Rethinking Network Troubleshooting: Smarter Tools and Better Visibility at Nexthop

DAVID BROWN
Co-Founder /
Director of Unscheduled Maintenance

AusNOG 2025

ROUTE-VIEWS.OPTUS.NET.AU

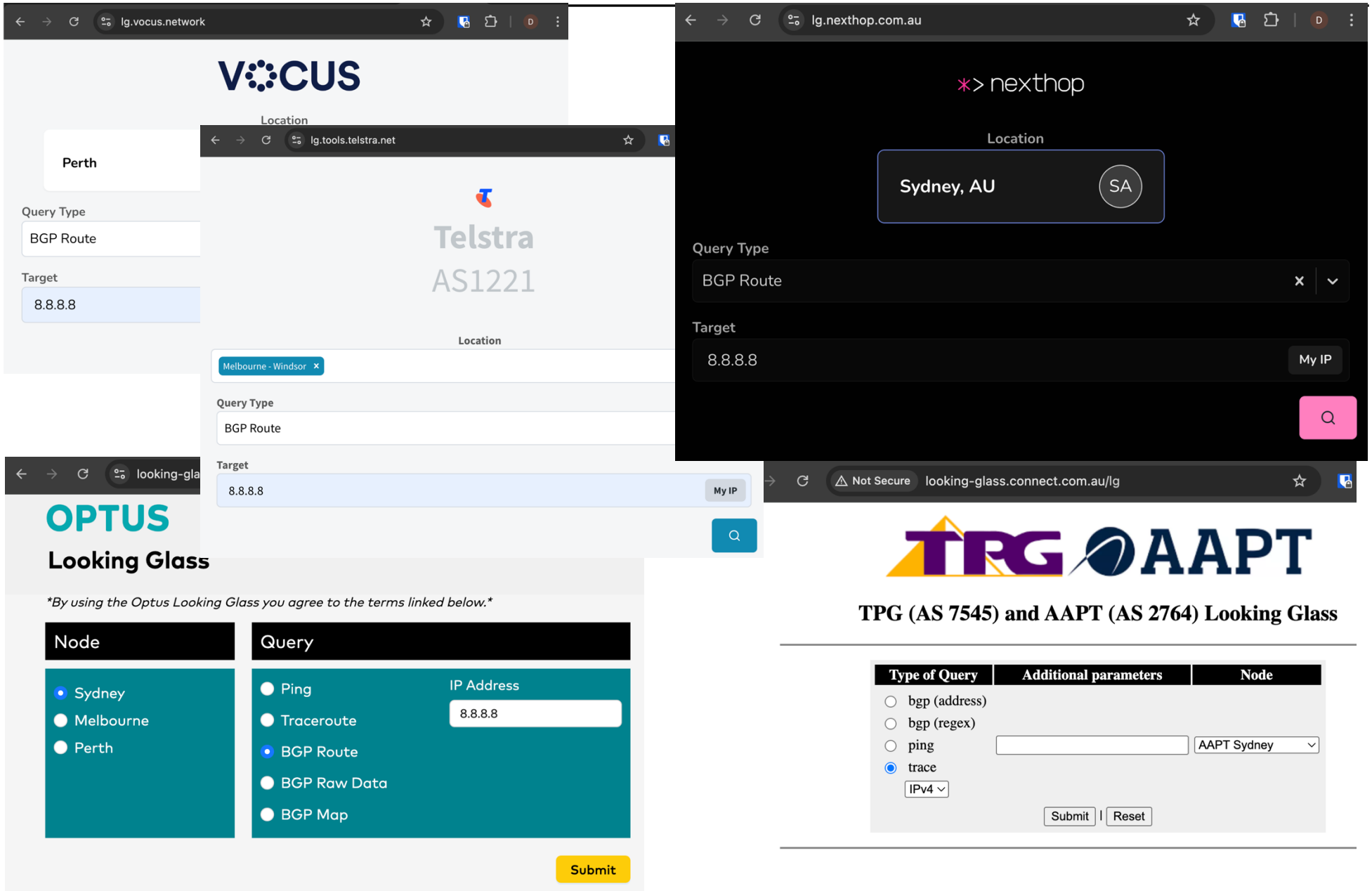
[AusNOG] Optus LG

Nathan Brookfield Nathan.Brookfield at simtronic.com.au
Mon Mar 7 20:25:34 EST 2016

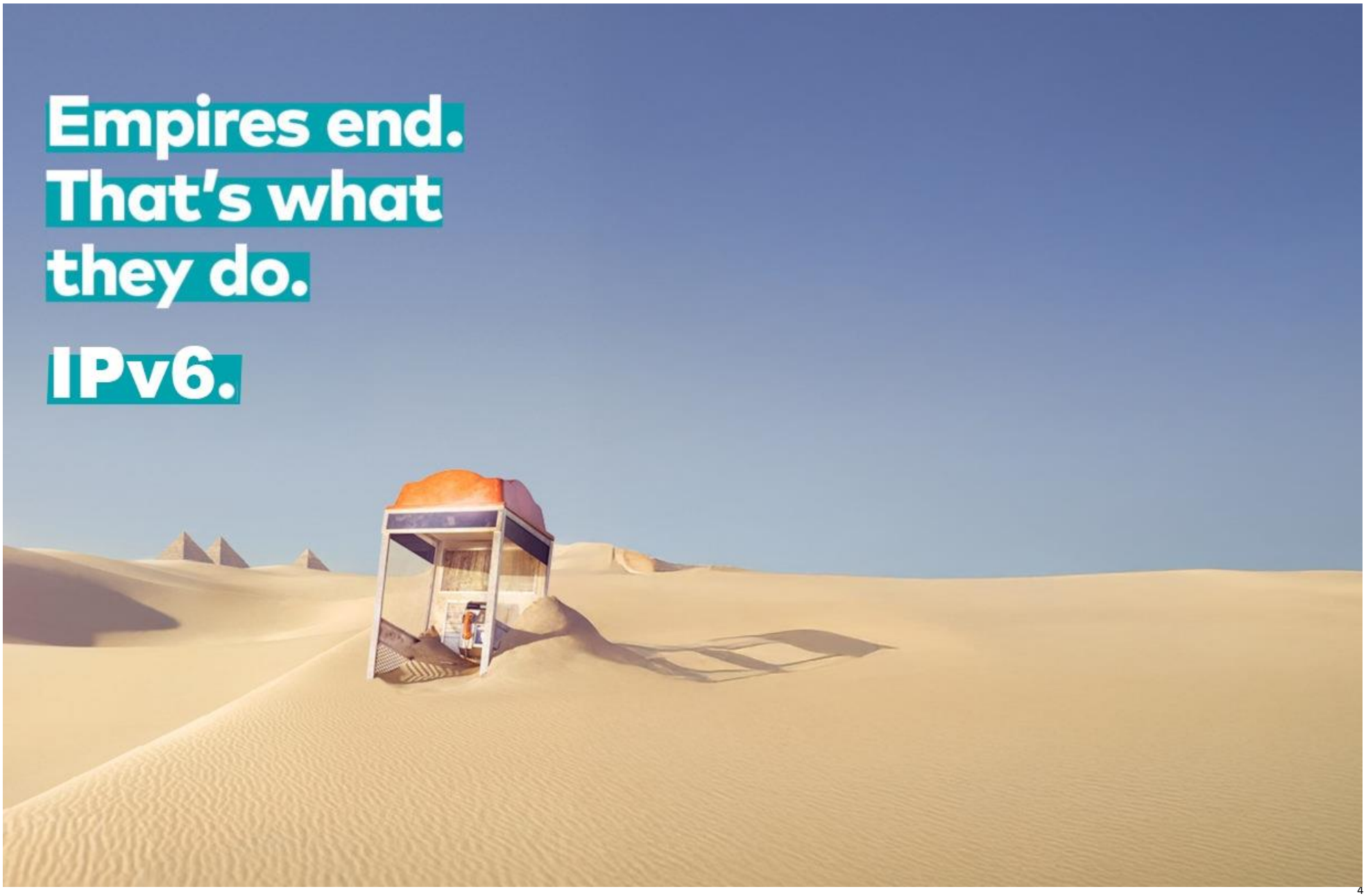
- Previous message: [AusNOG] Optus LG
- Next message: [AusNOG] Optus LG
- **Messages sorted by:** [date] [thread] [subject] [author]

```
nathan at bdr01:~$ telnet route-views.optus.net.au

Entering character mode
Escape character is '^]'.

##########################################################################
                        Optus BGP Route Viewer
       203.202.125.6   route-views.optus.net.au , Sydney , Australia

 This router has the complete view of Optus AS7474 routes.

 This router should _not_ be used to verify Optus backbone routing policy.
 The best path shown is the current best path *from this router*.

 Please contact noc at optus.net.au if you have questions or comments about
 this service, its use, or if you might be able to contribute your view.

 The Optus route-views server is NOT to be used with ANY automated scripts
 unless expressly authorised by Optus.


##########################################################################

route-views.optus.net.au>
```

WEB BASED LOOKING GLASS



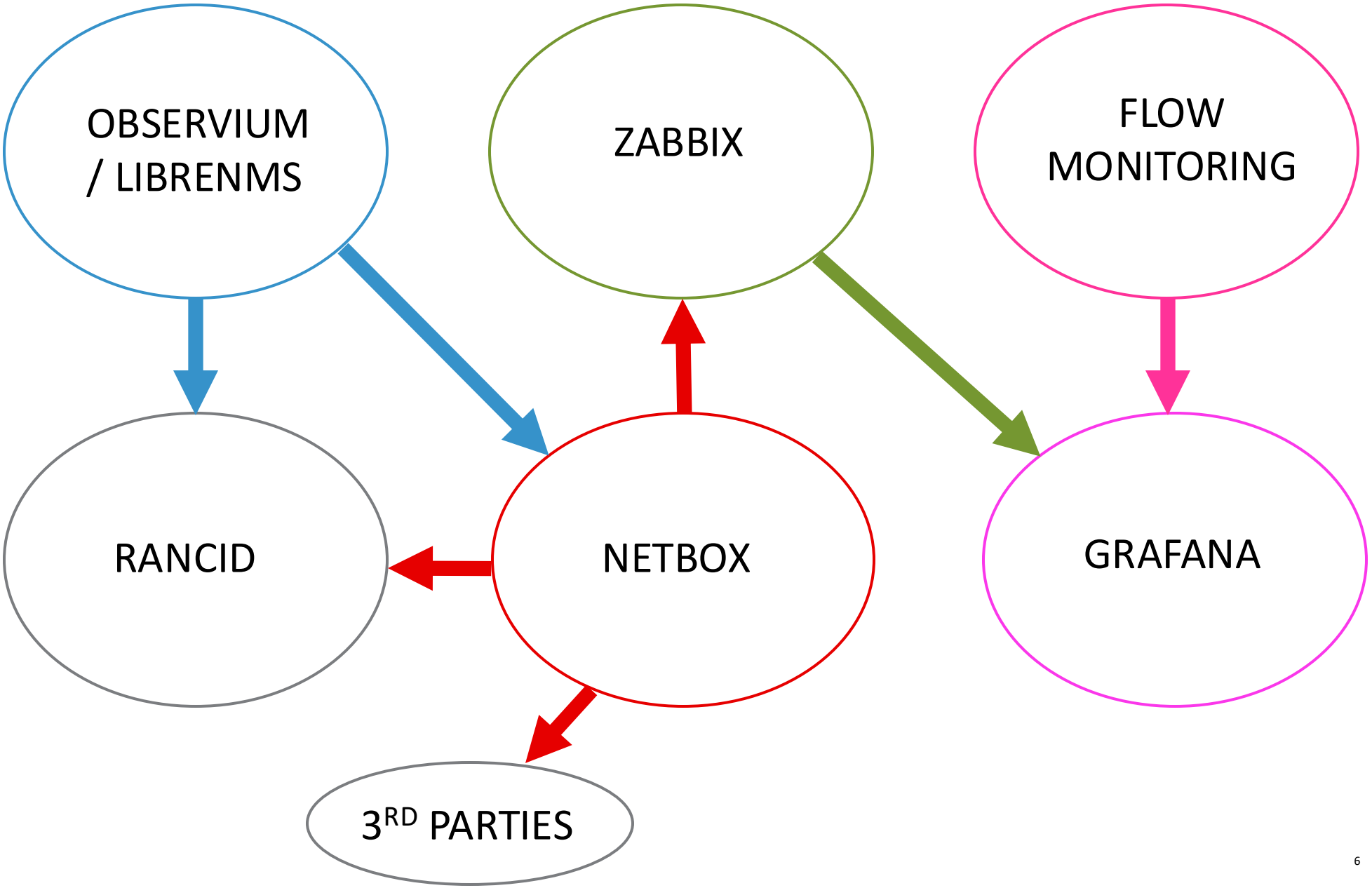
IPV6?



