RIPE Atlas a NLNOG RING

Ondřej Caletka

21. dubna 2015

Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O systému RIPE Atlas

RIPE Atlas

- systém aktivního měření Internetu
- budován od roku 2010
- používá hardwarové sondy hostované u dobrovolníků
- více než 8000 připojených sond (250 v ČR)
- vestavěná a uživatelsky definovatelná měření
- zaměřeno na nejnižší úroveň funkce IP sítí
  - ping
  - traceroute
  - DNS

Sonda RIPE atlas

- speciální hardware použitý s ohledem na nízkou spotřebu a cenu
- napájení z USB, 10/100Mbps připojení do sítě
- žádné ovládací prvky, žádné ovládací rozhraní, žádný otevřený port
- může být zapojena za NAT
- udržuje spojení s řídicími servery u RIPE NCC
- provádí měření a posílá výsledky řídicím serverům

Sondy verze 1 a 2

- založeny na Lantronics Xport Pro
- procesor bez MMU, uClinux
- měřicí software založený na Busyboxu
- výroba zastavena v roce 2012

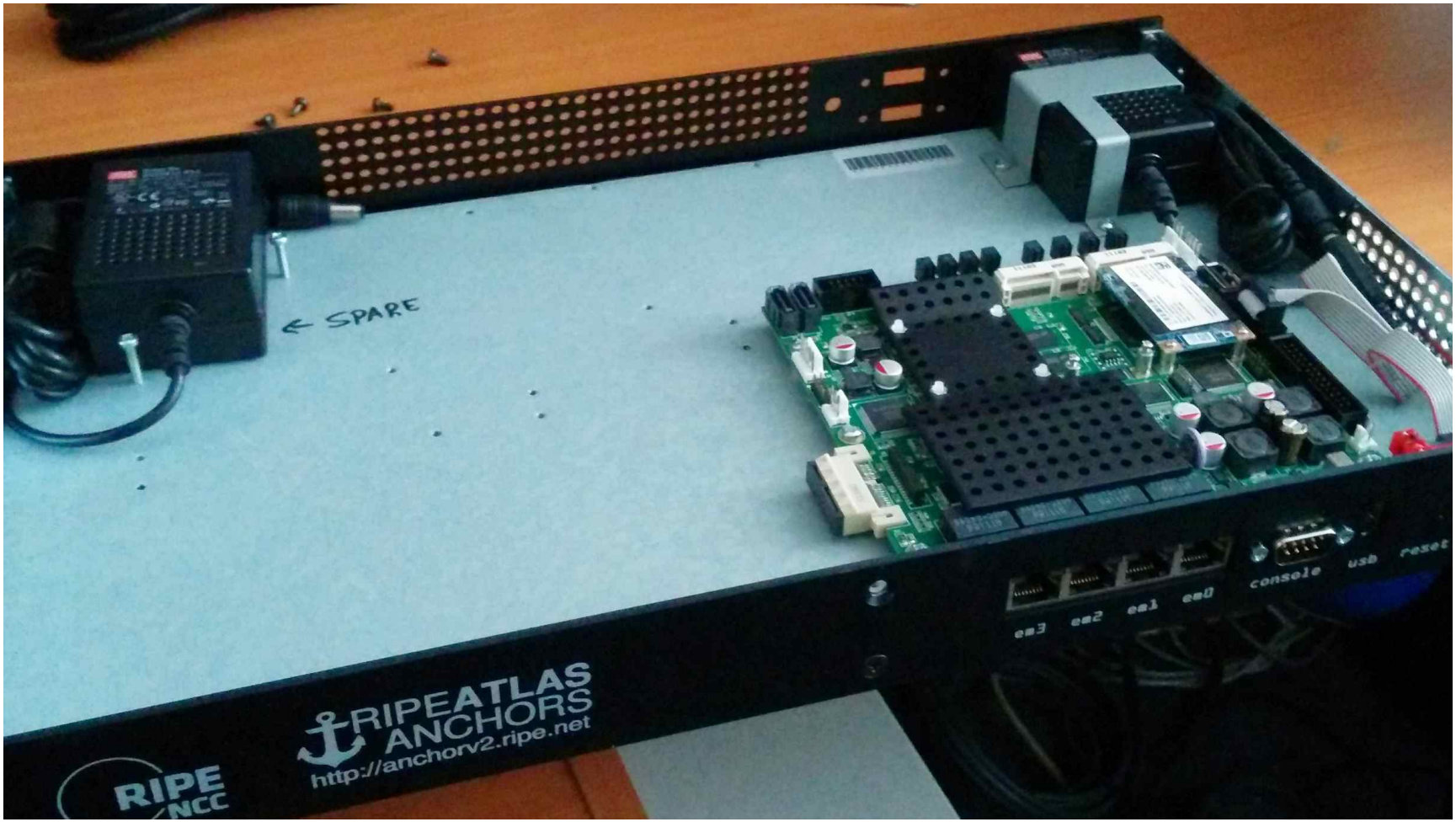
Sondy verze 3

- založeny na TP-Link MR3020
- výkonnější a levnější
- firmware založený na OpenWRT
- USB flash disk pro OS a data
