AmLight ExP
Americas Lightpaths Express & Protect

IX Fórum 16 - 26-28/Out, 2022

Como Obter o Melhor do Monitoramento via Syslog, SNMP, Flows e Telemetria? Caso de Uso da AmLight

Renata Frez - Network Engineer - RNP/AmLight

Sumário

- O que é a AmLight:
  - Conectividade da Rede AmLight
  - Características da AmLight
- Qual Ferramenta/Técnica Utilizar Para a Monitoração de Rede?
  - Uma Breve Conceituação do INT
  - SNMP
  - sFlow
  - Syslog
  - perfSONAR
  - Telemetria (JTI)
  - In-band Network Telemetry
- Exemplos do dia-a-dia...:
  - Detectando anomalias na Rede de Produção: sFlow x SNMP x JTI
  - Analisando Erros de Interface na Rede de Produção: JTI x SNMP
  - Analisando Flaps de Interfaces na Rede de Produção: Syslog
- Simulações no ambiente de produção...
  - Analisando Bursts: SNMP x INT
  - Analisando Congestionamento: SNMP x INT
- Comentários Finais

O que é a AmLight?

- Um ponto de distribuição acadêmico construído para possibilitar a colaboração entre a América Latina, África e os Estados Unidos.

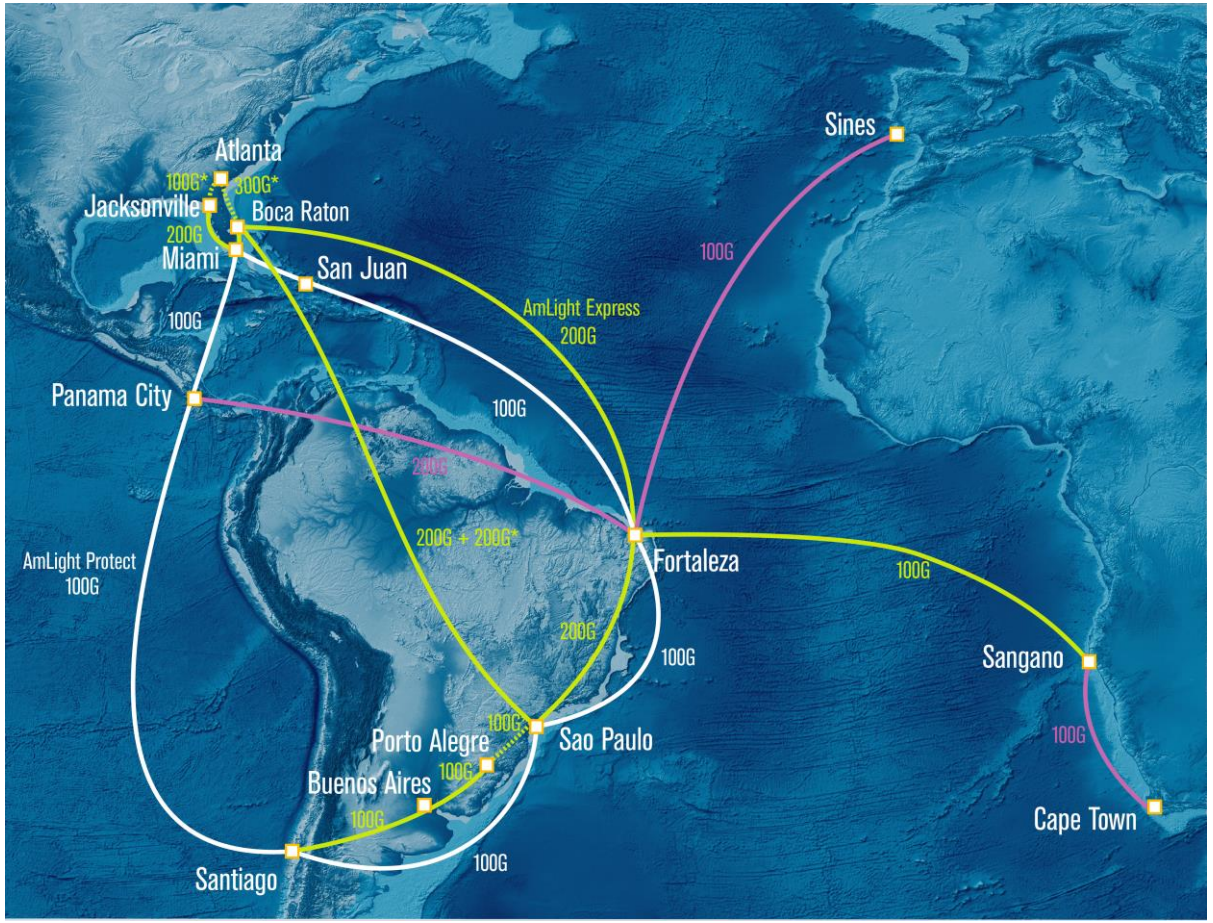
- Suportado pela NSF, OAC, e o programa IRNC através do award # OAC-2029283 de 2021-2025

- Parcerias com redes de R&E nos EUA, América Larina, Caribe e África, construídas através de camadas de confiança e abertura, compartilhando:
  - Recursos de infraestrutura
  - Recursos humanos

AmLight ExP
Americas Lightpaths Express & Protect
(NSF Award # OAC-2029283)

Características da Rede AmLight

- 600Gbps de capacidade upstream de entre os EUA e a América Latina e 100Gbps para a África
- 2+ Tbps de conectividade internacional
- Datacenters: Estados Unidos(3), Brasil(2), Chile, Porto Rico, Panamá e África do Sul
- Layer 2/3:
  - Roteadores Juniper e RARE/Freerouter
  - Switches Brocade, Dell, Corsa, Noviflow e Whiteboxes P4
- SDN:
  - Desde 2014 em produção
  - OESS e Kytos-NG como orquestradores
  - OpenFlow 1.0 e 1.3 como interfaces southbound
- Programabilidade de Data Plane:
  - Desde 2021 em produção
  - Possibilita a monitoração utilizando INT (In-band Network Telemetry)
  - Em uso atual através de switches Noviflow (Tofino ASIC)

