LINX 84: SmokeTrace

Network Path Monitoring

https://github.com/jwbensley/Smoketrace
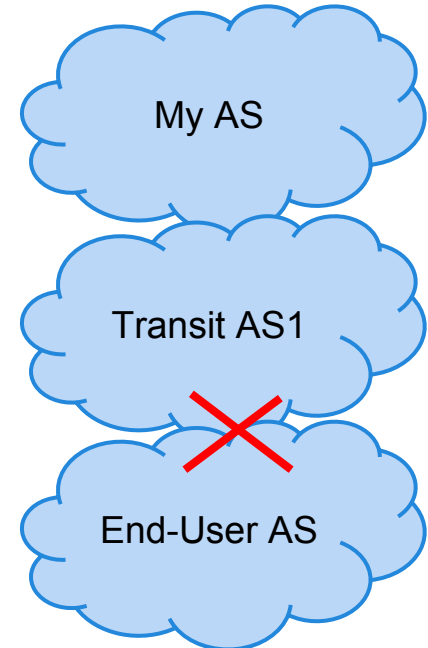
James Bensley,
Vostron Ltd,
jwbensley@gmail.com

VOSTRON

mission critical networks
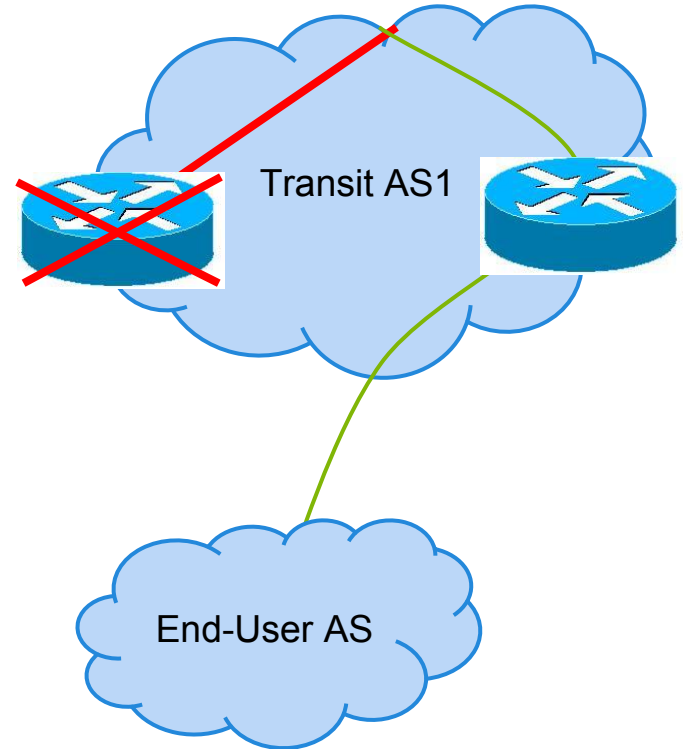
Background To The Problem

- Off-net customer complains to service desk they have very poor or no connectivity to their colo environment

- Customer is connecting over the Internet with at least 1 intermediary AS

Real Life Scenario

Background To The Problem

- A worse scenario occurs when connectivity quality is reduced due to an external AS issue but service is still operational

Transit AS1

End-User AS
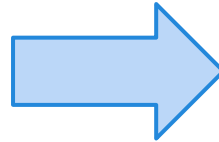
Background To The Problem

- Non-technical customers can find it difficult to understand the issue

- Hard to prove we are not at fault

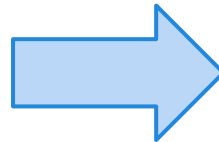- Even harder to get an issue between two ASs resolved which we are not "related" to in any way