- vestavěná Wi-Fi není SW podporovaná

Sondy Atlas Anchor

- výkonné sondy určené do datových center
- sondu zakupuje hostující organizace za 770 €
- založeno na x86 platformě Soekris Net6501-70
- slouží také jako cíl pro měření malých sond
- 120 sond po světě, 4 v ČR

Uvnitř sondy Atlas Anchor



Služby sondy Atlas Anchor

Autoritativní DNS server

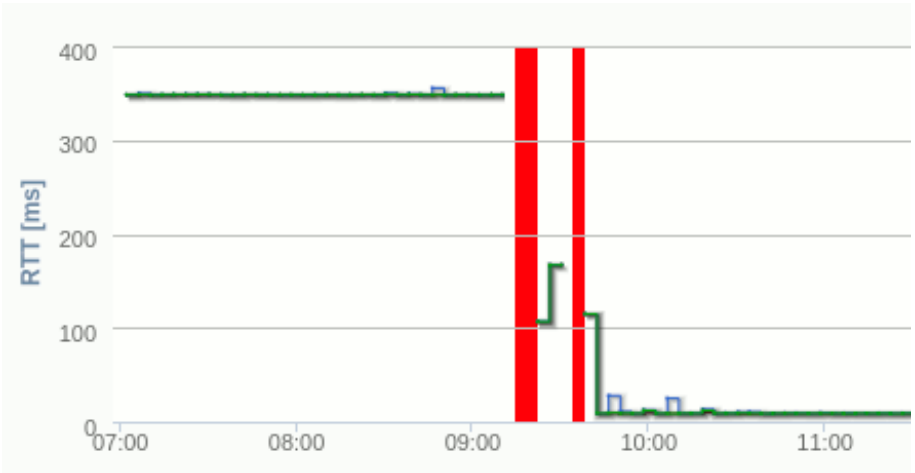
```
$ dig 512.4.dns.cz-prg-as2852.anchors.atlas.ripe.net txt
"XXXXXXXXXXXXXXXXXXXXXXXXXXXX…
…XXXXXXXXXXXXXXXXXXXXXXXXXXXX"
```

HTTP(S) server

```
$ curl http://cz-prg-as2852.anchors.atlas.ripe.net/3
{
      "anchor": "cz-prg-as2852.anchors.atlas.ripe.net",
      "client": "2001:718:1:6::134:196",
      "payload": "AAA"
}
```

Co sondy měří

- Ping vybraných cílů
- Traceroute k vybraným cílům
- DNS dotazy ke kořenovým serverům
- HTTP dotazy na `ripe.net`
- SSL spojení k `ripe.net`
- Uživatelská měření



Uživatelská měření

- možnost spouštět měření na celé síti sond
- platba virtuální měnou
- získání kreditu za hostování sond
- kompletní přístup pomocí JSON REST API
- oficiální knihovna Sagan pro Python