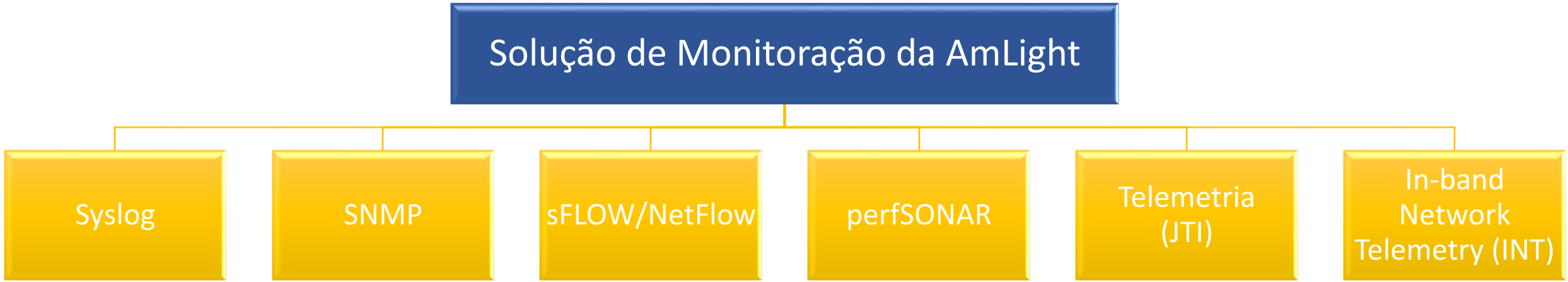


* and dashed lines represent on going efforts

AmLight ExP
Americas Lightpaths Express & Protect

Qual Ferramenta/Técnica Utilizar Para a Monitoração de Rede?

Ferramentas/Técnicas em Uso na AmLight



Antes de continuarmos... O que é o INT?

Uma Breve Conceituação do INT [1]

- O INT (In-band Network Telemetry) é uma aplicação P4 que insere dados de telemetria dentro do pacote enquanto o mesmo passa por dois pontos em um caminho na rede
  - *O objetivo é reportar o estado da rede como visto por cada pacote.*

- O INT exporta relatórios diretamente do Data Plane: sem impacto para o Control Plane
  - *Traduzindo: você pode acompanhar/monitorar/avaliar TODO pacote único em line rate e em real time.*

- Exemplos de informações de telemetria adicionadas:
  - *Timestamp, ingress port, egress port, queue buffer utilization, sequence #, entre outras.*

Uma Breve Conceituação do INT [2]

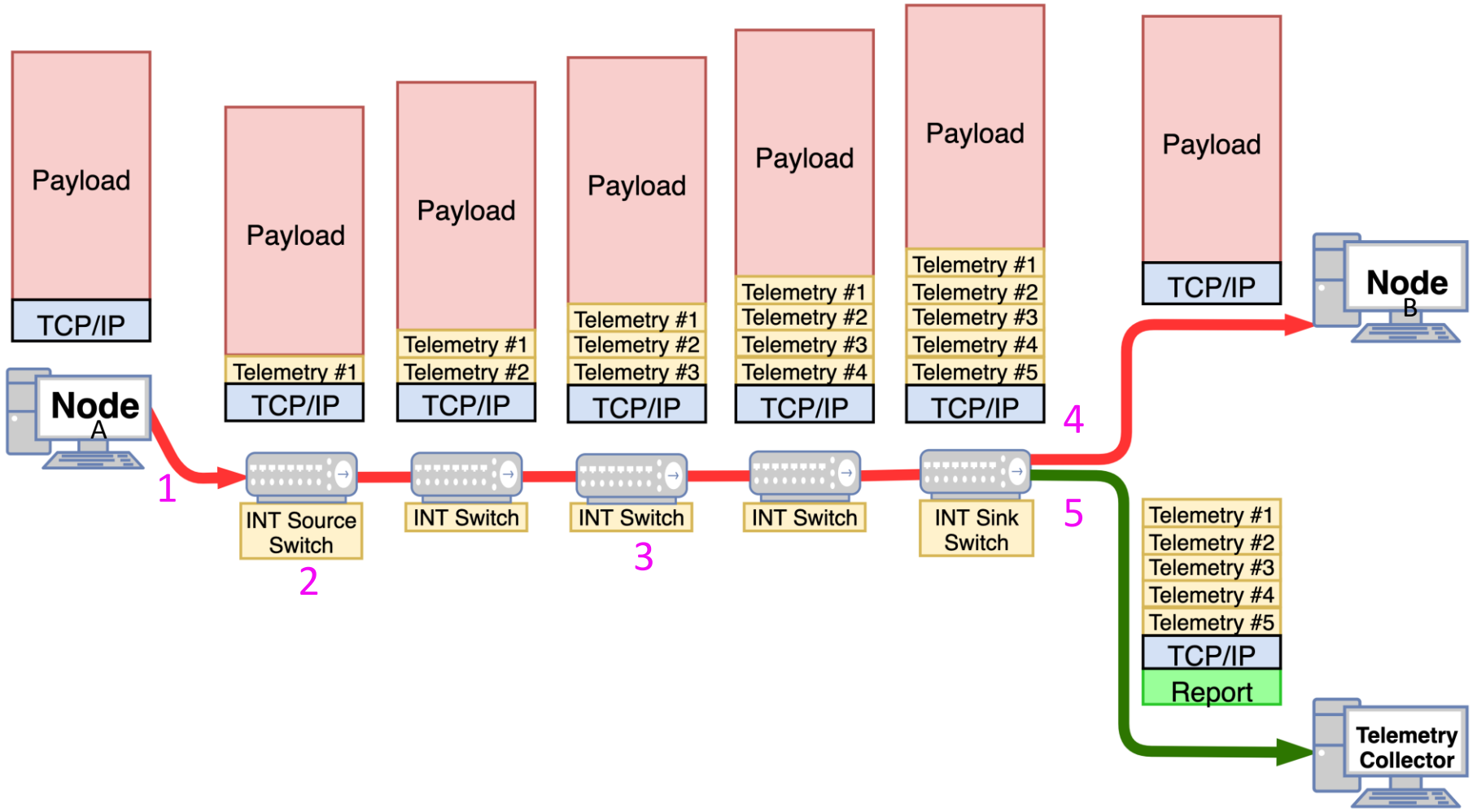
1 – O usuário envia um pacote TCP ou UDP sem conhecimento do INT.

2 – O primeiro switch (INT Source Switch) adiciona o INT header + metadata.

3 – Cada switch INT insere seus próprios metadata. Switches não-INT apenas ignoram o conteúdo INT.

4 – O último switch (INT Sink Switch) extrai a telemetria e encaminha o pacote original para seu destino.

5 – O ultimo switch (INT Sink Switch) encaminha o relatório de telemetria 1:1 para o Telemetry Collector



E agora, as técnicas utilizadas…

Syslog

Quando utilizar?

- ✓ Na detecção de novidades
- ✓ Na obtenção de informações de aplicações

Quando evitar o uso?