MONITORING SYSTEMS

nexthop

MONITORING SYSTEMS



BEFORE NETBOX

NETBOX SCRIPTS

CUSTOMIZATION / SCRIPTS

Central script runner - previous runs, date/time/user/success

Sync Device from Observium

IP Address Assignment / LOA Generation

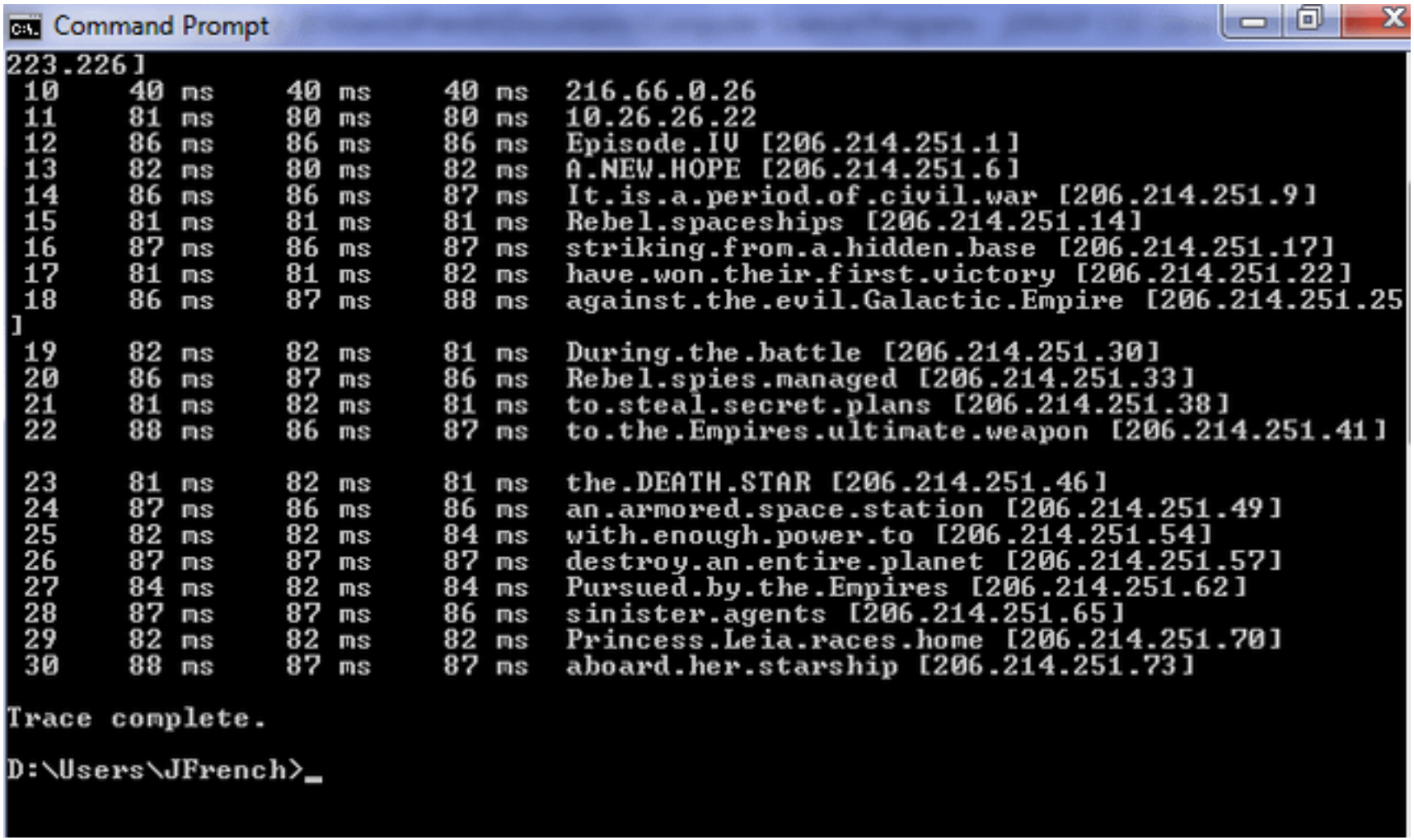
Audit Netbox rear ports with Inventory Report

TYPICAL FAULT PROCESS

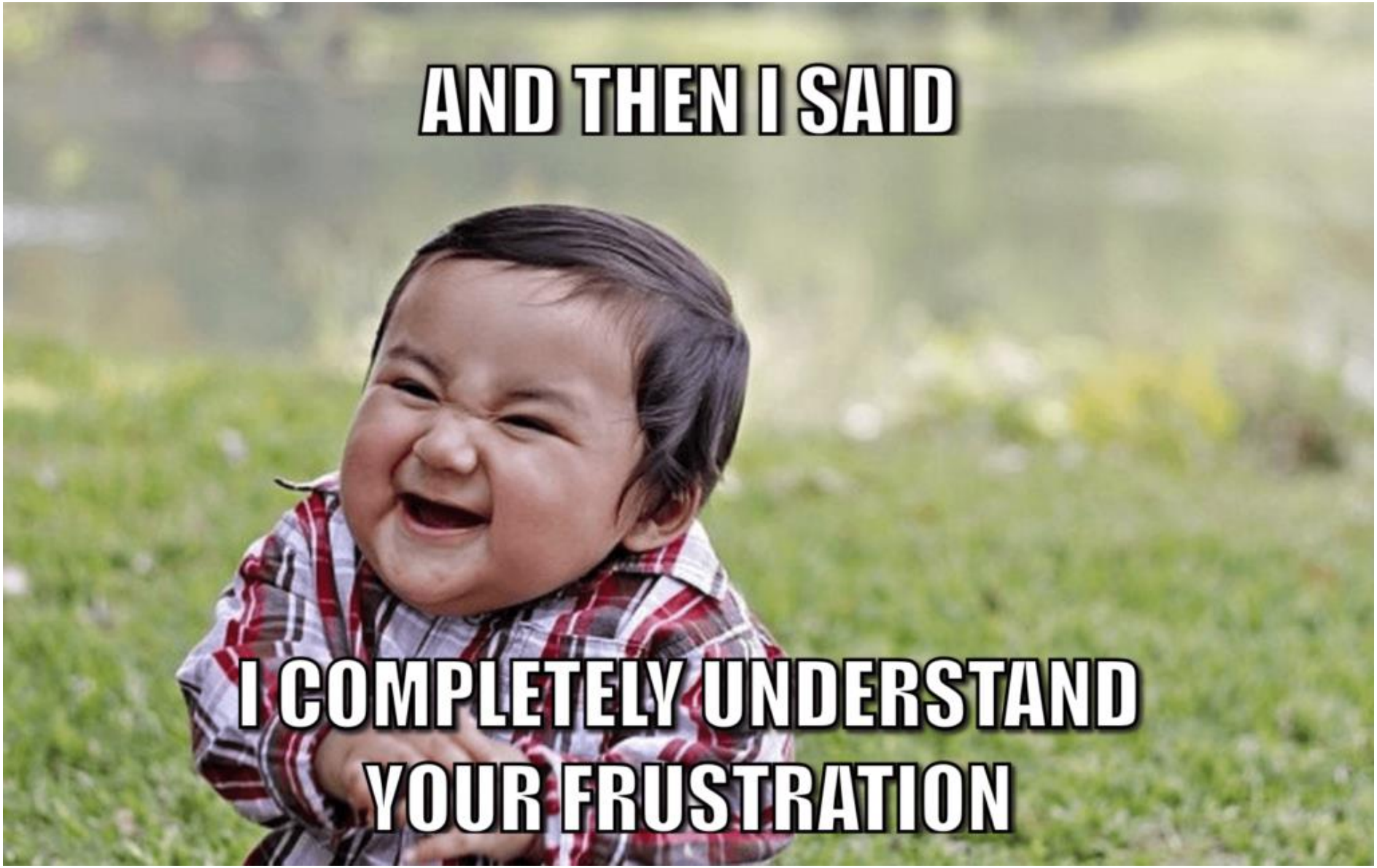
*> nexthop

P1 FAULT LOGGED

SCREENSHOTS



ACKNOWLEDGE FAULT



ROUTER TROUBLESHOOTING

rtr01.syd27[RACK123/EQUINIX SY99]> show ip bgp 203.0.113.0/24

BGP routing table information for VRF default
Router identifier 203.0.113.0, local AS number 9507
BGP routing table entry for 203.0.113.0/24
Paths: 2 available
65000
203.0.113.1 from 203.0.113.1 (203.0.113.1)
Origin IGP, metric 0, localpref 1337, IGP metric 20, weight 0, tag 0
Received 1337d00h ago, valid, external, best
Community: 65000:1234
Rx SAFI: Unicast
Tunnel RIB eligible