My AS

Transit AS1

Transit AS2

Worst case scenarios

End-User AS
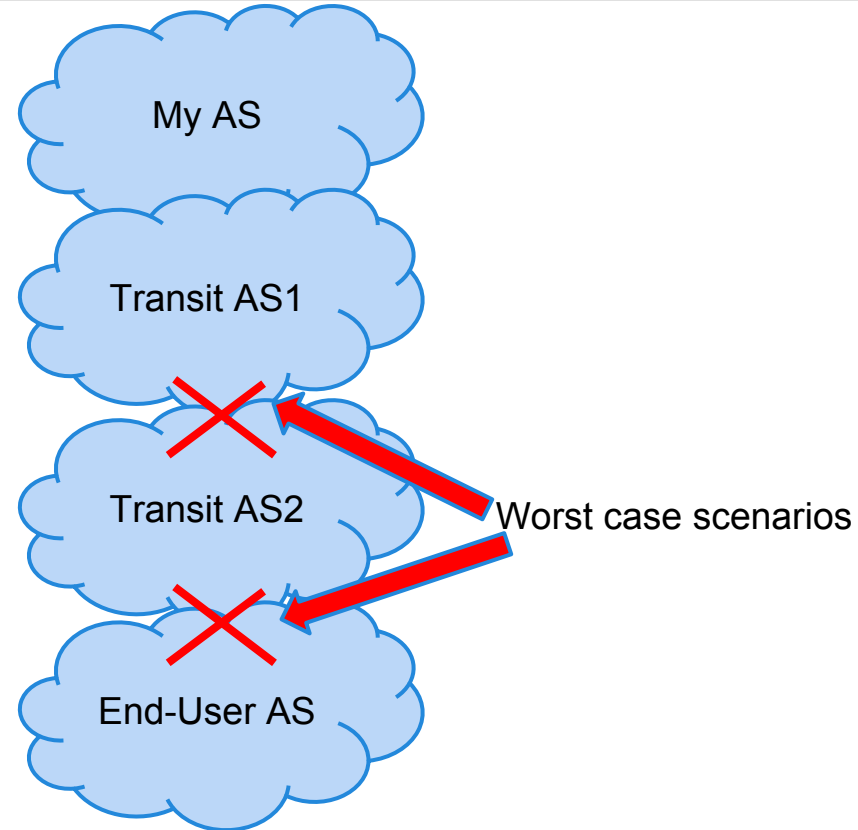
Problem Definition

We can ask the intermediary AS NOC or service desk;

- Is there a problem in your network and if so, what is the ETA for fix? → The email is ignored

- We are seeing an issue (here is some ping and traceroute output) do you see the same? → The email is ignored

Phone calls typically result in "Are you our customer?" or "what is your company name?" - Phone hangs up!

Problem Definition

- We have no direct PoC for random AS service desks or NOCs

- They don't care about our problems

- Our mutual customer might not have the "weight" to incentivise the engineering team (ADSL customers over larger contracts)

Problem Definition

- Wrong end of the reactive vs proactive support scale

- Difficult to monitor external an AS at all, let alone filter out false positives

- I'm not aware of any tool that can currently help with this problem to the level we need

My Solution: SmokeTrace

Collecting route path data and performing continual tests on those paths, then alert based on performance criteria