- ✗ Na extração de informações com alto grau de padronização
- ✗ Em sistemas muito complexos

```
$ tail -20 /var/log/servers/67.17.206.203/2022/03/22/local7.log
Mar 22 13:11:41 MIA-MI1-SW03 %STKUNIT1-M:CP %SSH-6-CONNECTION: Disconnected from 112.85.42.229
Mar 22 13:11:41 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 112.85.42.229 )
Mar 22 13:12:08 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:13:45 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 124.133.27.62 )
Mar 22 13:14:26 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:15:33 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:15:49 MIA-MI1-SW03 %STKUNIT1-M:CP %SSH-6-CONNECTION: Disconnected from 112.85.42.15
Mar 22 13:15:49 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 112.85.42.15 )
Mar 22 13:16:46 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:17:46 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 115.57.127.137 )
Mar 22 13:17:55 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:19:04 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:20:13 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:22:07 MIA-MI1-SW03 %STKUNIT1-M:CP %SSH-6-CONNECTION: Connection closed by 66.240.236.116
Mar 22 13:22:07 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 66.240.236.116 )
Mar 22 13:22:32 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:23:42 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:24:58 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
Mar 22 13:25:00 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 92.255.85.135 )
Mar 22 13:26:06 MIA-MI1-SW03 %STKUNIT1-M:CP %SEC-3-LOGIN_FAILURE: Login failure on line vty0 ( 61.177.173.6 )
```

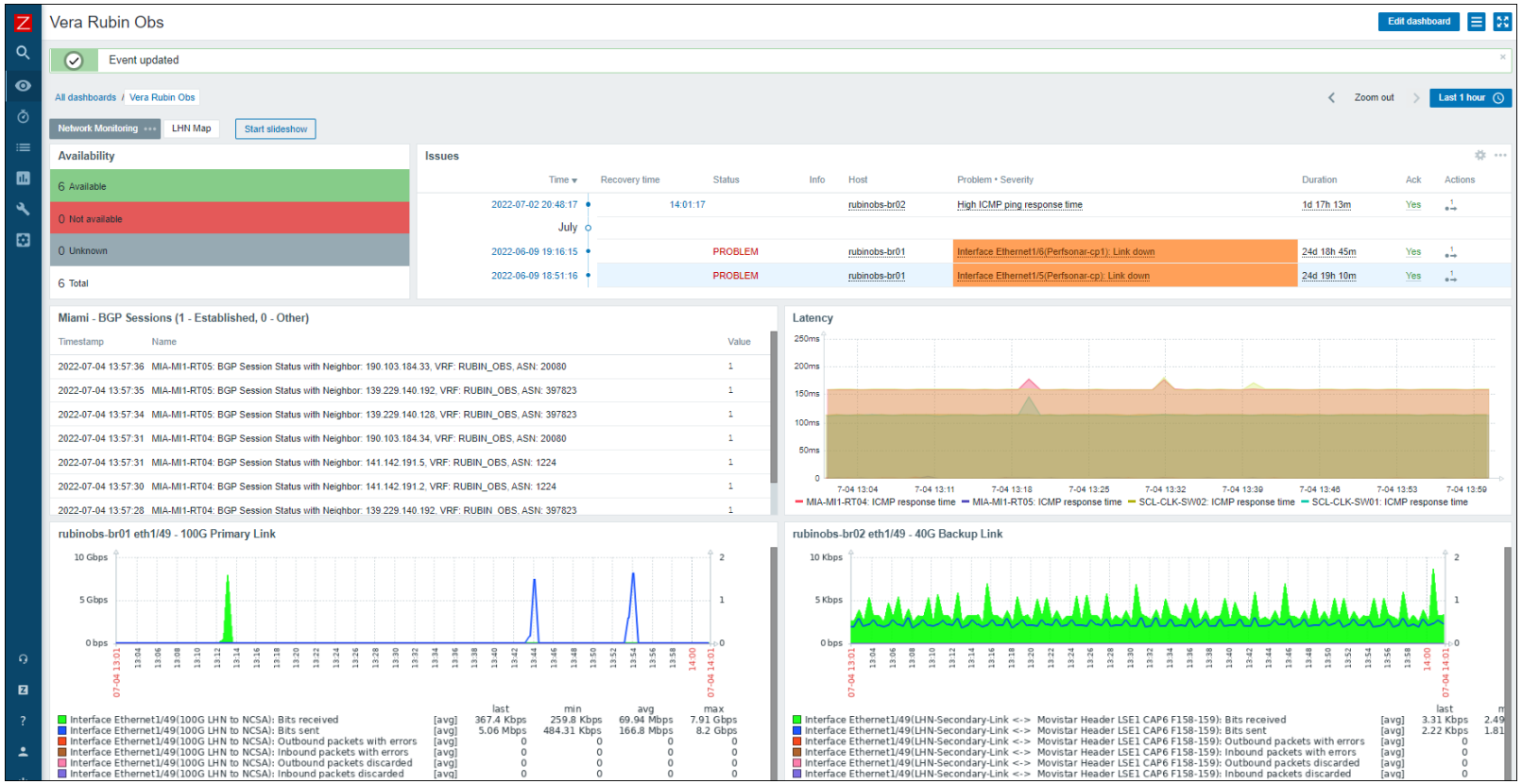
SNMP

Quando utilizar?

- ✓ Na coleta de contadores com polling > 30 segundos
- ✓ Na geração de relatórios gerenciais
- ✓ No troubleshooting de eventos de média/longa duração

Quando evitar o uso?

- ✗ Na análise de eventos abaixo da ordem de segundos
- ✗ No detalhamento do tipo de tráfego
- ✗ Em dispositivos onde o polling com menor intervalo pode prejudicar a CPU do equipamento