conf t
prompt **<prompt goes here>**

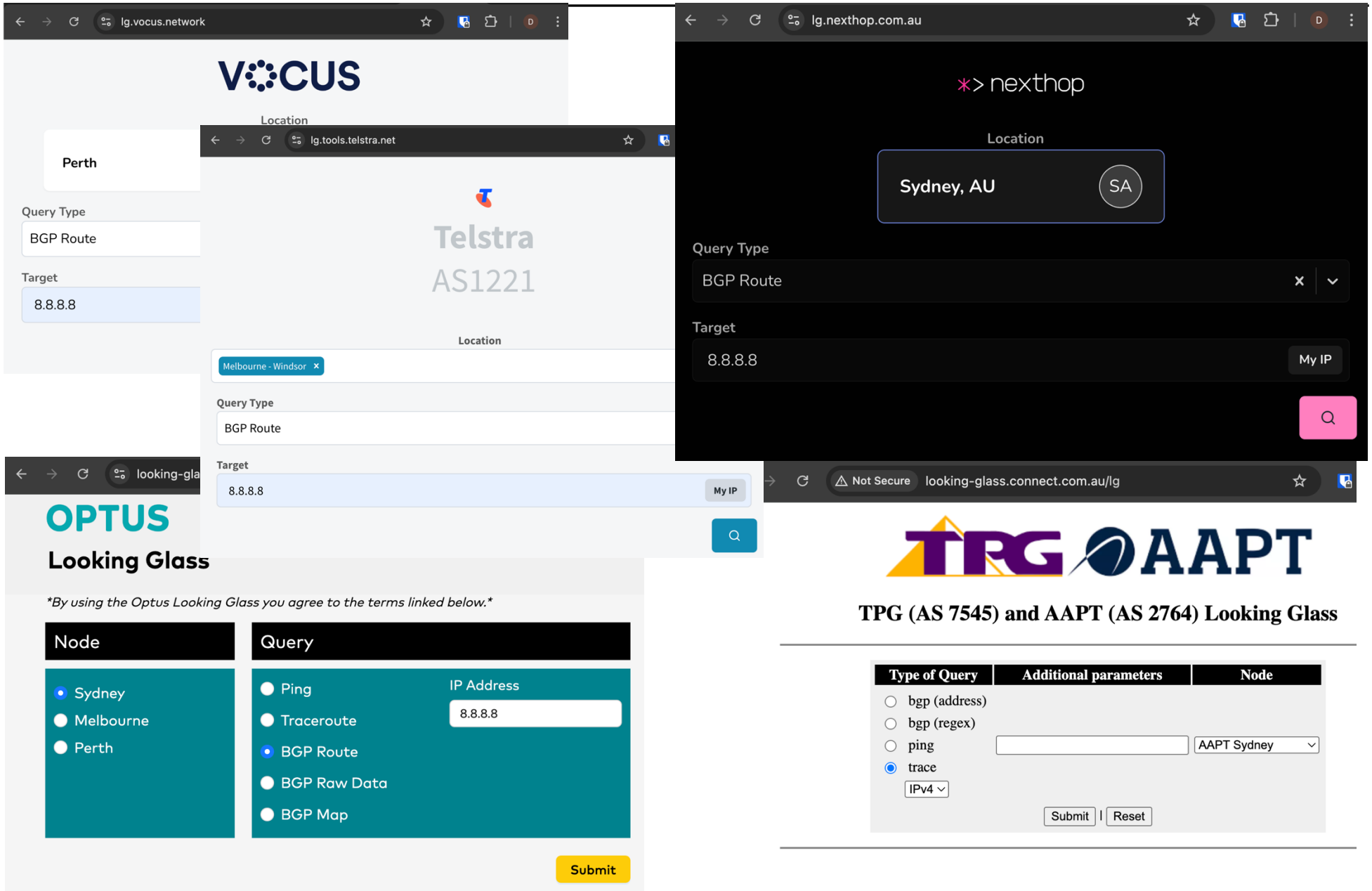
ping 203.0.113.1 repeat 100000 source lo0

traceroute 203.0.113.1 source lo0

show interfaces Eth30/1

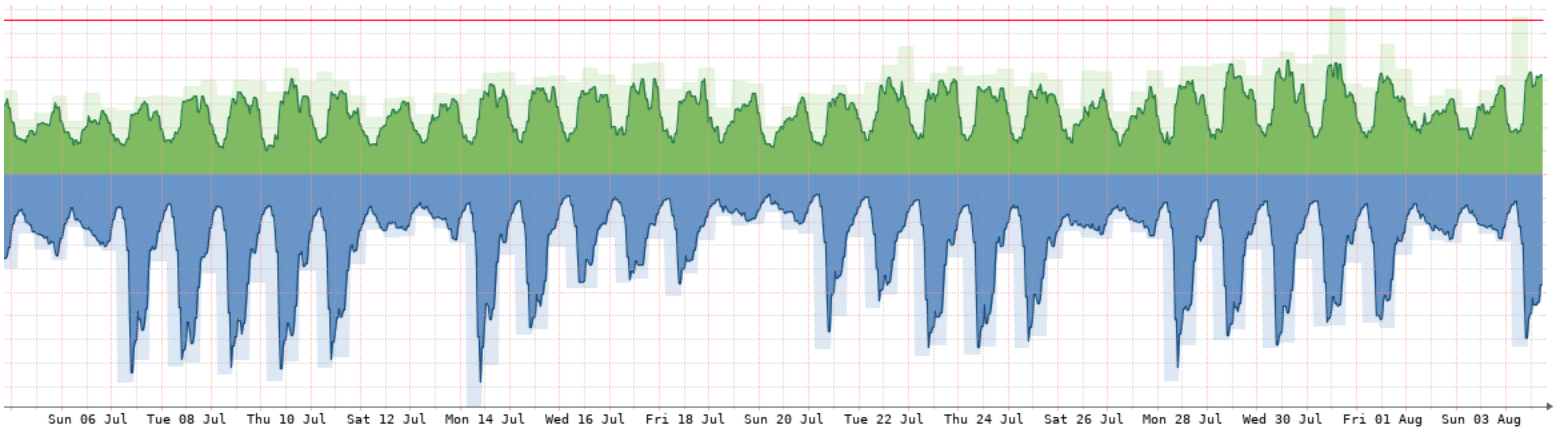
show interfaces Eth30/1 transceiver

REMEMBER US ?


lg.vocus.network
VOCUS
Location
Perth
Query Type
BGP Route
Target
8.8.8.8
lg.tools.telstra.net
Telstra
AS1221
Location
Melbourne - Windsor
Query Type
BGP Route
Target
8.8.8.8
My IP
lg.nexthop.com.au
nexthop
Location
Sydney, AU
SA
Query Type
BGP Route
Target
8.8.8.8
My IP
looking-gla
OPTUS
Looking Glass
By using the Optus Looking Glass you agree to the terms linked below.
Node
Sydney
Melbourne
Perth
Query
Ping
Traceroute
BGP Route
BGP Raw Data
BGP Map
IP Address
8.8.8.8
Submit
Not Secure
looking-glass.connect.com.au/lg
TPG AAPT
TPG (AS 7545) and AAPT (AS 2764) Looking Glass
Type of Query
Additional parameters
Node
bgp (address)
bgp (regex)
ping
trace
AAPT Sydney
IPv4
Submit
Reset

EVERYTHING LOOKS OK

Traffic looks normal

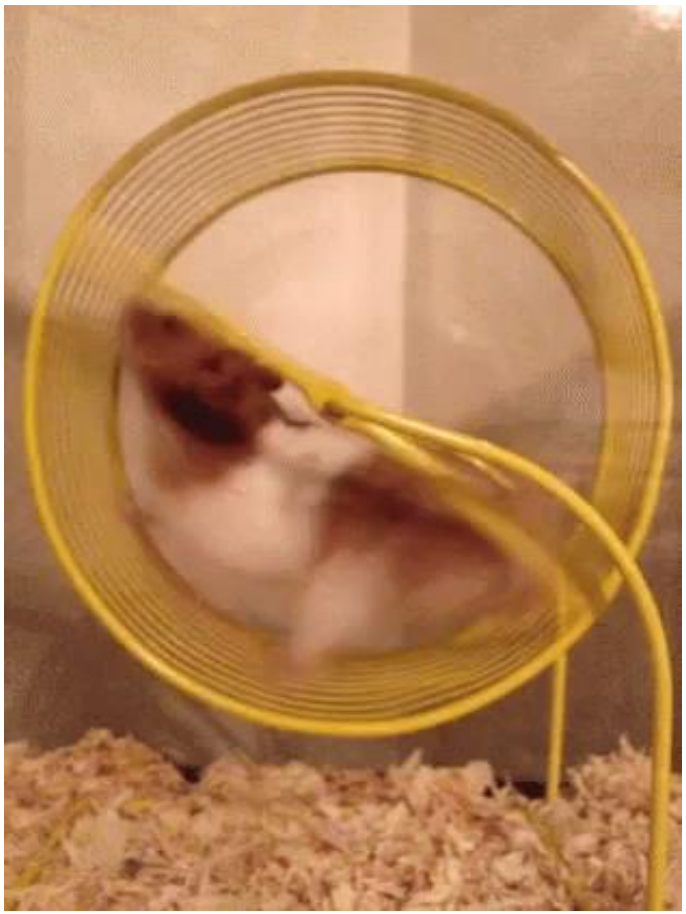


No other complaints

REPLY TO CUSTOMER

CAN FINALLY REPRODUCE

Customer persistence



Packet loss confirmed

```
Router# ping 203.0.113.1 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 203.0.113.1, timeout
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!..!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!..!!!!!!!!!!..!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!..!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!..!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!..!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Success rate is 94 percent (943/1000), round-trip min/avg/
```

PORTALS TO ANOTHER DIMENSION

Fault Details

* Fault Symptom

Full Fault Description

Number of users Impacted

* Date/Time Fault First Noticed

DD/MM/YYYY HH:mm:ss

What is the business critical impact

Evidence to be provided (CRC errors, Qos details etc.)

Does this circuit provide "Special Services"

-- None --

Do you have a secondary/backup service for this link ?

-- None --

Troubleshooting

Is the NTU Powered up?

-- None --

* Has the NTU been rebooted /power cycled

-- None --

* Has the customer site cabling been checked

-- None --

* Is the fault continuous or intermittent? Does it only occur during peak hours?

* Non-working site IP details Source & Destination

* Forward trace routes for working and non-working setup (Essential to investigate end – end network path)

What is the NTU LED status?