It's a LAMP stack!

```
                  My traceroute  [v0.80]
bensley-n2 (0.0.0.0)                          Sat Feb  1 20:17:24 2014
Keys:   Help    Display mode    Restart statistics    Order of fi
elds    quit          Packets                   Pings
 Host                     Loss%    Snt    Last    Avg   Best   Wrst StDev
 1. 10.0.58.1             0.0%     39     1.2    2.9    1.1    7.9   2.5
 2. 92.24.208.1           0.0%     39    20.9   21.3   20.4   22.7   0.6
 3. 78.151.230.13         0.0%     39    22.6   35.1   22.0  256.9  38.0
    78.151.230.138
 4. 78.151.230.13         2.6%     39    33.8   34.6   22.2   79.6  17.2
 5. 78.144.0.73           0.0%     39    34.0   37.8   26.1   83.8  17.4
 6. 195.66.226.74         0.0%     38    26.2   27.5   25.9   44.3   3.0
 7. 89.21.224.19          0.0%     38    28.5   28.2   26.0   55.5   4.7
 8. 89.21.235.194         0.0%     38    26.7   27.0   25.6   28.9   1.0
```
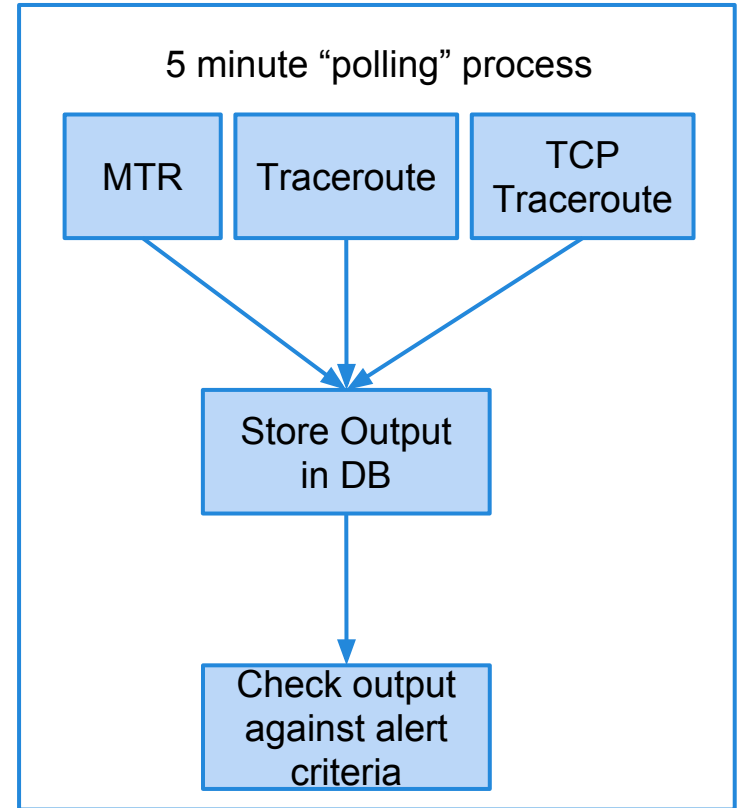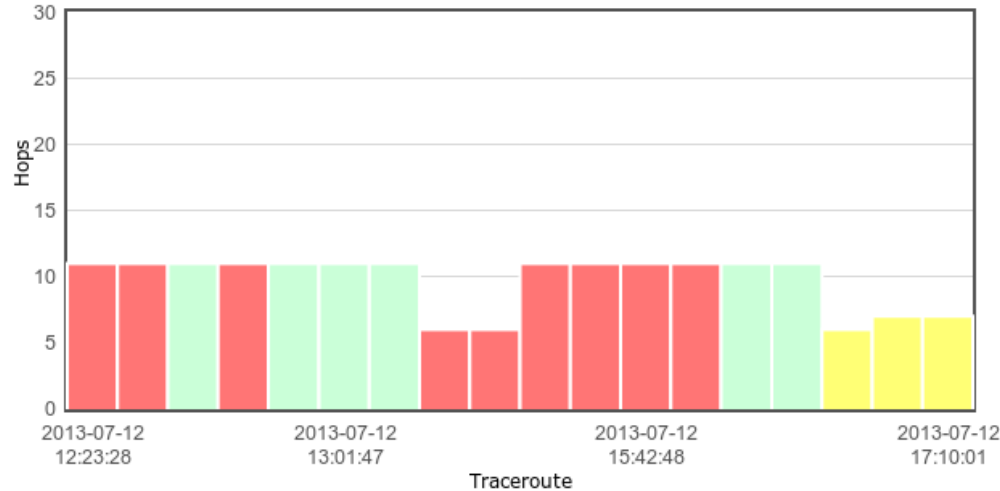
My Solution: SmokeTrace

Initial release is code framework;

- Data input from a variety of binaries

- Alert the variance in number of hops

- Alert the variance of hop IPs (Un/ECMP)