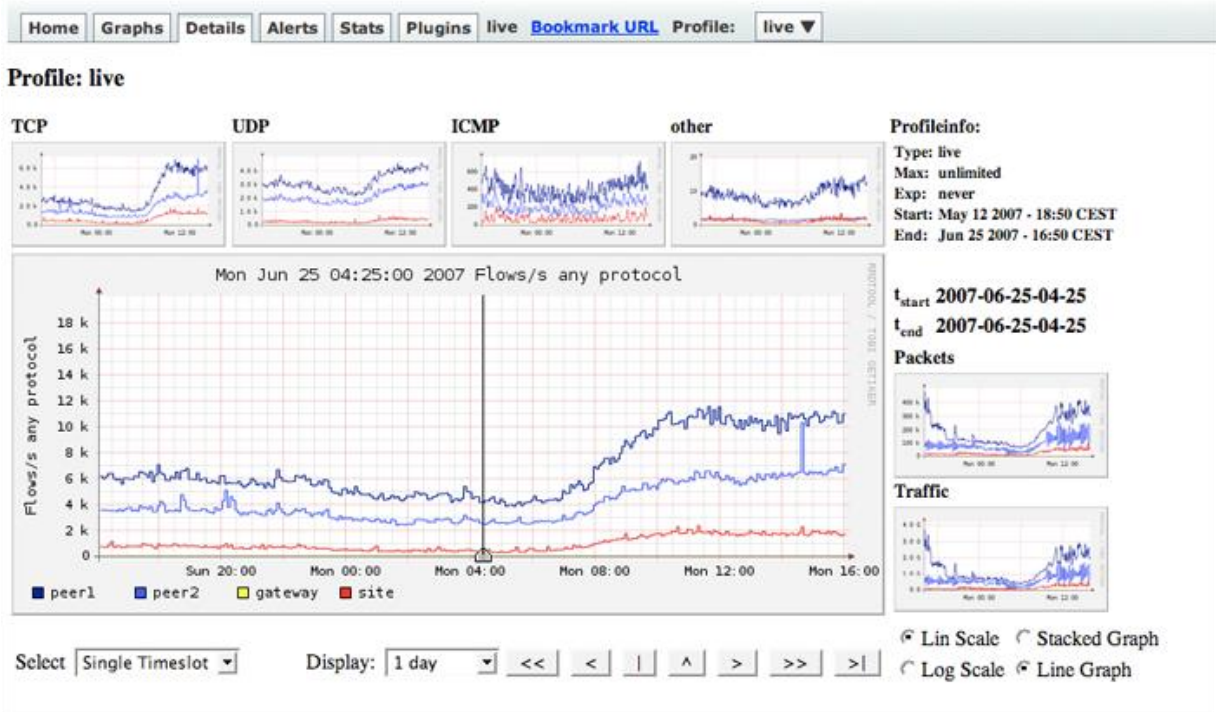


AmLight ExP
Americas Lightpaths Express & Protect

sFLOW/NetFlow

Quando utilizar?

- ✓ No troubleshooting de eventos atípicos
- ✓ Na geração de relatórios com o comportamento da rede, por exemplo, TOP usuários.



Quando evitar o uso?

- ✗ Em ambientes com informações sigilosas
- ✗ Em ambientes com pouco poder de armazenamento
- ✗ Em análises que requerem maior granularidade de dados

```
$ flow-cat -p /var/netflow/tmp/jax-clk-sw01/2022/2022-03/2022-03-22/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
$
```

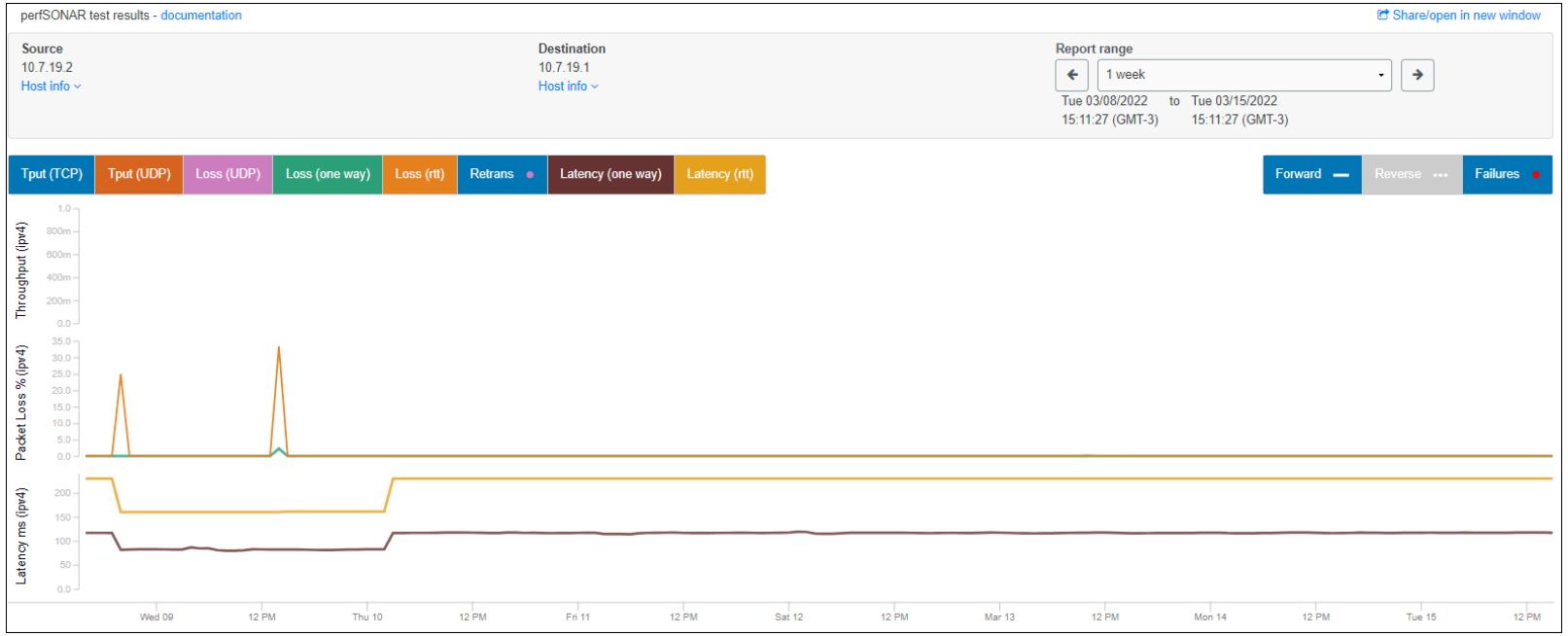
perfSONAR

Quando utilizar?

- ✓ Em testes end-to-end
- ✓ Na análise da qualidade em relação a visão do usuário

Quando evitar o uso?

- ✗ Em redes com alta utilização de banda (para testes de throughput)
- ✗ Na indisponibilidade de servidores dedicados
- ✗ Em análises que requerem maior granularidade de dados



Para mais informações, acesse a página oficial do perfSONAR: https://www.perfsonar.net...

