users, non-LIRs, Summary email

Next meeting:

25.02.2004 at 200pm (Wed)