-- None --

* Has the CPE been rebooted /power cycled

-- None --

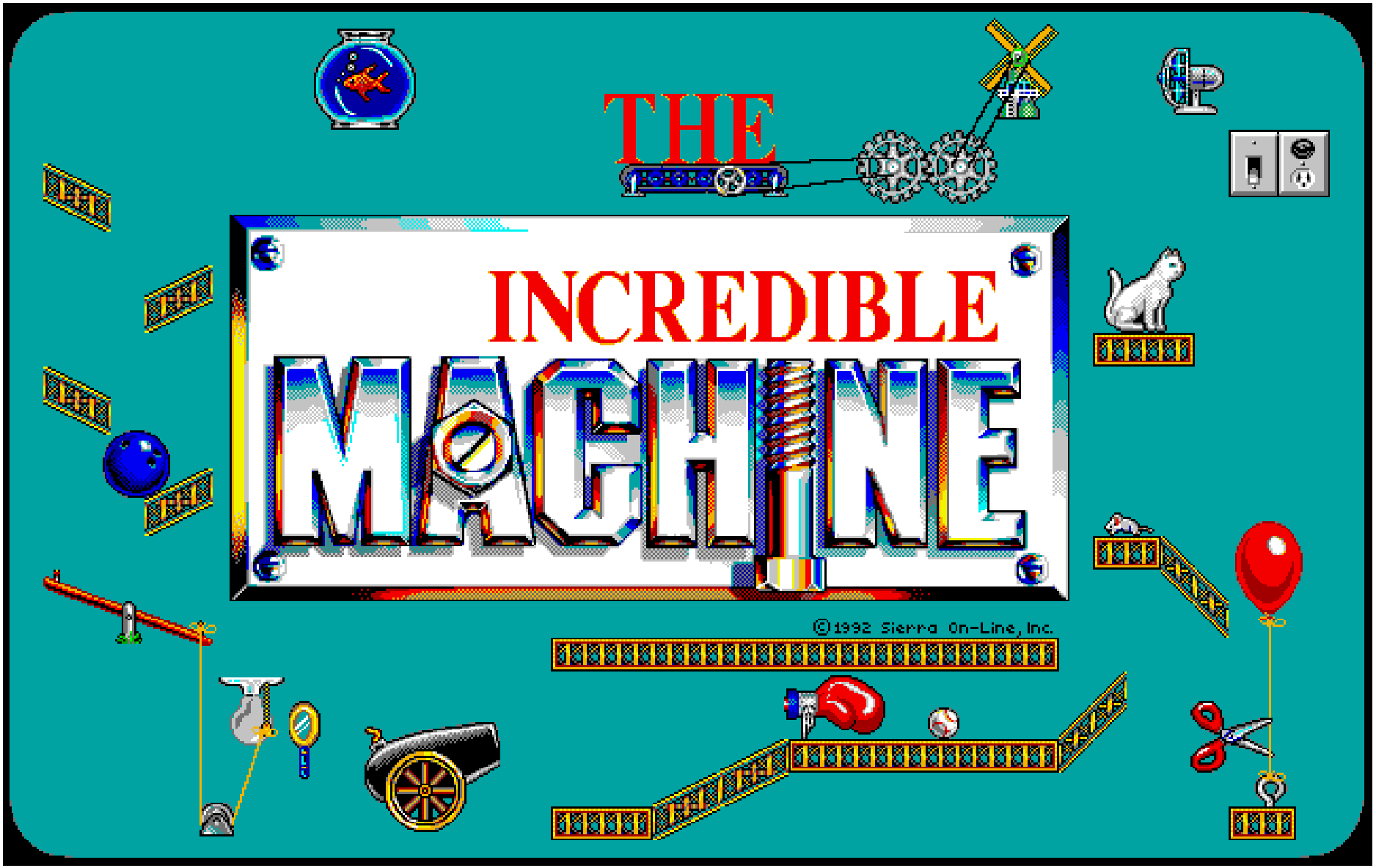
* Please provide the A end interface status and configuration

* Are there any similar working circuits with Optus? If so, please share the working circuit details.

* Evidence for the fault with Ping logs

* Reverse trace routes for working and non-working setup (Essential to investigate end – end network path)

INTO THE MACHINE



NO FAULT FOUND, CAN PING GOOGLE

Hello team,

Our investigation has concluded, and below is a summary of the incident along with the actions taken to address it.

Fault Reported: Packet Loss

Investigation Performed:
- Engineers have investigated and confirmed that the PE interface is UP.

- Successful ping test to Google DNS showed no packet loss:
-- 8.8.8.8 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss

OPTICS

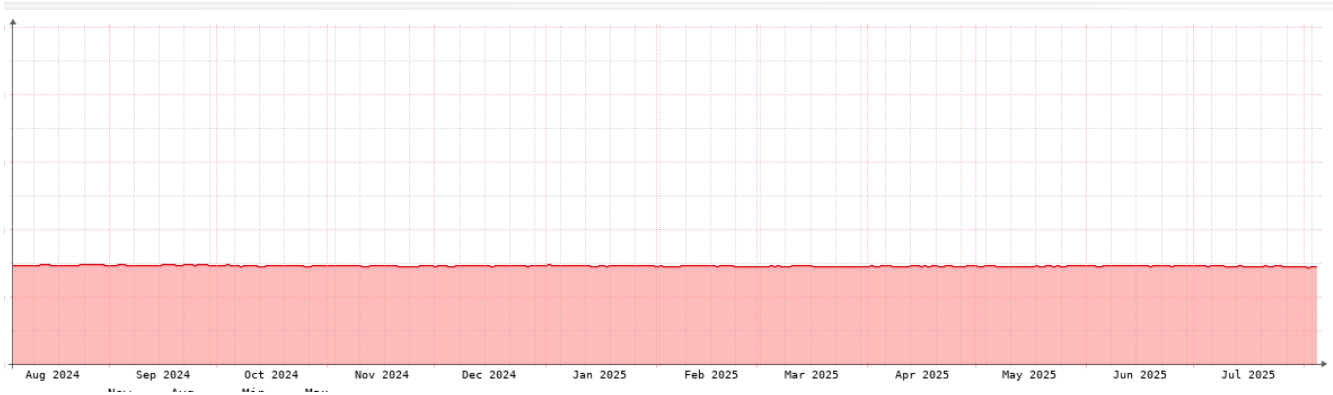
- Further checks on the DWDM path at Macquarie Park revealed no errors:
  - Transmit Power: -2.79 dBm
  - Receive Power: -18.86 dBm