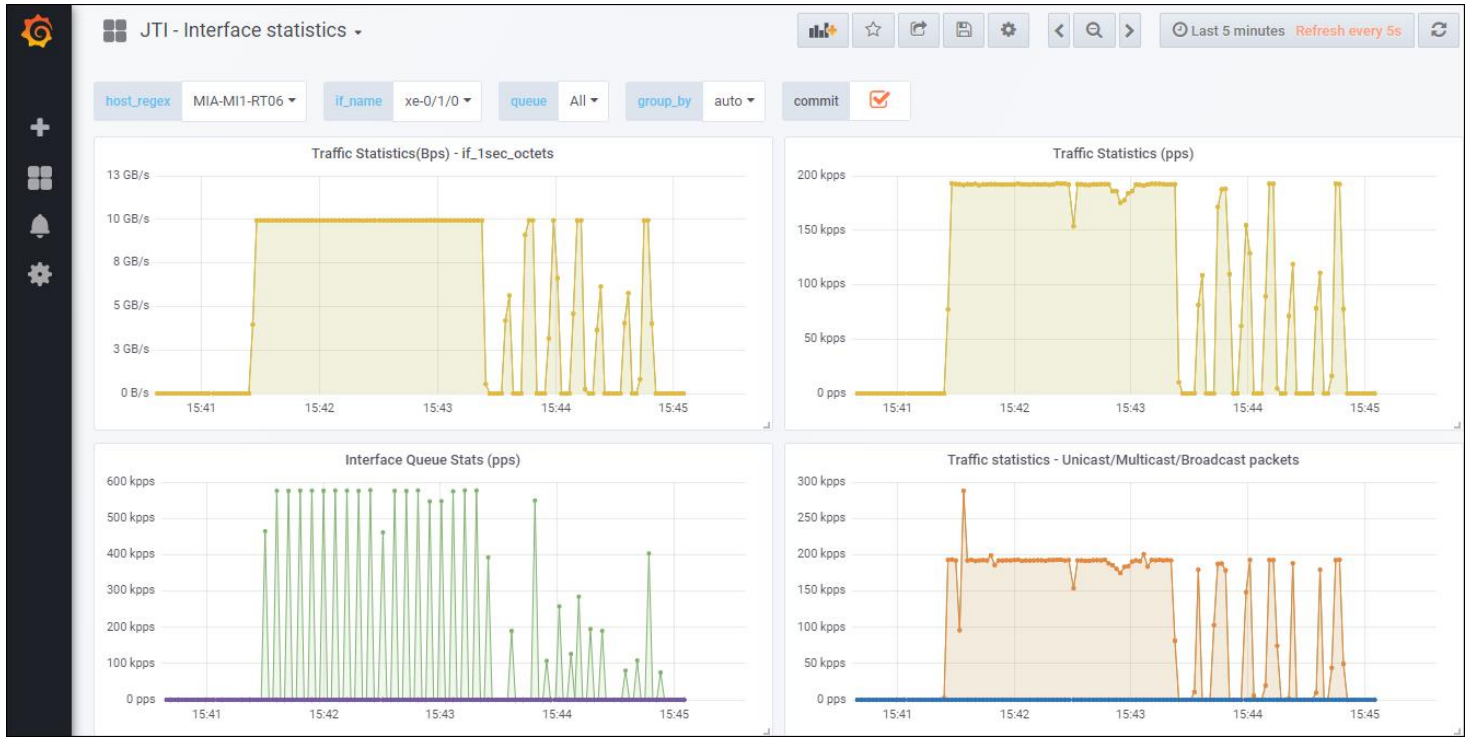
Telemetria – Juniper Telemetry Interface (JTI)

Quando utilizar?

- ✓ Em testes com maior granularidade sem impactar a CPU
- ✓ Na análise da dados provenientes de sensores mais próximos da origem

Quando evitar o uso?

- ✗ Em ambientes com muitos equipamentos sem suporte a telemetria
- ✗ Em ambientes com pouco poder de armazenamento



AmLight ExP
Americas Lightpaths Express & Protect

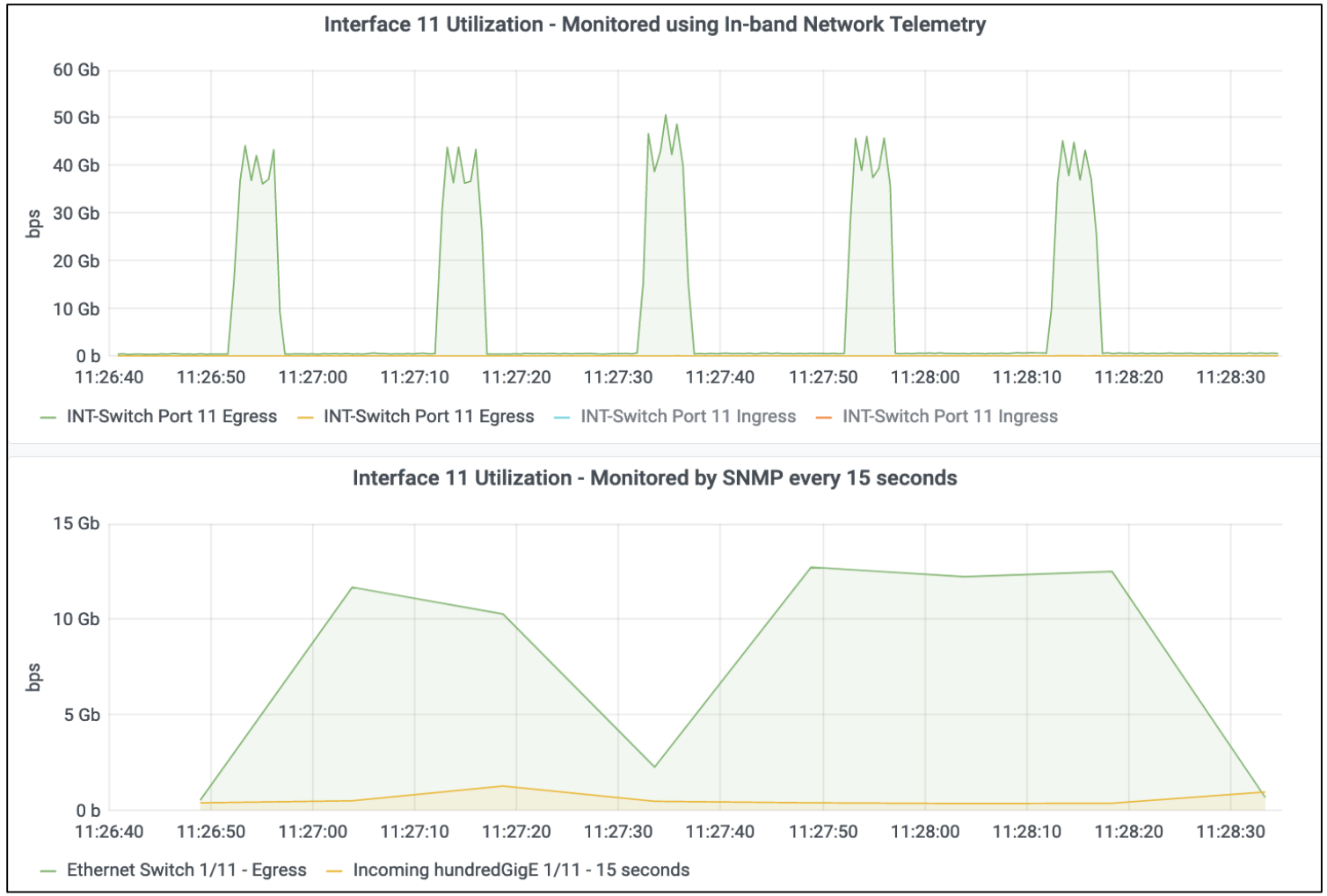
In-band Network Telemetry (INT)

Quando utilizar?

