

**SA3CC Meeting - April 20<sup>th</sup>, 2022**



**AmLight-ExP: Monitoring and Measurement @ AmLight**

**Renata Frez - Senior Network Engineer - RNP/AmLight**

# Agenda / First thoughts

- Measurement/Monitoring Tools in use at AmLight:
  - Different use cases = Different Tools
    - sFlow
    - perfSONAR
    - Telemetry
    - INT (In-band Telemetry)
  - Zabbix
  - Security
- Benefits for the SA3CC community:
  - Complete network visibility
  - Historical data
  - Identify and resolve outages
  - Identify security threats
  - Monitor SLAs
  - Recognize points for improvement

# Measurement/Monitoring Tools in use at AmLight

## AmLight Monitoring Solution

### SNMP

- ✓ Open Standard
- ✓ Compatibility
- ✓ Active or passive monitoring
- ✗ Scalability
- ✗ CPU consuming in old devices
- ✗ Long polling interval (normally > 30s seconds)

### sFlow

- ✓ Runs at the hardware level
- ✓ Sampling: Packet-based or Time-based
- ✓ Packet's detailed information
- ✗ Security (packet details exported)
- ✗ Overhead

### Syslog

- ✓ System's detailed information
- ✓ Diversity
- ✓ Packet detailed information
- ✗ Lack of standardization
- ✗ Complex analysis for non-common applications

### perfSONAR

- ✓ End-to-end test
- ✓ User perspective
- ✓ Inter-domain
- ✗ Dedicated node desirable
- ✗ Continuous testing adds heavy traffic

### Telemetry (JTI)

- ✓ Data streaming using Protocol Buffers language
- ✓ Sensors gathering data close to the source
- ✓ Scalability
- ✗ Lack of standardization
- ✗ Requires compatible nodes

### In-band Telemetry (INT)

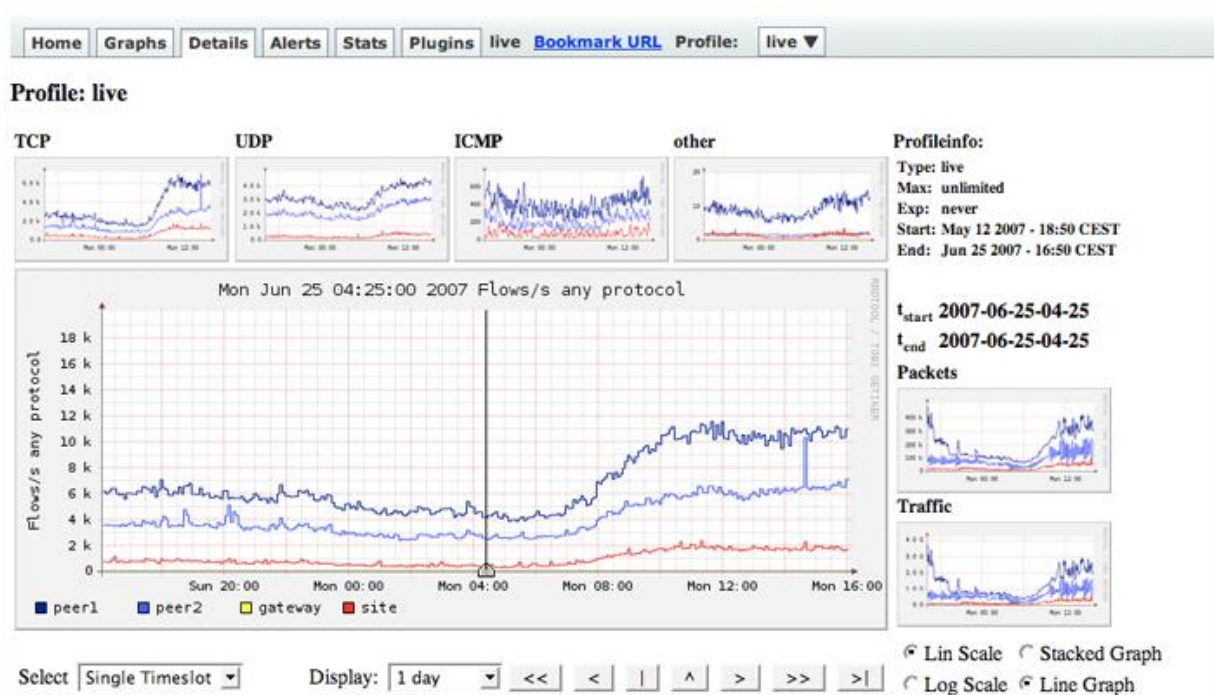
- ✓ Per-packet telemetry
- ✓ Metadata variety
- ✓ Real time
- ✗ Process/Storage constrains
- ✗ Requires compatible nodes