Jak ~~si hrát~~ měřit

- není třeba hostovat sondu (ČR je dostatečně pokryta)
- vytvořte účet RIPE NCC Access `https://access.ripe.net`
- požádejte kamaráda o kredity
- ~~hrajte si~~ měřte

O systému NLNOG RING

NLNOG RING

- síť důvěry mezi síťovými operátory
- reciproční sdílení SSH účtů na linuxových serverech
- centrální správa, jednotné prostředí
- vhodné zejména pro pokročilý debugging Internetu

CESNET

Nody NLNOG RINGu

- (virtuální) server s 64-bit Ubuntu 12.04 LTS
- 1 IPv4, 1 IPv6 adresa
- hostující organizace má vlastní ASN v default-free zone
- centrální management (upgrady, záplaty) pomocí Puppet
- každý člen má uživatelský přístup na všechny nody, sudo přístup na svoje nody
- logování TTY příkazů, nulová tolerance ke zneužití

Jak použít RING

- žádná hesla, používá se SSH klíč
- doporučuje se samostatný klíč

Konfigurace OpenSSH .ssh/config

```
Host *.ring.nlnog.net
User cesnet
IdentityFile ~/.ssh/nlnogring
UserKnownHostsFile ~/.ssh/known_hosts_ring
```

Synchronizace otisků nodů

```
$ scp cesnet01.ring.nlnog.net:\
> /etc/ssh/ssh_known_hosts \
> ~/.ssh/known_hosts_ring
```

ring-ssh

- eliminace rizika s forwardováním SSH agenta
- spustí samostatného agenta a nahraje do něj samostatný SSH klíč pro RING
- následně spustí SSH s tímto agentem
- k dispozici na `https://github.com/NLNOG/nlnog-ring/blob/master/scripts/ring-ssh`

Hromadné nástroje

`ring-all` spuštění příkazu na všech nodech

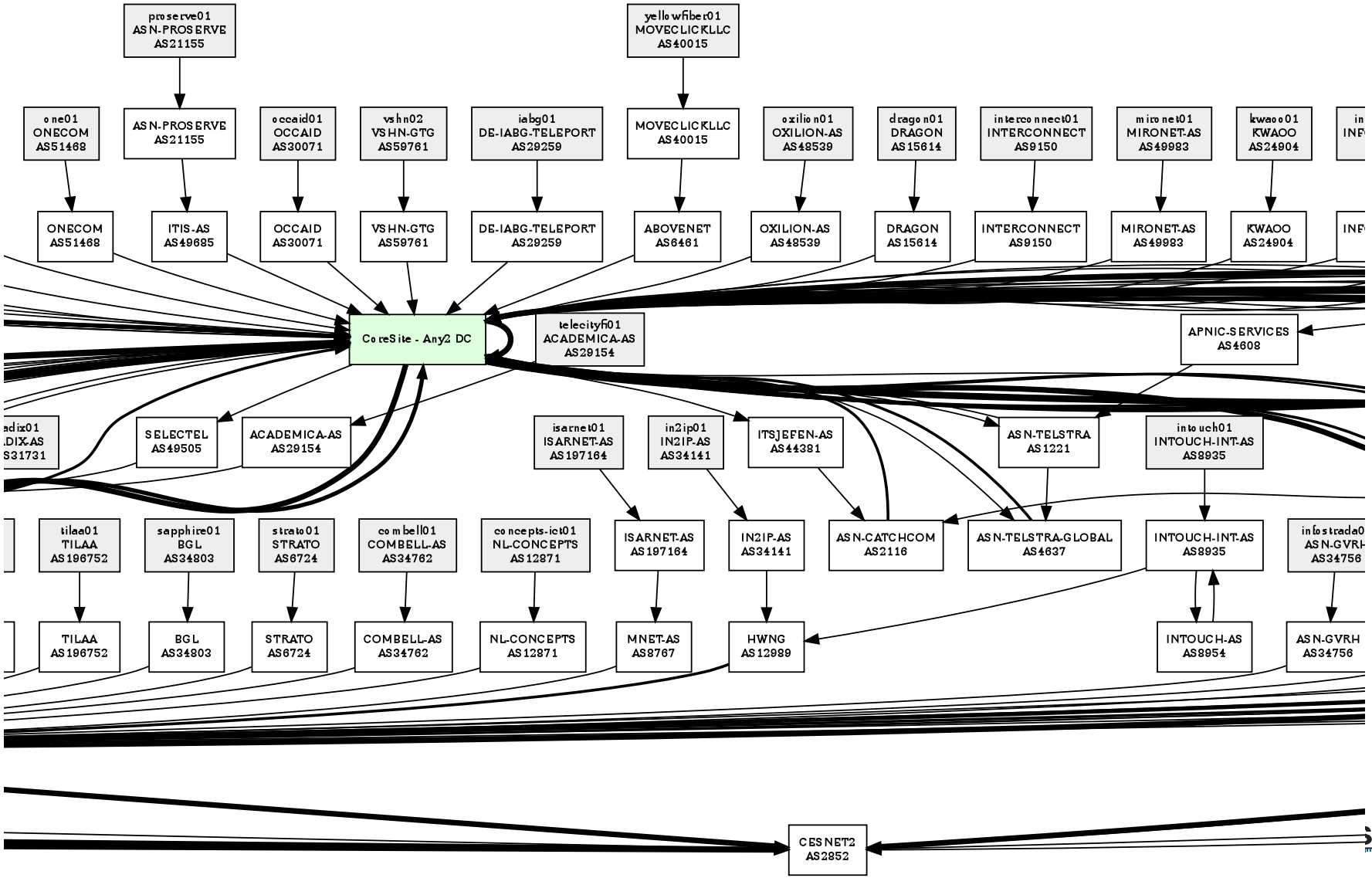
`ring-ping` ping ze všech nodů, agregovaný výsledek