RX POWER: -18.86 dBm

10KM OPTIC INSIDE A DC

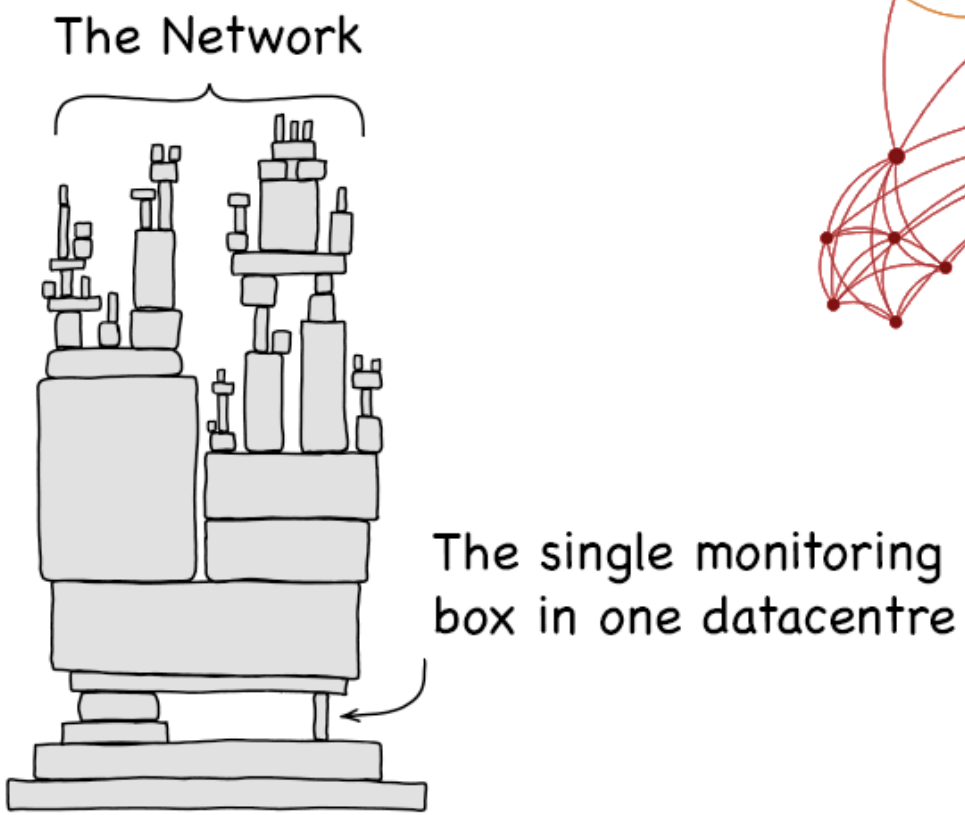
MONITORING GAP

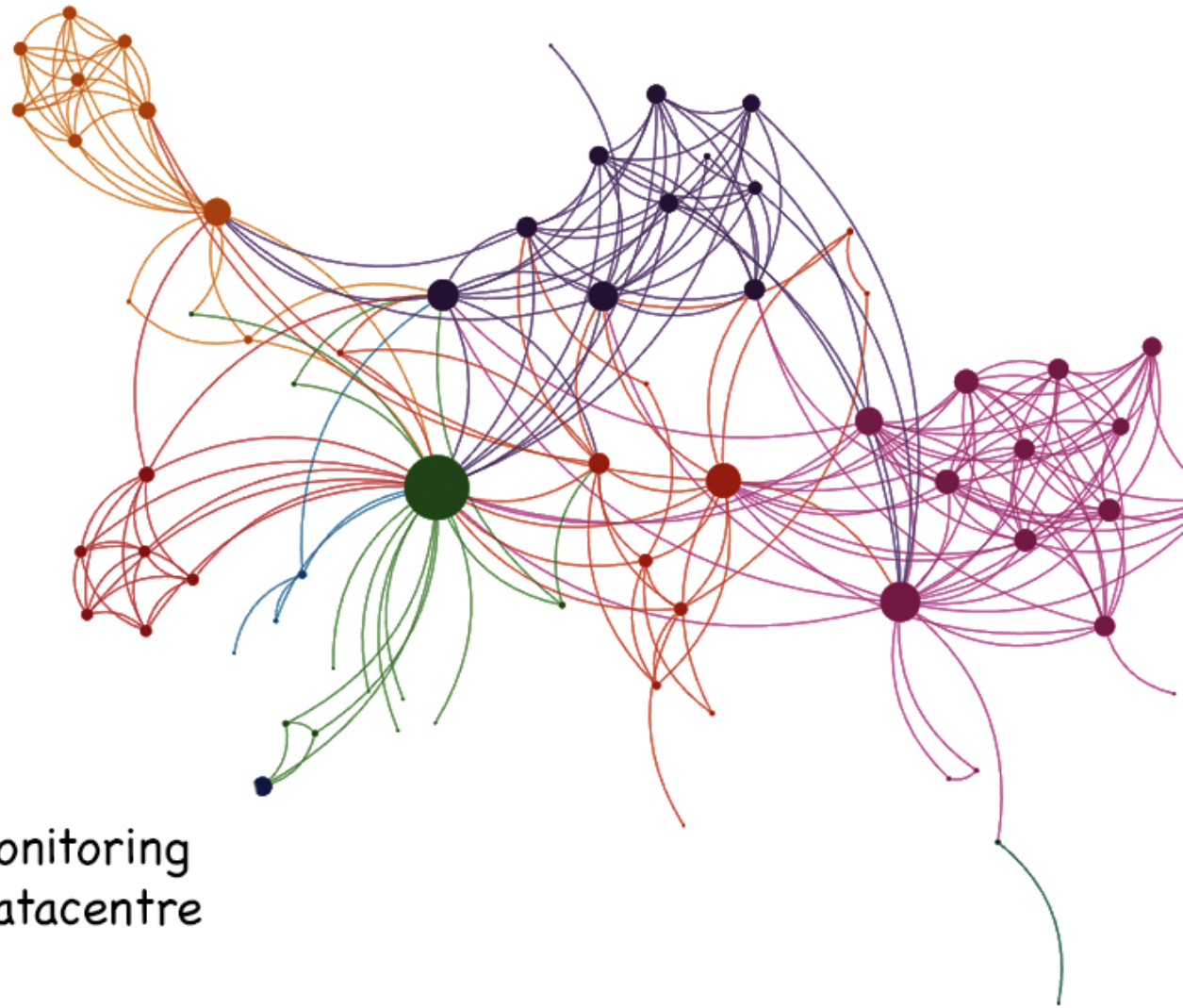
OPTICS DIE A SLOW DEATH AND TX MONITORING LIES ALL THE TIME



MONITORING IS TOO INWARD FACING

PING ALL THE THINGS





https://xkcd.com/2347/

ARISTA CONNECTIVITY MONITOR

Feature History

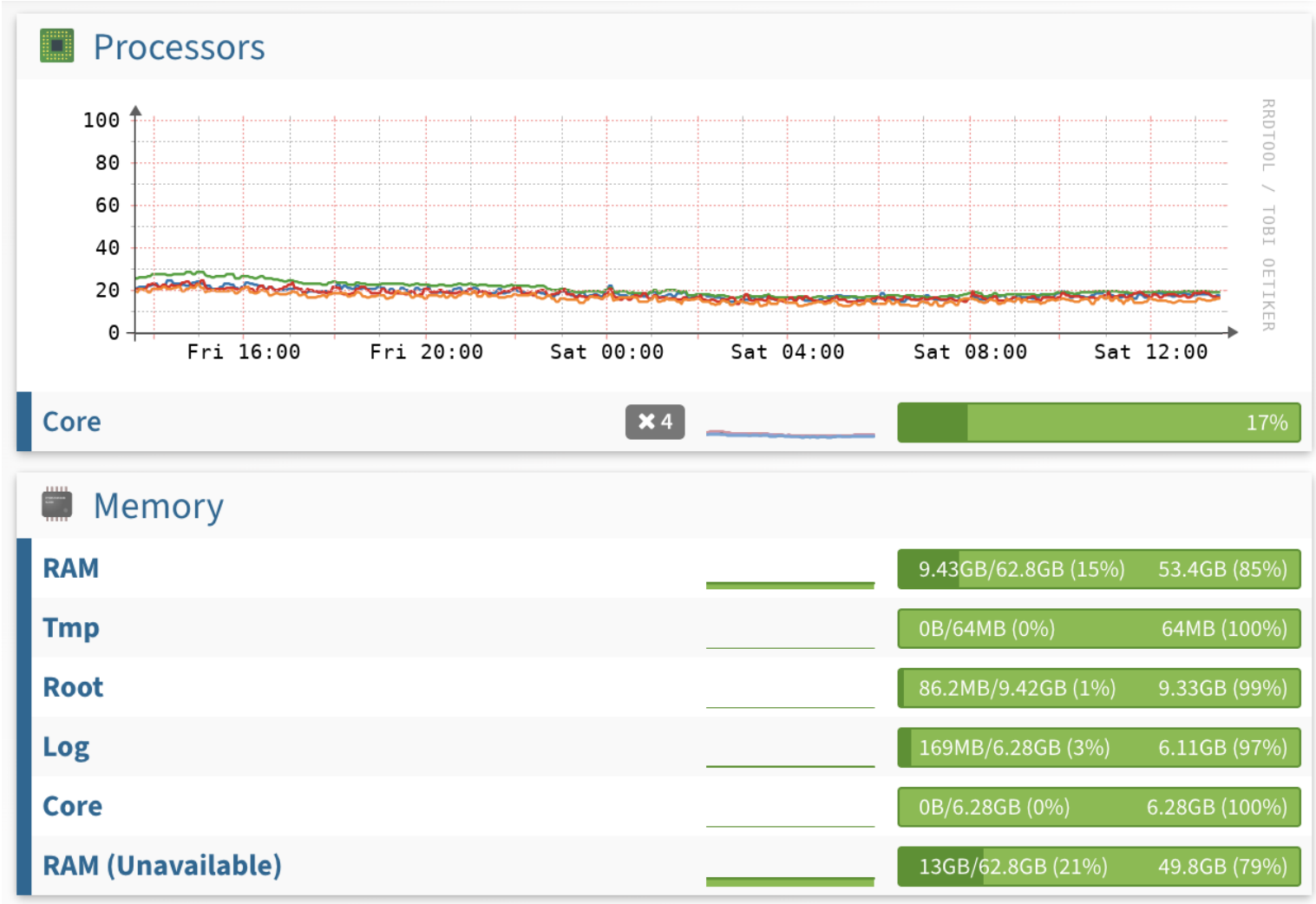
Release	Update
4.24.2F	Initial support for ConnectivityMonitor Feature
4.27.2F	Allow configuration of ICMP payload size
4.28.0F	Support for IPv6 ICMP probes
4.28.1F	Support logical source interfaces
4.31.1F	Support for Nameserver Groups
4.32.0F	Support for hostname ICMP endpoint
4.32.1F	Support for configurable ICMP DSCP bit Support for probing out of a source interface Added Syslog for loss of connectivity
4.33.0F	Support for configurable ICMP Probe frequency
4.33.1F	Support for TCP probes Support for ICMP shut down

Configuration

Connectivity Monitor is configured under the monitor-connectivity submode:

```
switch(config)# monitor connectivity
switch(config-mon-connectivity)#?
  host              Configure host parameters
  interface         Configure a set of source interfaces
  interval          Configure probe interval in seconds (default is 10 seconds)
  local-interfaces  Configure the default interface set for probing
  shutdown          Shutdown connectivity monitor
  vrf               Configure VRF for connectivity probes
```

ROUTE ENGINE



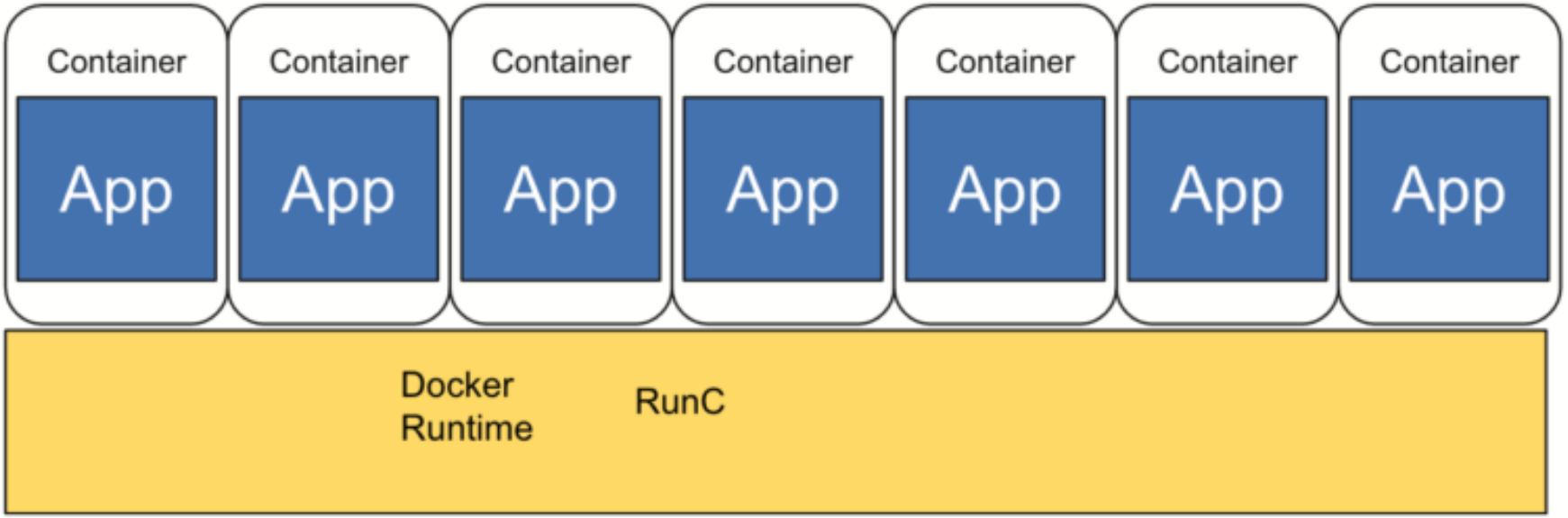
17%

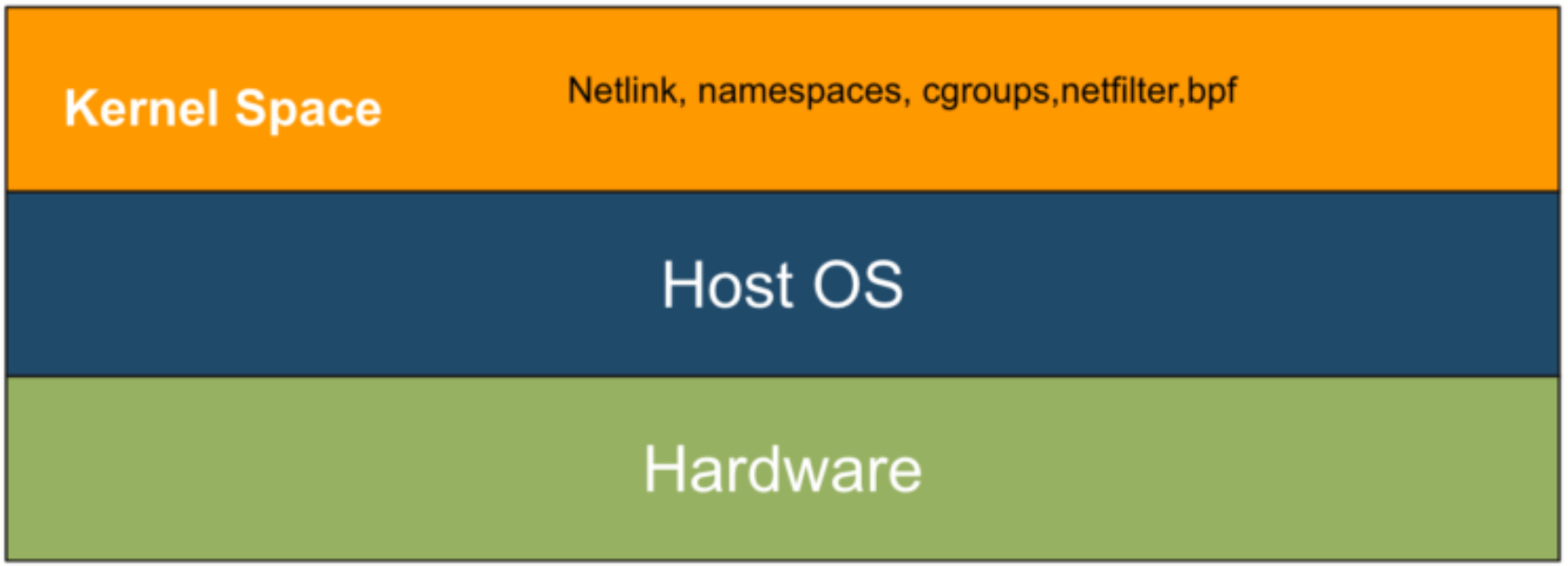
21%

13 GB/

62.8 GB

ARISTA LINUX





LINUX ROUTE ENGINE

```
arista01#bash

Arista Networks EOS shell


[admin@arista01 ~]$ hostnamectl
   Static hostname: (unset)
Transient hostname: arista01
         Icon name: computer-desktop
           Chassis: desktop
        Machine ID: 4d02e62f013c427691361763ed6e765
           Boot ID: 8cef6f6a9e934b6aa088a954bc7ae178
  Operating System: AlmaLinux 9.4 (Seafoam Ocelot)
       CPE OS Name: cpe:/o:almalinux:almalinux:9::baseos
            Kernel: Linux 5.10.165.Ar-41743436.4333F
      Architecture: x86-64
  Firmware Version: Aboot-norcal9-9.0.3-4core-14223577
```

NORMAL LINUX NETWORKING

```
[root@arista01 ~]# ip netns list
ns-INTERNET (id: 2)
ns-mgmt (id: 1)
default

[root@arista01 ~]# ip link show et23_1
52: et23_1:
<BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc prio state UP mode DEFAULT group
default qlen 1000
    link/ether 12:34:56:78:ff:ff brd
ff:ff:ff:ff:ff:ff
```

HOW FAST CAN IT GO?