# Measurement/Monitoring Tools: Different use cases = Different Tools [1]

## sFlow

- Used for Traffic Analysis in AmLight routers and switches.
- Shows information about TCP/IP headers.
- Many open-source tools are available to plot graphs or create reports using flow data. For example *nfsen* and *flow-tools*.



```
$ flow-cat -p /var/netflow/tmp/jax-clk-sw01/2022-03/2022-03-22/ft-v05.2022-03-22.01300
0+0000 | flow-stat -f10 -P -S4 | head -n 30
# --- --- --- Report Information --- --- ---
#
# Fields:      Percent Total
# Symbols:     Disabled
# Sorting:     Descending Field 4
# Name:        Source/Destination IP
#
# Args:        flow-stat -f10 -P -S4
#
# src IPaddr   dst IPaddr   flows   octets   packets
#
200.2.5.1      203.178.129.220 19.204  28.396   19.204
203.178.129.220 200.2.5.1      6.804  0.898    6.804
141.211.29.100 146.141.240.111 3.427  4.834    3.427
190.103.184.103 67.58.53.140   3.377  28.355   3.377
130.183.36.80  200.17.30.65   3.226  0.331    3.226
132.195.125.239 200.17.30.65   2.823  0.205    2.823
136.145.61.76  129.114.63.48  2.571  3.764    2.571
130.183.36.68  200.17.30.65   2.319  0.126    2.319
132.195.125.234 200.17.30.65   2.218  0.123    2.218
132.195.125.231 200.17.30.65   2.117  0.113    2.117
132.195.125.230 200.17.30.65   2.016  0.107    2.016
132.195.125.233 200.17.30.65   1.966  0.162    1.966
194.80.35.168  200.17.30.136  1.915  2.852    1.915
130.183.36.67  200.17.30.65   1.764  0.265    1.764
130.183.36.81  200.17.30.65   1.714  0.180    1.714
130.183.36.82  200.17.30.65   1.714  0.093    1.714
139.229.22.23  210.98.54.10   1.663  1.606    1.663
132.195.125.229 200.17.30.65   1.512  0.081    1.512
$
```