`ring-trace` traceroute ze všech nodů, koncetrovaný do grafu (ideální pro tapety ☺)

Příklad ring-ping

```
cesnet@cesnet01:~$ ring-ping -6 nebezi.cz
45 servers: 67ms average
unreachable via: networkoperations01
ssh connection failed: backbone02 cybercom01
 mknetzdienste01 nonattached01
```

ring-trace


proserve01
ASN-PROSERVE
AS21155
yellowfiber01
MOVECLICKLLC
AS40015
one01
ONECOM
AS51468
ASN-PROSERVE
AS21155
occaid01
OCCAID
AS30071
vshn02
VSHN-GTG
AS59761
iabg01
DE-IABG-TELEPORT
AS29259
MOVECLICKLLC
AS40015
oxilion01
OXILION-AS
AS48539
dragon01
DRAGON
AS15614
interconnect01
INTERCONNECT
AS9150
mironet01
MIRONET-AS
AS49983
kwaoo01
KWAOO
AS24904
ONECOM
AS51468
ITIS-AS
AS49685
OCCAID
AS30071
VSHN-GTG
AS59761
DE-IABG-TELEPORT
AS29259
ABOVENET
AS6461
OXILION-AS
AS48539
DRAGON
AS15614
INTERCONNECT
AS9150
MIRONET-AS
AS49983
KWAOO
AS24904
CoreSite - Any2 DC
telecityfi01
ACADEMICA-AS
AS29154
APNIC-SERVICES
AS4608
SELECTEL
AS49505
ACADEMICA-AS
AS29154
isarnet01
ISARNET-AS
AS197164
in2ip01
IN2IP-AS
AS34141
ITSJEFEN-AS
AS44381
ASN-TELSTRA
AS1221
intouch01
INTOUCH-INT-AS
AS8935
tilaa01
TILAA
AS196752
sapphire01
BGL
AS34803
strato01
STRATO
AS6724
combell01
COMBELL-AS
AS34762
concepts-ict01
NL-CONCEPTS
AS12871
ISARNET-AS
AS197164
IN2IP-AS
AS34141
ASN-CATCHCOM
AS2116
ASN-TELSTRA-GLOBAL
AS4637
INTOUCH-INT-AS
AS8935
TILAA
AS196752
BGL
AS34803
STRATO
AS6724
COMBELL-AS
AS34762
NL-CONCEPTS
AS12871
MNET-AS
AS8767
HWNG
AS12989
INTOUCH-AS
AS8954
ASN-GVRH
AS34756
CESNET2
AS2852