- ✓ Na coleta de telemetria em real-time por pacote (1:1)
- ✓ No troubleshooting de eventos de curta duração
- ✓ Na avaliação do caminho percorrido por um pacote

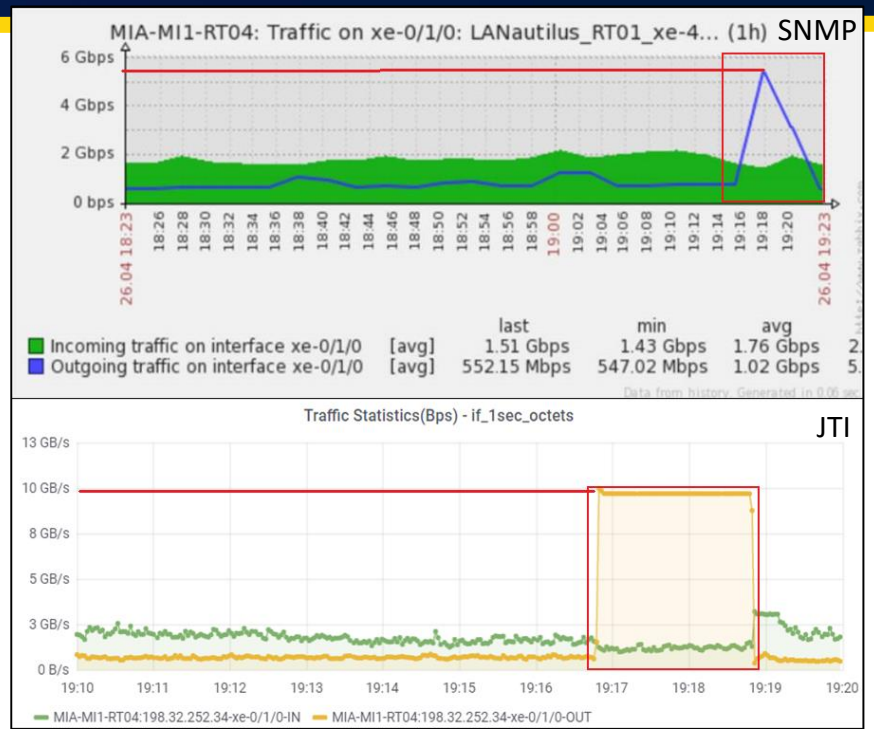
Quando evitar o uso?

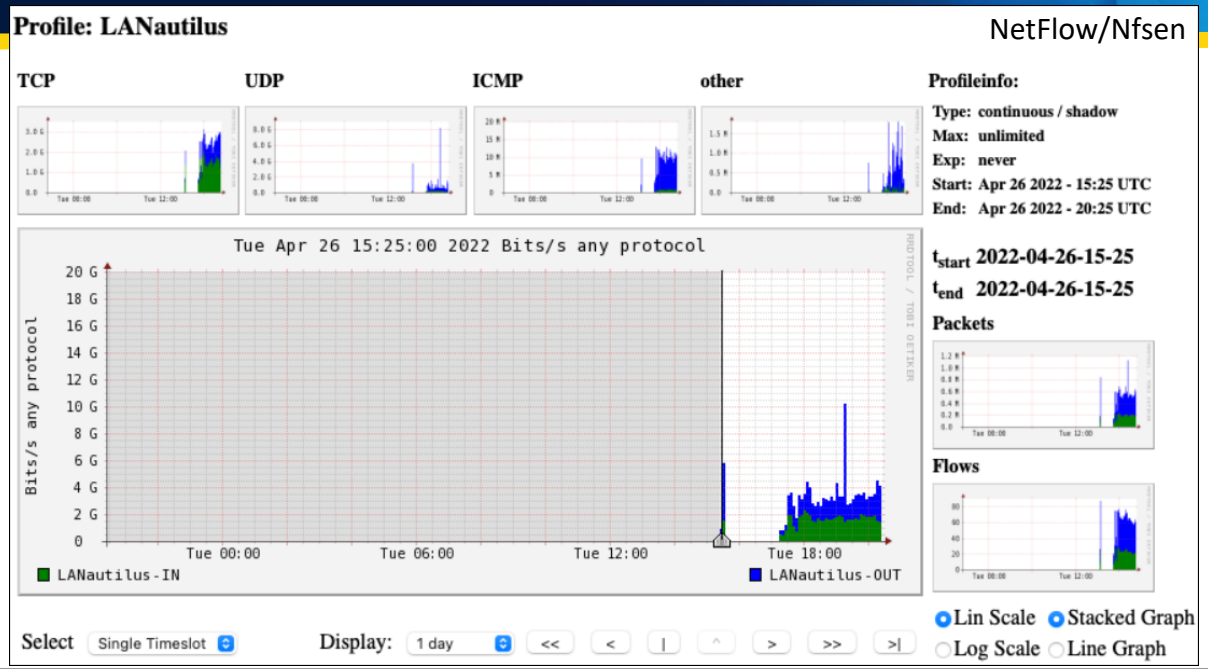
- ✗ Em ambientes com pouco poder de processamento e armazenamento
- ✗ Na geração de relatórios gerenciais