# Measurement/Monitoring Tools: Different use cases = Different Tools [2]

## perfSONAR

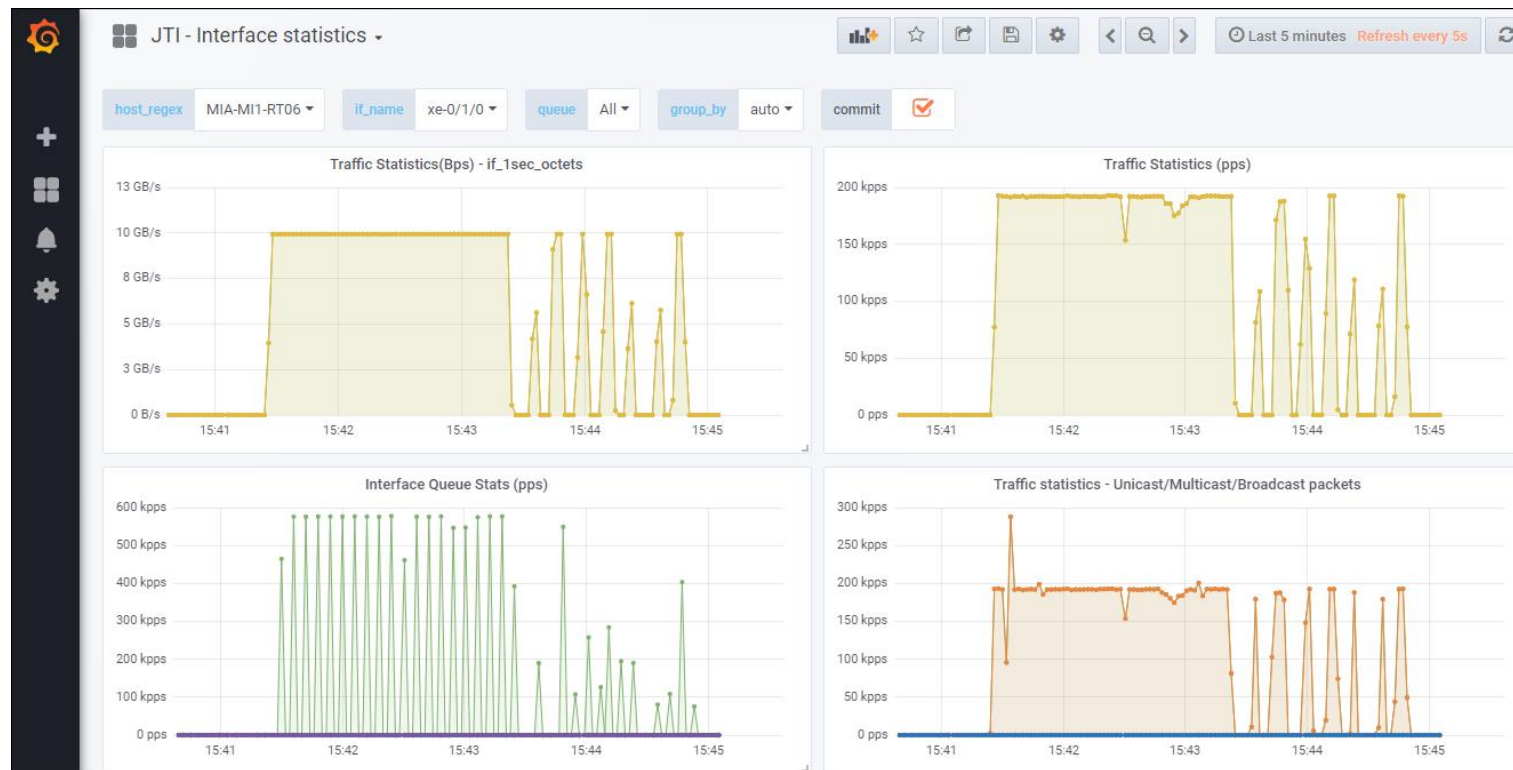
- Used to run schedule tests (Throughput, Latency, Loss).
- Reflects the user experience.
- Tests are easily deployed between two different domains.