RING SQA

- dohledový systém postavený nad RINGem
- nody se každých 30 sekund pingají UDP zprávami
- při nárůstu rozbitosti je vygenerována notifikace
- traceroute na čerstvě rozbité nody usnadňuje hledání občasných chyb
- systém s minimem false positives

```
Subject: cesnet01.ring.nlnog.net: raising ipv6 alarm - 11 new nodes down
List-Id: ring-sqa <sqa.ring.nlnog.net>
X-Mailer: ring-sqa
Regarding: cesnet01.ring.nlnog.net ipv6
Message-Id: <20141206063543.E57FAE0BD8@cesnet01.ring.nlnog.net>
Date: Sat,  6 Dec 2014 06:35:43 +0000 (UTC)

This is an automated alert from the distributed partial outage
monitoring system 'RING SQA'.

At 2014-12-06 06:35:43 UTC the following measurements were analysed
as indicating that there is a high probability your NLNOG RING node
cannot reach the entire internet. Possible causes could be an outage
in your upstream's or peer's network.

The following 11 nodes previously were reachable, but became unreachable
over the course of the last 3 minutes:

- hostway01.ring.nlnog.net                                2606:6a00::a:c  AS14280   CA
- lchost01.ring.nlnog.net                               2a01:70:1:217:2::125  AS25098   GB
- sixdegrees01.ring.nlnog.net                         2a02:298:81:1337::b33f  AS6908    GB
- viatel01.ring.nlnog.net                  2a01:258:8:6:20c:29ff:fe95:1965  AS31122   IE
- iij01.ring.nlnog.net                       2001:240:10c:5:0:69:696a:3031  AS2497    JP
- nautile01.ring.nlnog.net                2404:e400:998:0:216:3eff:fe7e:a08f  AS45345   NC
- softlayer05.ring.nlnog.net                          2607:f0d0:2002:6e::2  AS36351   US
- direcpath01.ring.nlnog.net       2607:f1e8:f0f0:b:528a:1948:db90:ec59  AS31939   US
- flhsi01.ring.nlnog.net                            2606:2400:223:4::6  AS36295   US
- softlayer01.ring.nlnog.net                          2607:f0d0:1004:d3::2  AS36351   US
- inerail01.ring.nlnog.net                             2604:5980:1001:d::4  AS33031   US
```