5 minute "polling" process

| MTR | Traceroute | TCP Traceroute |

Store Output in DB

Check output against alert criteria

My Solution: SmokeTrace

- Generate ugly graphs to visualise route changes

- An "overview" page lists destinations with most frequent issues

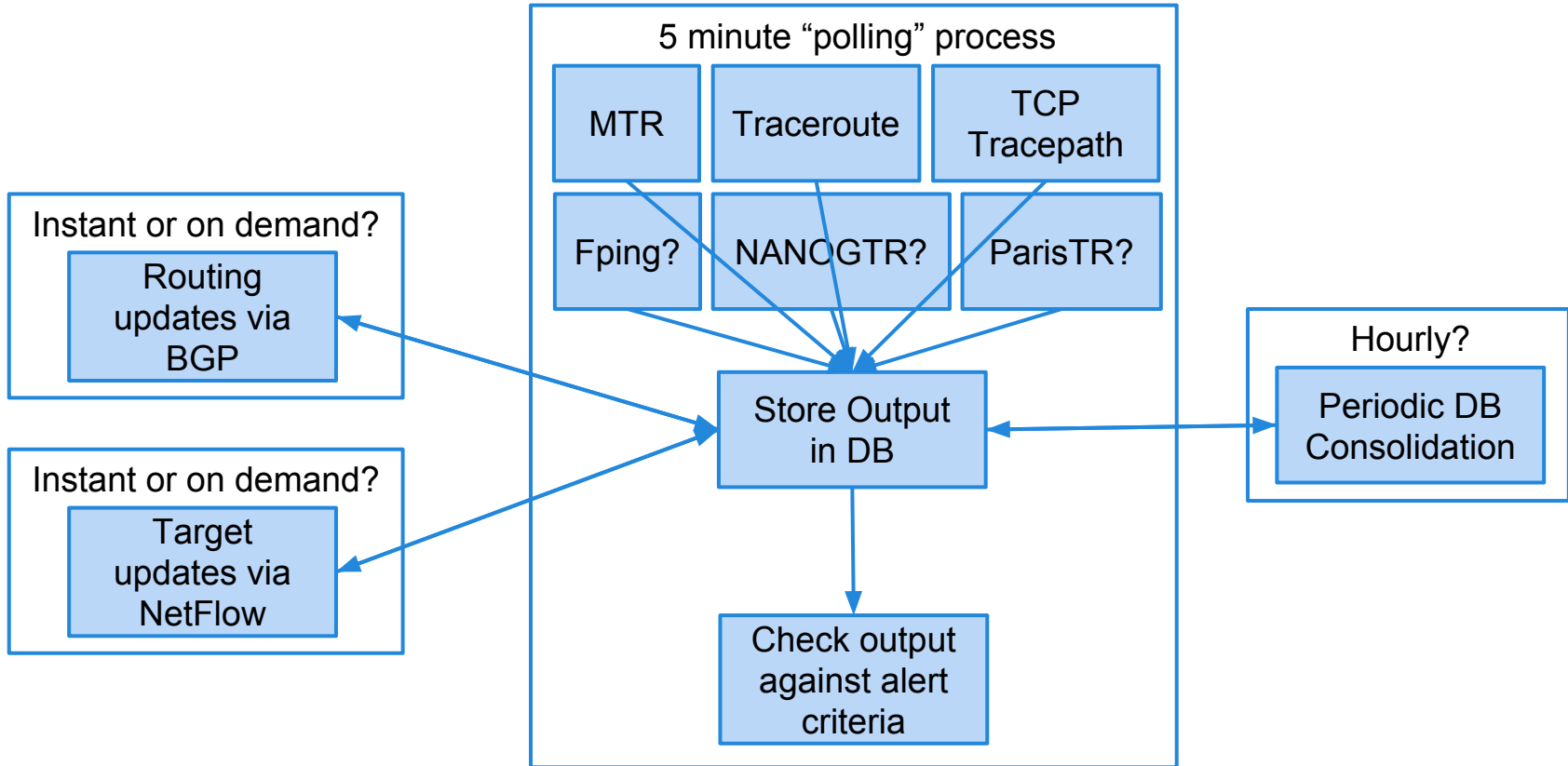- Store data to create route performance history to evaluate routing decisions

My Solution: SmokeTrace

The GUI is ugly but that is a low priority!

I have no interest in porting to another OS!
(minor LINUX hard-codes someone else could easily change)

Future Development

- Routing feed via BGP: Alert on route change? *Reinventing the wheel*

- Binary specific criteria - TCPTraceroute connectivity? Code more modular

- Min/Max/Avg/Delta delay at each hop or along the end-to-end path

- Loss threshold per hop and end-to-end

- Latency thresholds per hop and end-to-end

- Track MTU also with pathtrace or similar?

Q1 Q2 2014 ==
SmokeTrace Beta 0.11

https://github.com/jwbensley/Smoketrace

I'm looking for more networks to test on!

James Bensley,
Vostron Ltd,
jwbensley@gmail.com

VOSTRON
mission critical networks