# Measurement/Monitoring Tools: Different use cases = Different Tools [3]

## Telemetry

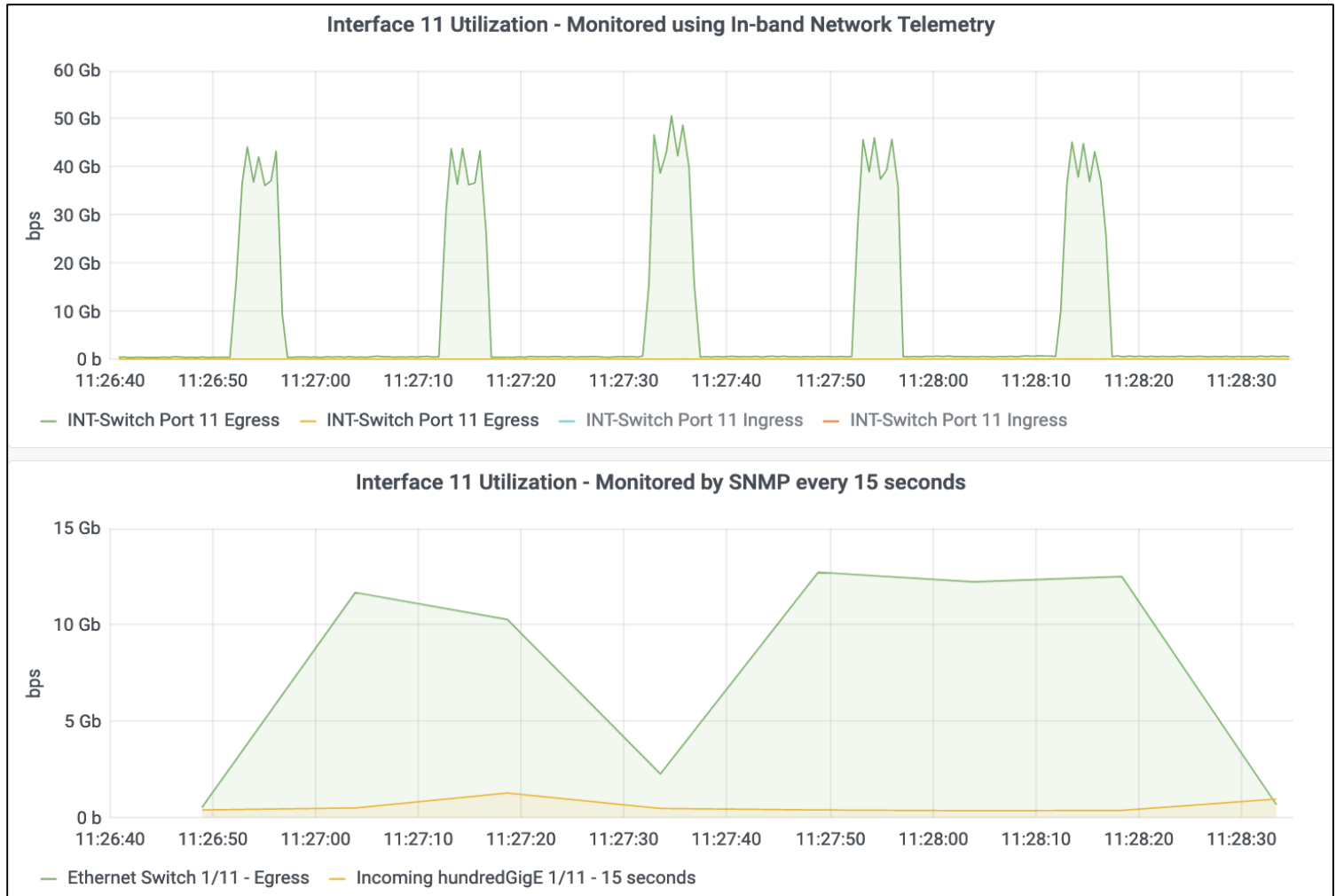
- Data streams periodically (up to 2 seconds) from the Juniper routers (JTI).
- Native sensors export data close to the source, such as the line card or network processing unit (NPU).
- Easily scales.



# Measurement/Monitoring Tools: Different use cases = Different Tools [4]

INT

- P4 application exporting reports directly from the Data Plane.
- Each user packet triggers a telemetry report (1:1).
- Used on the Noviflow switches.