As a debug starting point 3 traceroutes were launched right after
detecting the event, they might assist in pinpointing what broke:

```
softlayer01.ring.nlnog.net          AS36351  (US)
mtr -i0.5 -c5 -r -w -n 2607:f0d0:1004:d3::2
  1.|-- 2001:718:1:1f::1           0.0%     6    1.1   1.7   0.8   5.6   1.9
  2.|-- 2001:798:1b:10aa::19       0.0%     5    7.1   8.0   7.1   9.0   0.9
  3.|-- 2001:798:cc:3301:1b01::5   0.0%     5    7.0   7.1   7.0   7.2   0.1
  4.|-- 2001:798:cc:1001:3301::1   0.0%     5    8.3   8.3   8.3   8.4   0.0
  5.|-- 2001:7f8:30:0:2:1:0:6939   0.0%     5   14.3  11.0   8.6  14.3   2.6
  6.|-- 2001:470:0:284::2          0.0%     5    8.7  12.3   8.7  19.1   4.3
  7.|-- 2001:7f8:14::84:1          0.0%     5   16.0  16.0  15.9  16.4   0.2
  8.|-- 2607:f0d0:2:2::d0          0.0%     5   21.4  21.6  21.4  21.9   0.2
  9.|-- 2607:f0d0:2:2::ce         20.0%     5  220.5 225.7 220.5 231.9   4.8
 10.|-- 2607:f0d0:2:2::42         20.0%     5  210.0 222.1 210.0 230.5   8.8
 11.|-- 2607:f0d0:2:2::19         60.0%     5  222.8 228.5 222.8 234.1   8.0
 12.|-- 2607:f0d0:2:2::6          60.0%     5  250.5 255.4 250.5 260.4   7.0
 13.|-- 2607:f0d0:2:2::51         40.0%     5  251.6 255.4 251.6 257.5   3.3
 14.|-- 2607:f0d0:1000:1::82      60.0%     5  258.6 258.9 258.6 259.1   0.3
 15.|-- 2607:f0d0:1004:d3::2      80.0%     5  257.1 257.1 257.1 257.1   0.0

lchost01.ring.nlnog.net             AS25098  (GB)
mtr -i0.5 -c5 -r -w -n 2a01:70:1:217:2::125
  1.|-- 2001:718:1:1f::1           0.0%     6    1.3   1.1   1.0   1.3   0.1
  2.|-- 2001:798:13:10aa::1        0.0%     5    0.3   0.4   0.3   0.4   0.0
  3.|-- 2001:798:cc:1301:1401::6   0.0%     5    6.8   6.9   6.8   6.9   0.0
  4.|-- 2001:978:2:7::5:1          0.0%     5    7.3   7.4   7.3   7.6   0.1
  5.|-- 2001:550:0:1000::8275:3072 0.0%     5    7.6   7.7   7.5   7.8   0.1
  6.|-- 2001:550:0:1000::9a36:2521 0.0%     5   14.3  14.3  14.3  14.3   0.0
  7.|-- 2001:550:0:1000::9a36:276e 0.0%     5   21.9  21.8  21.7  22.0   0.1
  8.|-- 2001:550:0:1000::9a36:2781 40.0%    5   22.0  22.0  22.0  22.0   0.0
  9.|-- 2001:550:0:1000::8275:315a 60.0%    5   22.2  22.1  22.1  22.2   0.1
 10.|-- 2001:550:0:1000::9a36:3c96 0.0%     5   21.5  21.5  21.5  21.5   0.0
 11.|-- 2001:978:2:22::17:2        0.0%     5   22.4 131.1  22.4 210.2  82.7
 12.|-- 2a01:70:1:103::1           0.0%     5  135.2 141.5 135.2 146.8   4.7
 13.|-- 2a01:70:1:217:2::125      40.0%     5  138.9 141.1 138.9 142.9   2.0
```

```
An alarm is raised under the following conditions: every 30 seconds
your node pings all other nodes. The amount of nodes that cannot be
reached is stored in a circular buffer, with each element representing
a minute of measurements. In the event that the last three minutes are
1.2 above the median of the previous 27 measurement slots, a partial
outage is assumed. The ring buffer's output is as following:

29 min ago  64 measurements failed (baseline)
28 min ago  64 measurements failed (baseline)
27 min ago  64 measurements failed (baseline)
26 min ago  63 measurements failed (baseline)
…
15 min ago  63 measurements failed (baseline)
14 min ago  63 measurements failed (baseline)
13 min ago  64 measurements failed (baseline)
12 min ago  64 measurements failed (baseline)
11 min ago  63 measurements failed (baseline)
10 min ago  64 measurements failed (baseline)
 9 min ago  63 measurements failed (baseline)
 8 min ago  64 measurements failed (baseline)
 7 min ago  63 measurements failed (baseline)
 6 min ago  64 measurements failed (baseline)
 5 min ago  63 measurements failed (baseline)
 4 min ago  64 measurements failed (baseline)
 3 min ago  63 measurements failed (baseline)
 2 min ago 104 measurements failed (raised alarm)
 1 min ago  78 measurements failed (raised alarm)
 0 min ago  79 measurements failed (raised alarm)

Kind regards,

NLNOG RING
```

Závěr

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
http://Ondřej.Caletka.cz