Exemplos do dia-a-dia…

Detectando Anomalias: sFlow x SNMP x JTI



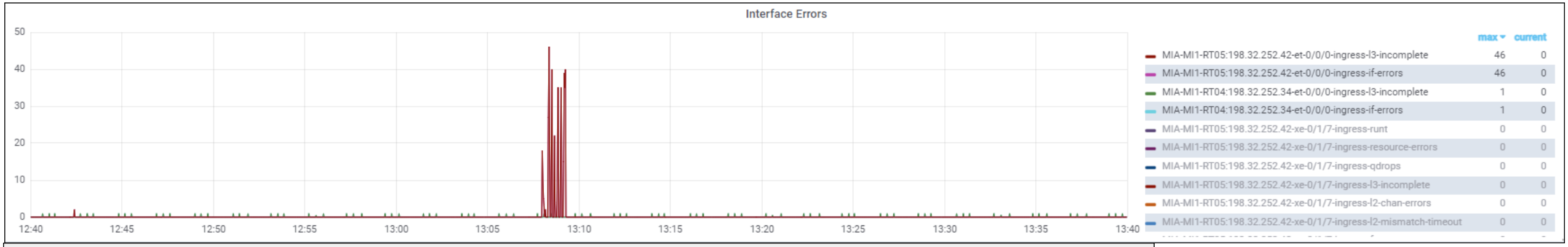


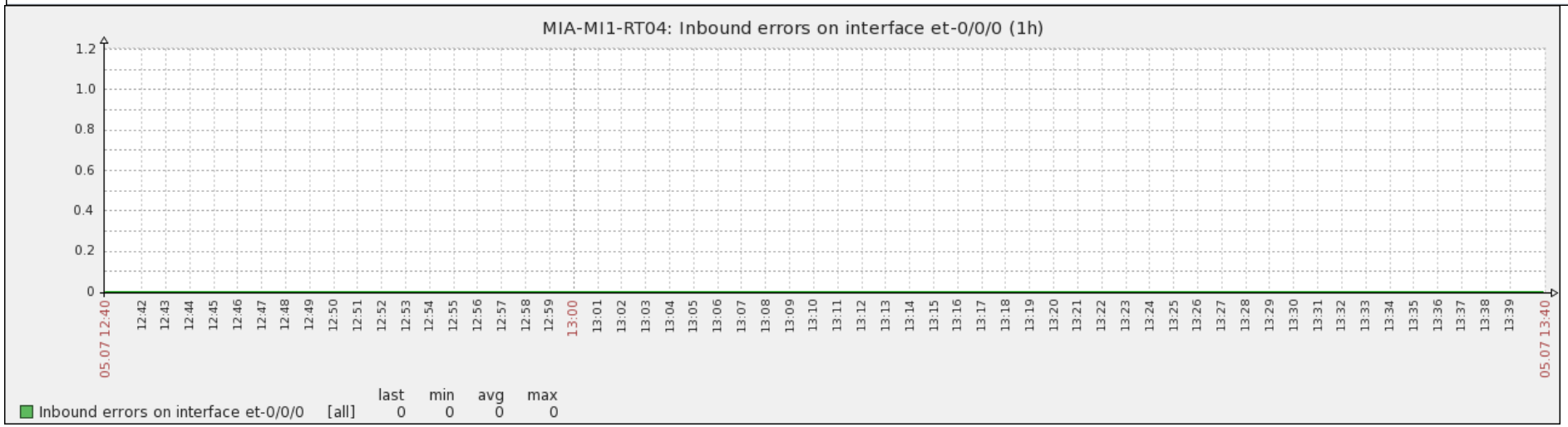

```
** nfdump -M /flows/nfdump/profiles-data/live/mia-mi1-rt04 -T  -R 2022-04-26/nfcapd.202204261910:2022-04-26/nfcapd.202204261915 -n 10 -s record/packets -B
nfdump filter:
(( ident mia-mi1-rt04) and (
OUT IF 719
)) and ( proto UDP )
Command line switch -s overwrites -a

Aggregated flows 2354
Top 10 flows ordered by packets:
Date first seen          Duration Proto      Src IP Addr:Port           Dst IP Addr:Port   Out Pkt   In Pkt Out Byte  In Byte Flows
2022-04-26 19:16:47.273   120.073 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:32318        0   22.5 M        0   32.1 G     3
2022-04-26 19:16:47.273   120.171 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:7571         0   22.1 M        0   31.5 G     3
2022-04-26 19:16:47.327   120.058 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:53705        0   21.7 M        0   30.9 G     3
2022-04-26 19:16:47.273   120.112 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:18745        0   21.5 M        0   30.7 G     3
2022-04-26 19:16:47.327   120.117 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:54999        0   21.2 M        0   30.3 G     3
2022-04-26 19:16:47.273   120.171 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:48468        0   20.2 M        0   28.8 G     3
2022-04-26 19:16:47.327   120.117 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:3309         0   19.6 M        0   27.9 G     3
2022-04-26 19:16:47.444   120.000 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:44338        0   19.5 M        0   27.8 G     3
2022-04-26 19:16:47.396   119.950 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:14311        0   19.4 M        0   27.6 G     3
2022-04-26 19:16:47.396   119.771 UDP    190.1[redacted].115:11211 <-> 42.157.128.23:39198        0   16.4 M        0   23.3 G     3
Summary: total flows: 4025, total bytes: 313.9 G, total packets: 239.9 M, avg bps: 3.8 G, avg pps: 362939, avg bpp: 1308
Time window: 2022-04-26 19:08:55 - 2022-04-26 19:19:55
Total flows processed: 171651, Blocks skipped: 0, Bytes read: 10986024
Sys: 0.047s flows/second: 3576658.6  Wall: 0.044s flows/second: 3857759.3
```

- Tráfego anormal no Upstream identificado através do SNMP e JTI.
- Identificado tráfego de 4Gbps UDP/11211 pelo NetFlow (sampling 1:4096) e através do TOP N fluxos, identificado o servidor de origem do tráfego.
- Após análise, identificada vulnerabilidade Memcached transformando o servidor em um “zombie” para ataques DDoS.
- Vulnerabilidade prontamente solucionada.