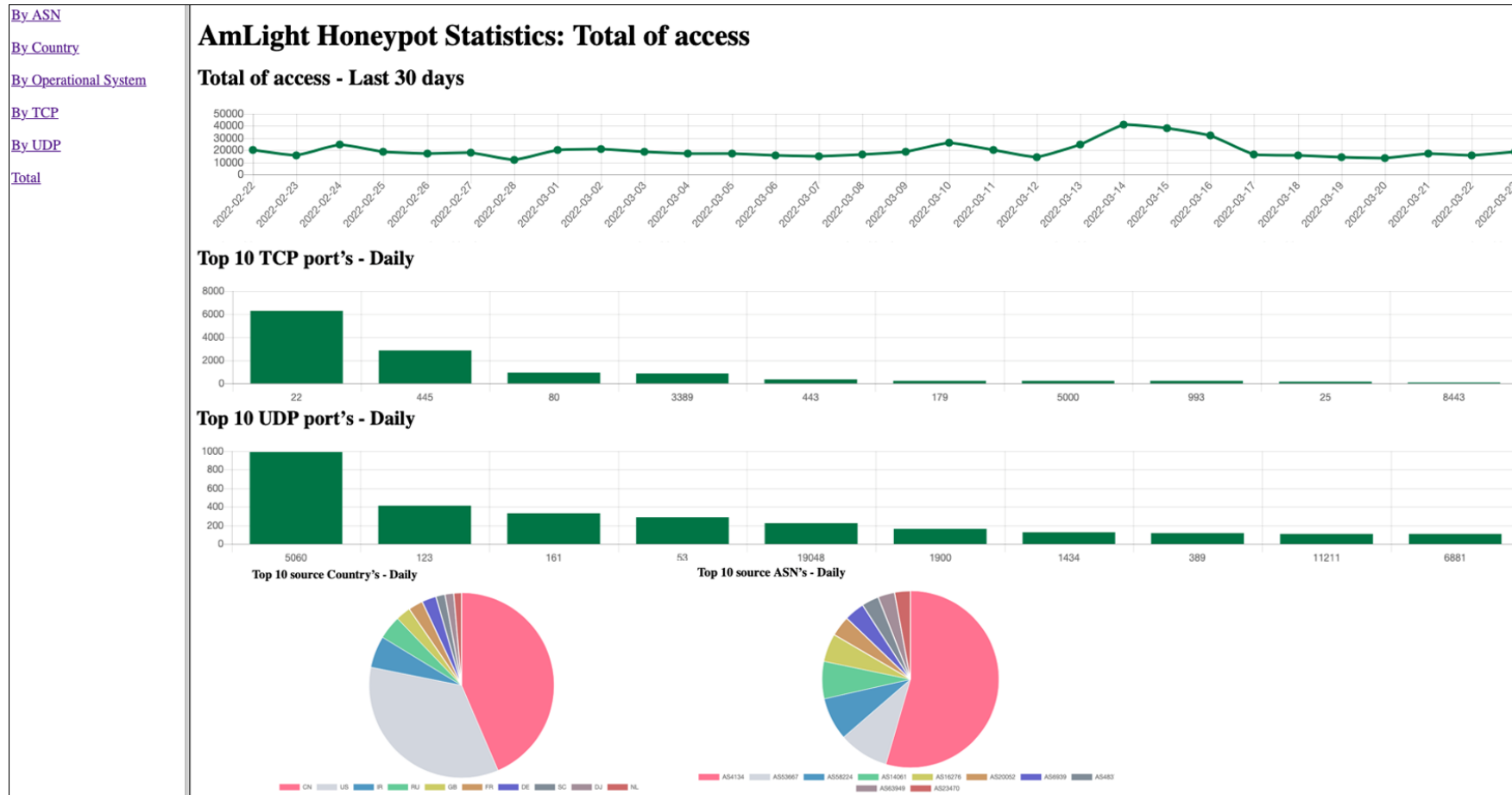
# Measurement/Monitoring Tools: Zabbix

- Zabbix is our major monitoring solution.
- Many official templates gather SNMP and other data formats from a diverse set of vendors.
- A native Zabbix agent runs on various supported platforms, including Linux, and collects data such as CPU, memory, disk, and network interface usage from a device.
- Custom scripts are combined with Zabbix to collect data using Netconf, gRPC, REST, and so on.
- Official integration plugins, such as Prometheus, Slack, and more.
- Easy visualization of historical data.



# Measurement/Monitoring Tools: Security [1]

- Honeypot: security mechanism running on an intentionally compromised server. Many reports are available.
- BGP Global Routing Table monitoring.
- DoS/DDoS monitoring.
- Threat Intelligence.