Arista Networks EOS shell

[admin@arista02 ~]$ **iperf -c 192.168.0.2**
tcp connect failed: Connection refused

Client connecting to 192.168.0.2, TCP port 5001
TCP window size: -1.00 Byte (default)

sudo iptables -I INPUT -p tcp -m tcp --dport 5001 -j ACCEPT
sudo iptables -I INPUT -p udp -m udp --dport 5001 -j ACCEPT

Server listening on TCP port 5001
TCP window size: 128 KByte (default)
---
[1] local 192.168.0.2 port 5001 connected with 192.168.0.1 port 56462
[ID] Interval Transfer Bandwidth
[1] 0.00-10.12 sec 286 MBytes 237 Mbits/sec

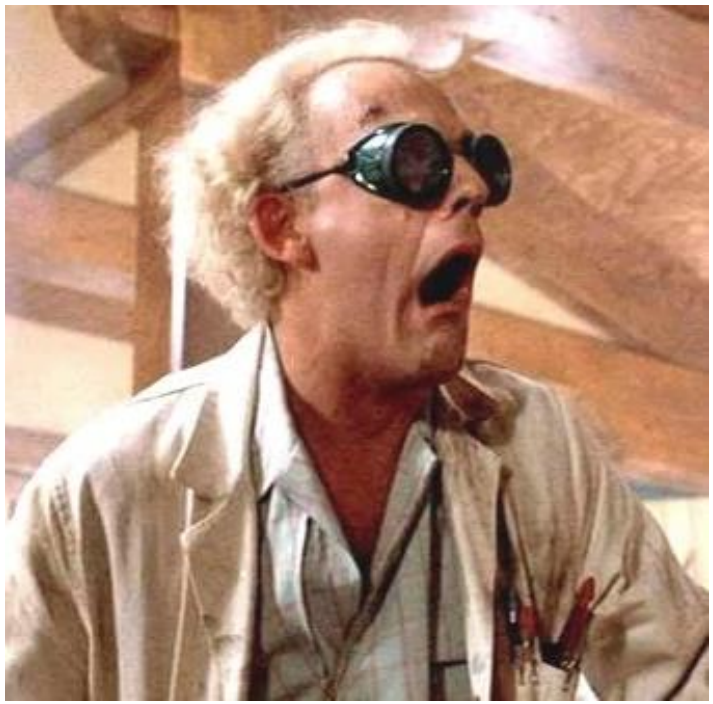
237 Mbits/sec

DISABLE ALL SAFEGUARDS

```
# clear rules
sudo iptables -X
sudo iptables -t nat -X
sudo iptables -t mangle -X
sudo iptables -t raw -X

# set default policies to ACCEPT
sudo iptables -P INPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT ACCEPT

# bye bye control plane protection
arista01(config)#
arista01(config)#system control-plane
arista01(config-system-cp)#no service-policy input copp-system-policy
```

1.21 GIGAWATTS

```
[admin@arista01 ~]$ iperf -c 192.168.0.2
------------------------------------------------------------
Client connecting to 192.168.0.2, TCP port 5001
TCP window size: 45.0 KByte (default)
------------------------------------------------------------
[  1] local 192.168.0.1 port 34790 connected with 192.168.0.2
port 5001
[ ID] Interval       Transfer     Bandwidth
[  1] 0.00-10.03 sec  1.42 GBytes  1.21 Gbits/sec
```



1.21 Gbits/sec

LINUX SOCKETS

#traceroute 213.133.116.44 source lo1

traceroute to 213.133.116.44 (213.133.116.44), 30 hops max, 60 byte packets
 1 103.251.4.57 (103.251.4.57) 0.191 ms 0.083 ms 0.091 ms
 2 103.251.4.12 (103.251.4.12) 14.803 ms 14.837 ms 14.833 ms
 3 103.251.4.51 (103.251.4.51) 60.496 ms 60.519 ms 60.513 ms
 4 103.251.4.23 (103.251.4.23) 106.597 ms 106.631 ms 106.624 ms
<snip>

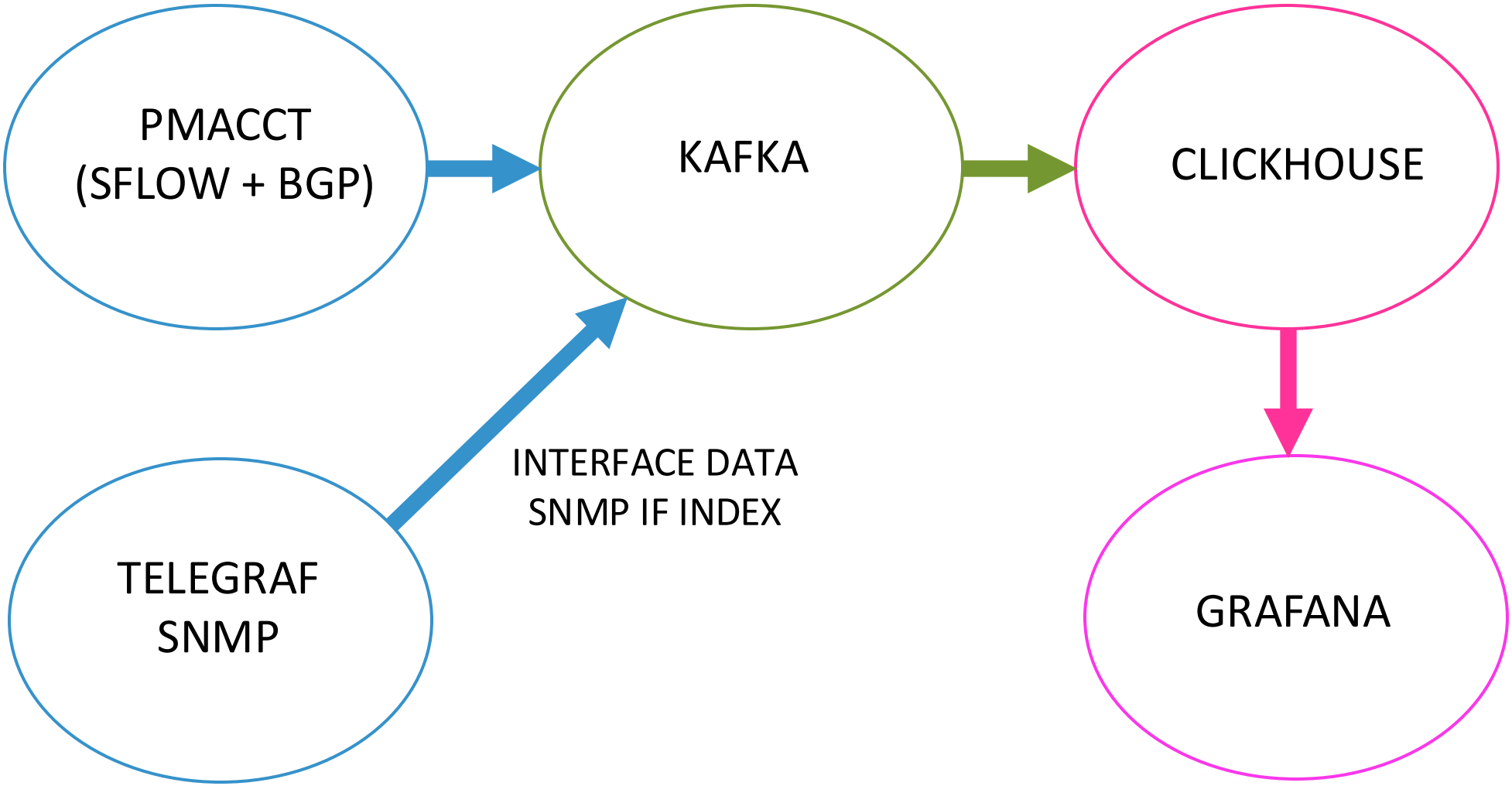
#traceroute 213.133.116.44 source port-Channel2 interface port-Channel2

traceroute to 213.133.116.44 (213.133.116.44), 30 hops max, 60 byte packets
 1 _gateway 0.993 ms 0.981 ms 1.159 ms
 2 203.50.11.240 (203.50.11.240) 2.614 ms 1.288 ms 1.323 ms
 3 203.50.13.157 (203.50.13.157) 15.158 ms 15.173 ms 15.930 ms
 4 203.50.6.106 (203.50.6.106) 16.912 ms 16.928 ms 15.506 ms
 5 203.50.13.94 (203.50.13.94) 15.924 ms 16.985 ms 15.890 ms
 6 203.50.13.94 (203.50.13.94) <MPLS:L=24121,E=2,S=1,T=255> 153.197 ms 152.087 ms 152.027 ms
<snip>

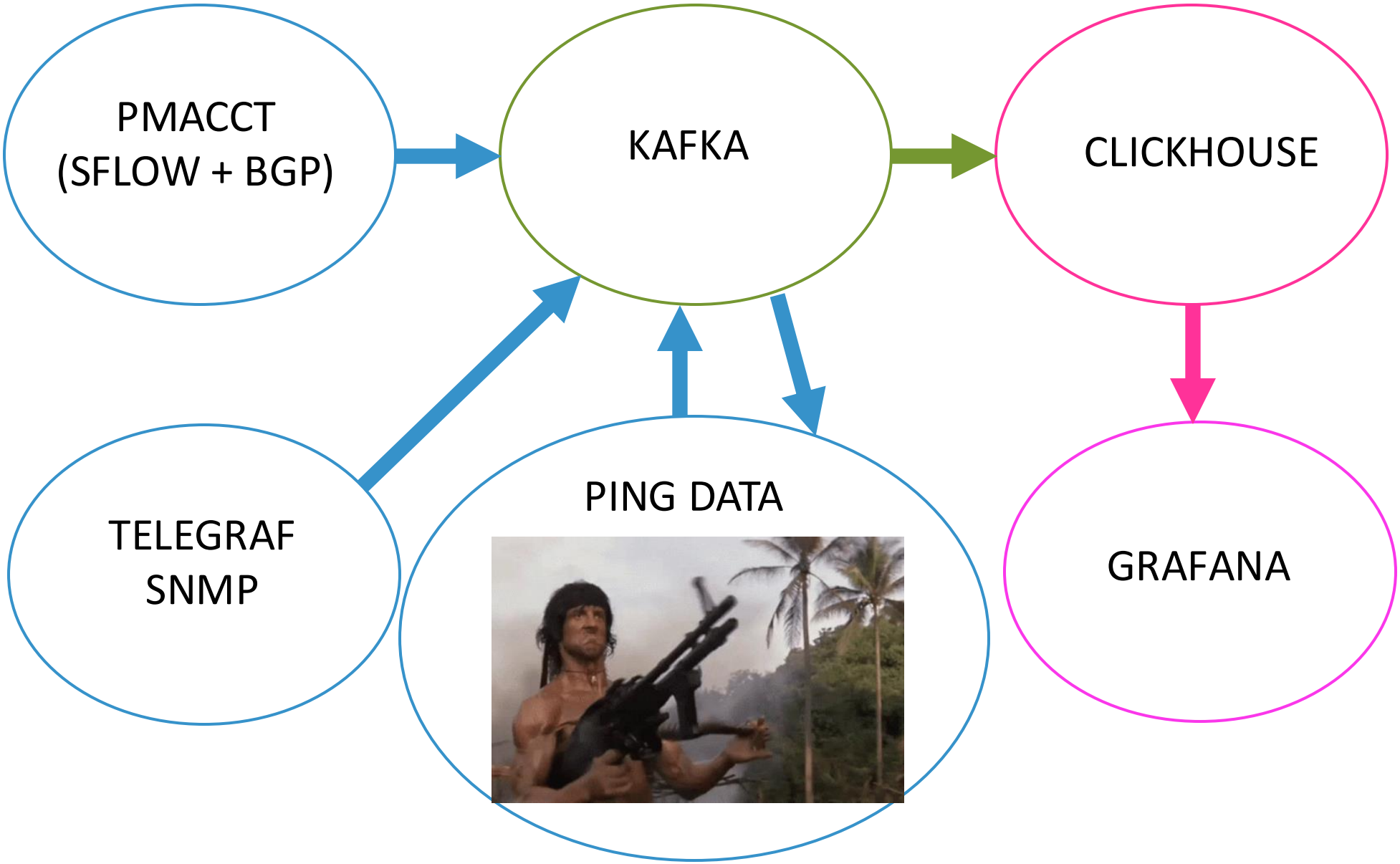
traceroute -e -4 -i po2 -s X.X.X.X -- 213.133.116.44 (hetzner.de)