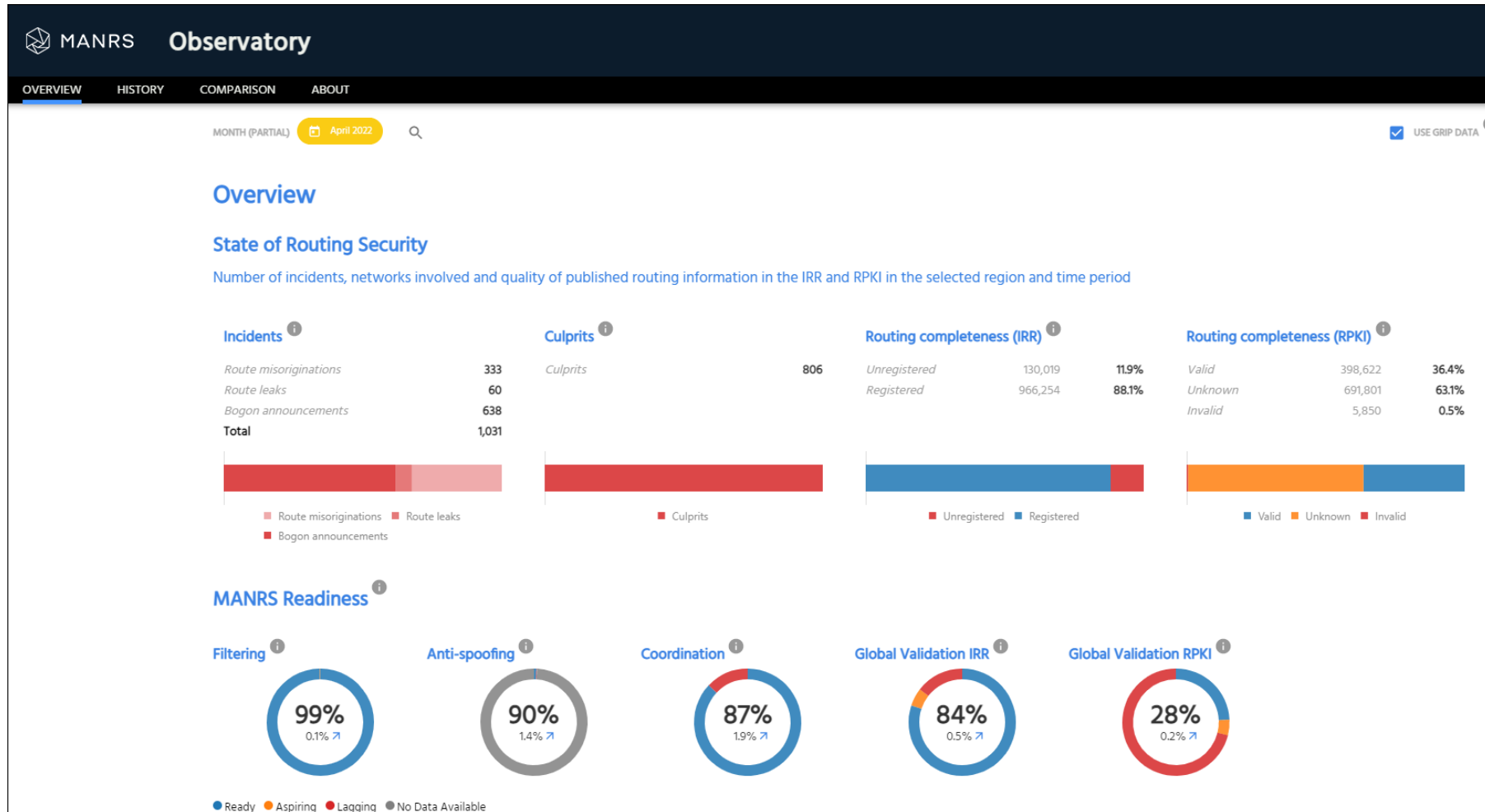
# Measurement/Monitoring Tools: Security [2]

➤ AmLight/AMPATH is part of the MANRS initiative to improve the security and resilience of today's Internet routing methods:

- Action 1: **Filtering** - Prevent propagation of incorrect routing information.
- Action 2: **Anti-spoofing** - Prevent traffic with spoofed source IP addresses.
- Action 3: **Coordination** - Facilitate global operational communication and coordination.
- Action 4: **Global Validation** - Facilitate routing information on a global scale – RPKI.



# Measurement/Monitoring Tools: Security [3]



# Final Comments

- AmLight has a rich set of tools to monitor its infrastructure and measure its performance.
- A dedicated Zabbix server for Rubin Observatory was set up, and it is continuously updated: <https://lsst.amlight.net/zabbix/zabbix.php?action=dashboard.view>.
- The perfSONAR results could be accessible by <https://dashboard.ampath.net/maddash-webui/index.cgi>.
- A Status page is available for the community to inform any ongoing events in a fast and direct way: <https://status.amlight.net>.
- Interfaces' utilization can be found on <https://my.amlight.net>.
- Monitoring every and any packet is possible with In-band network telemetry!
- INT has increased the network visibility beyond our expectations.
- Combining all monitoring tools enables AmLight to track any performance issue and user complain.
- Combining INT with learning tools will enable AmLight to create reliable trends and move towards a closed-loop orchestration SDN network.
- Monitoring security is a *must* nowadays.



Thank You! / Questions? / Comments?



**AmLight-ExP: Monitoring and Measurement @ AmLight**

Renata Frez <[renata@amlight.net](mailto:renata@amlight.net)>