ping -v -4 -b -A -c 1000 -s 72 -W 2 -i 0 -M dont -I X.X.X.X -I po2 -- 213.133.116.44

FLOW MONITORING



FLOW MONITORING



CUSTOM PYTHON DAEMON

- Connect to kafka/things_to_ping topic
- Grab list of things to ping
- Ping them based on interval/settings provided with kafka data
- Manage fping processes, one per source interface/source ip/vrf combo
- Send results back to kafka/things_we_pinged
- Send with router_id and if_index so it easily matches the sflow data
- Make sure sockets are created in the right vrf, particularly when kafka is in MGMT vrf

Install rpm's required, persist between reboots with boot-extensions:

```
daemon PingMonitorAgent
  exec /mnt/flash/PingMonitorAgent -router_id X.X.X.X
  option config_dsn value file:///mnt/flash/ping_monitor_agent.json
  option router_id value X.X.X.X
  no shutdown
```

AGENT/DAEMON FEATURES

ProcMgr will launch/re-launch your daemon if it crashes, with sensible backoff

arista01#show agent PingMonitorAgent logs
===> /var/log/agents/PingMonitorAgent-PingMonitorAgent-12278 Sun Aug 31 14:24:41 2025 <===

arista01#show daemon PingMonitorAgent
Agent: PingMonitorAgent (running with PID 27724)
Uptime: 2 days, 0:51:27 (Start time: Sat Aug 30 06:43:14 2025)
Configuration:

Option	Value
config_dsn	file:///mnt/flash/ping_monitor_config.json
router_id	172.21.4.189

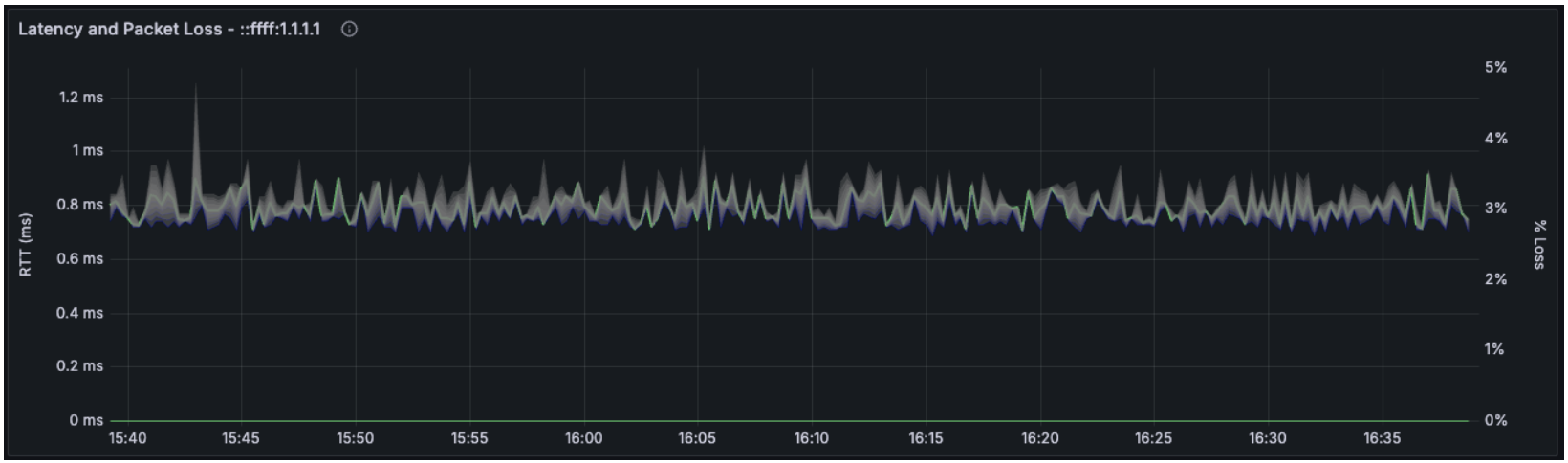
Status:

Data	Value
Config	Reloaded at 2025-08-29T14:27:02.543669

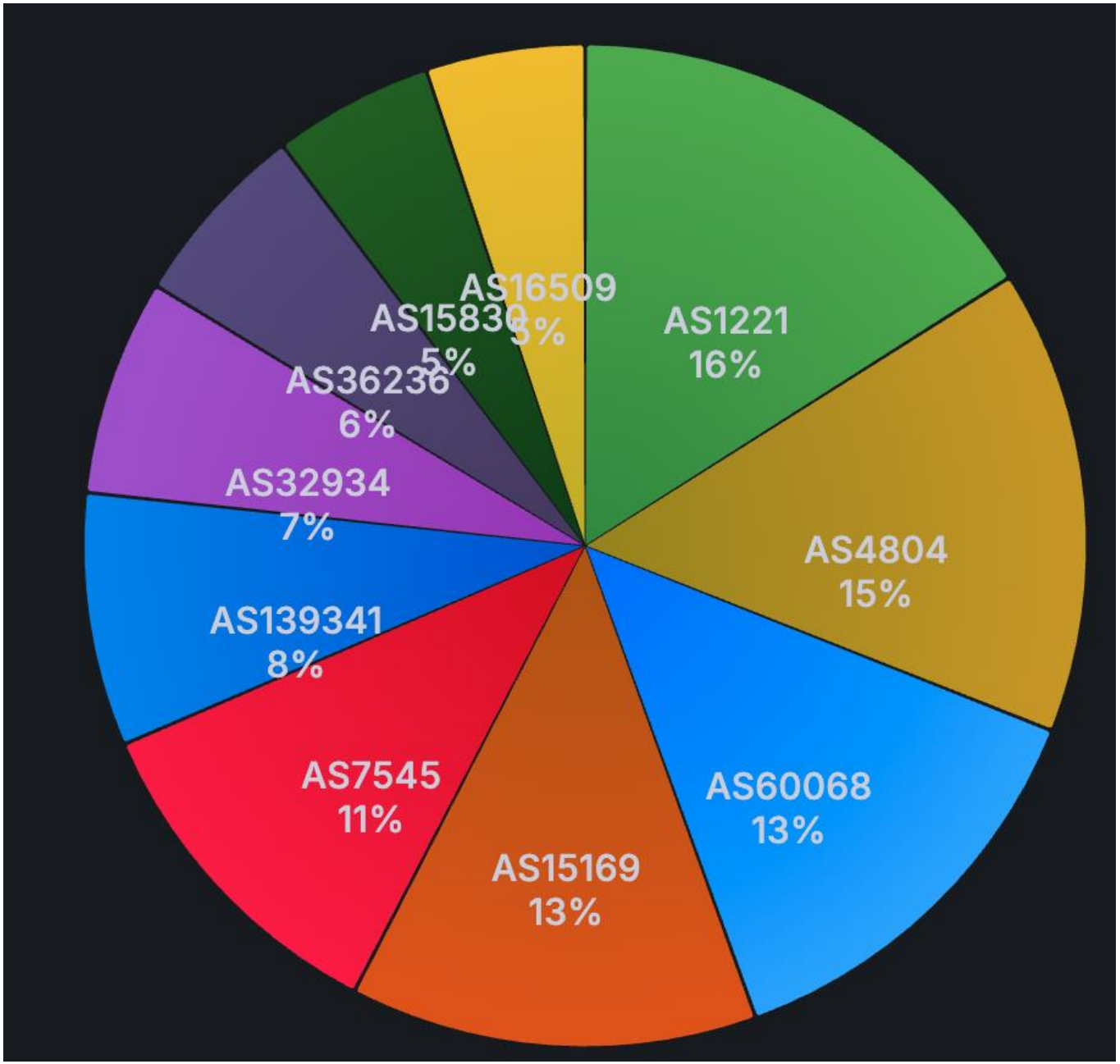
8.8.8.8 – Most pinged thing, 1.1.1.1 second

8.8.8.8

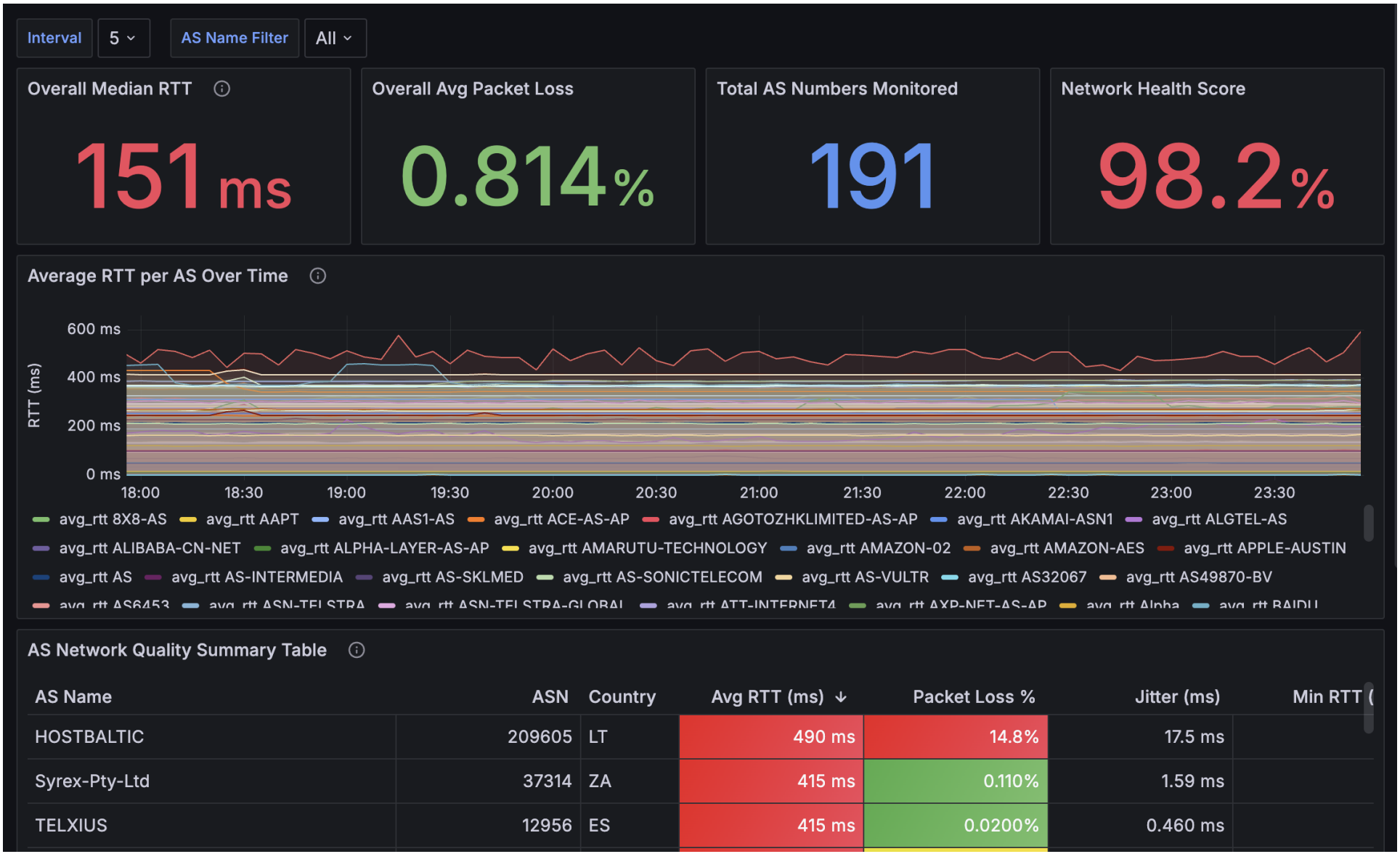
1.1.1.1



TOP 10 DESTINATION AS BY ICMP TRAFFIC



SOME GENERAL DATA



AS Network Quality Summary Table

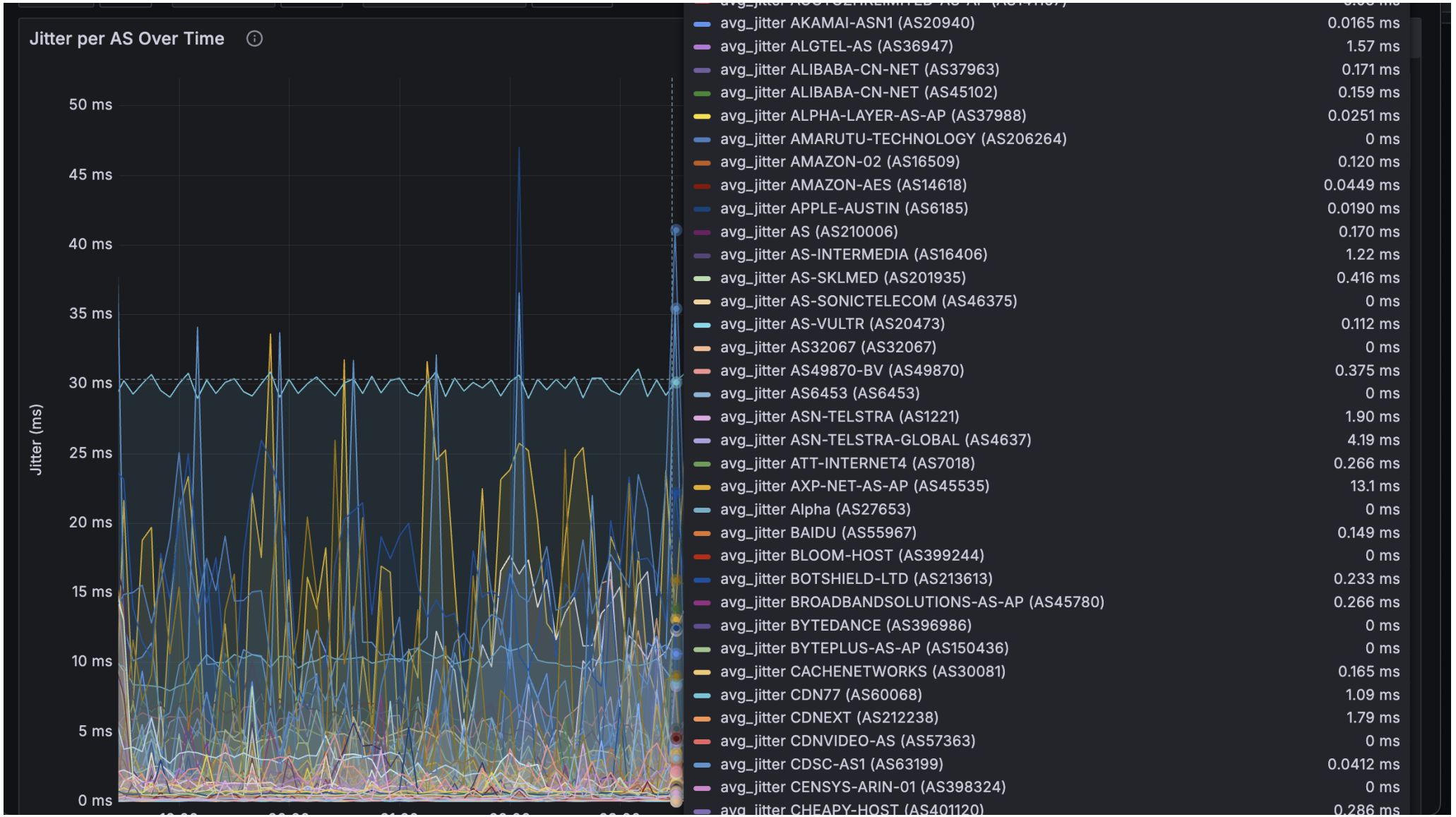
AS Name	ASN	Country	Avg RTT (ms) ↓	Packet Loss %	Jitter (ms)	Min RTT (
HOSTBALTIC	209605	LT	490 ms	14.8%	17.5 ms	
Syrex-Pty-Ltd	37314	ZA	415 ms	0.110%	1.59 ms	
TELXIUS	12956	ES	415 ms	0.0200%	0.460 ms	

MORE DATA

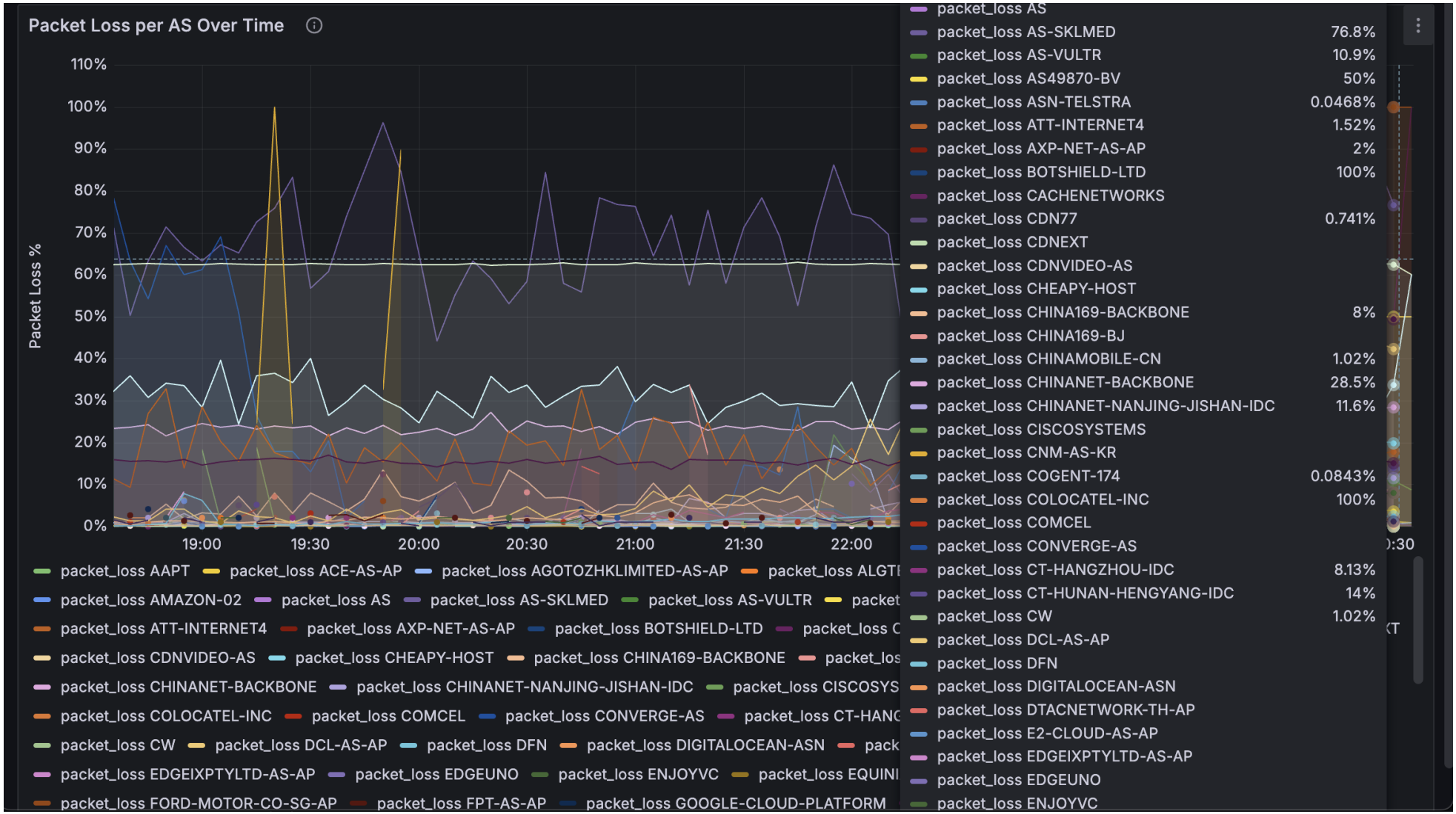
Top RTT Changes (Last Hour vs Previous)

AS Network	Recent RTT	Previous RTT	RTT Change % ↓
NTT-DATA-2914 (AS2914)	173 ms	135 ms	27.8%
ASN-TELSTRA (AS1221)	42.0 ms	34.7 ms	21.0%
DTACNETWORK-TH-AP (AS958	122 ms	139 ms	-11.9%
SYMBIO-AS-AU-AP (AS38333)	9.07 ms	10.6 ms	-14.3%
ZSCALER-INC (AS53813)	0.890 ms	1.07 ms	-17.3%
MauritiusTelecom (AS23889)	169 ms	243 ms	-30.5%
OMNITURE (AS15224)	188 ms	280 ms	-32.7%
LEVEL3 (AS3356)	94.4 ms	144 ms	-34.3%
TAOBAO (AS24429)	6.54 ms	70.9 ms	-90.8%

JITTER PER AS NUMBER



PACKET LOSS PER AS NUMBER



THANK YOU