Analisando Erros de Interface: JTI x SNMP

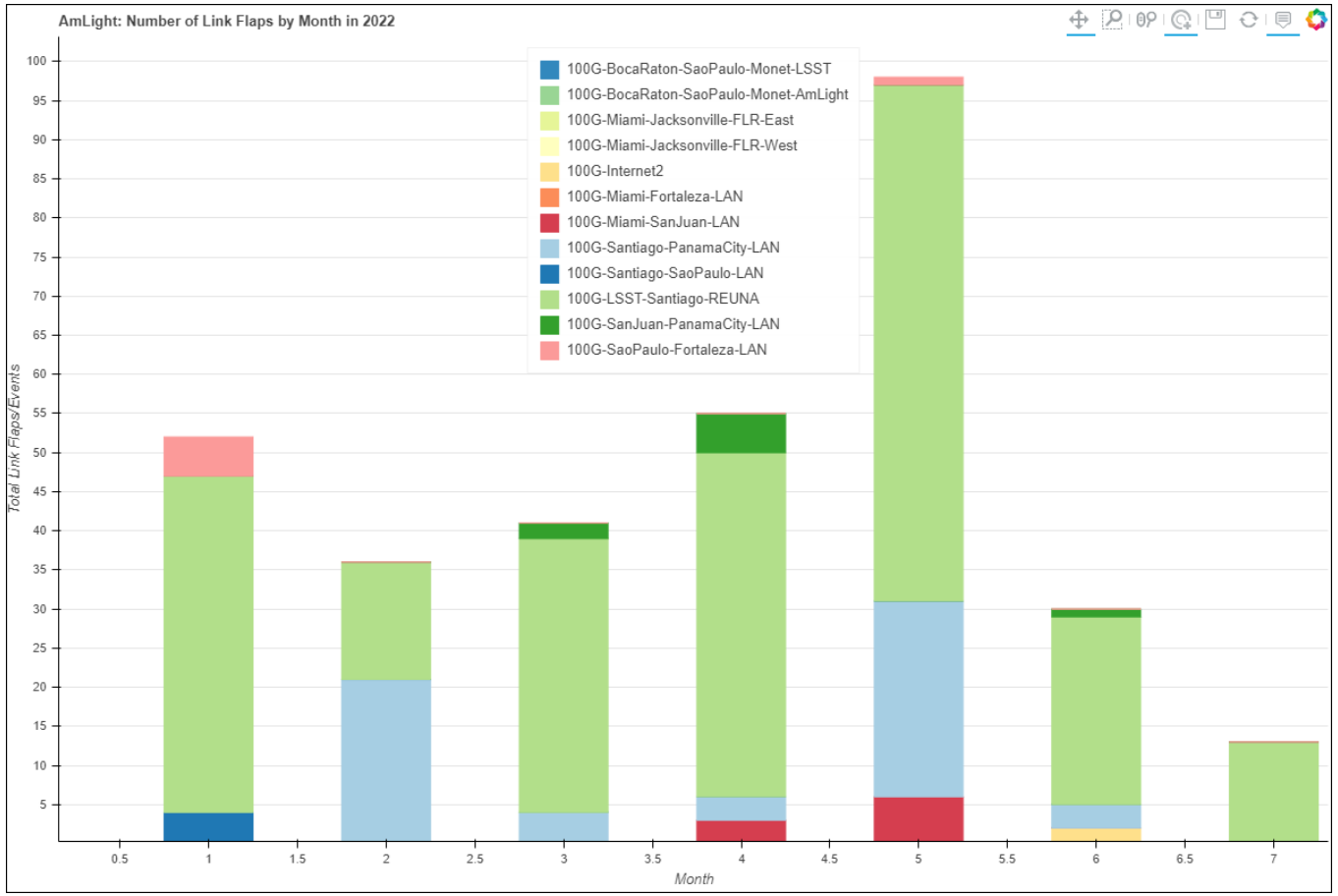
- Erros na entrada da interface et-0/0/0.





Analisando Flaps de Interfaces: Syslog

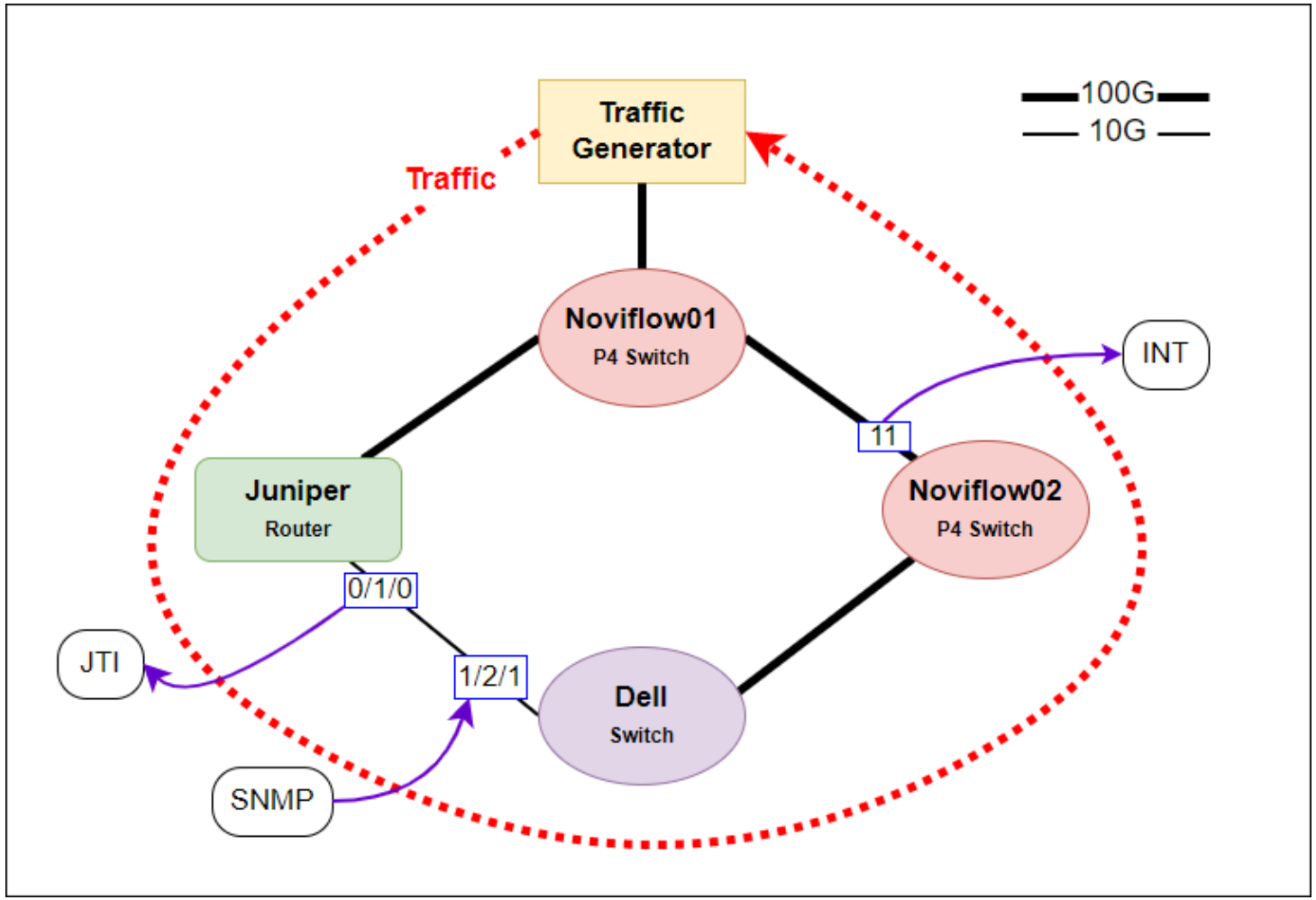
- Gráfico gerado via Bokeh com a análise do syslog dos equipamentos de rede.



AmLight ExP
Americas Lightpaths Express & Protect

Simulações no ambiente de produção…

Demo Setup

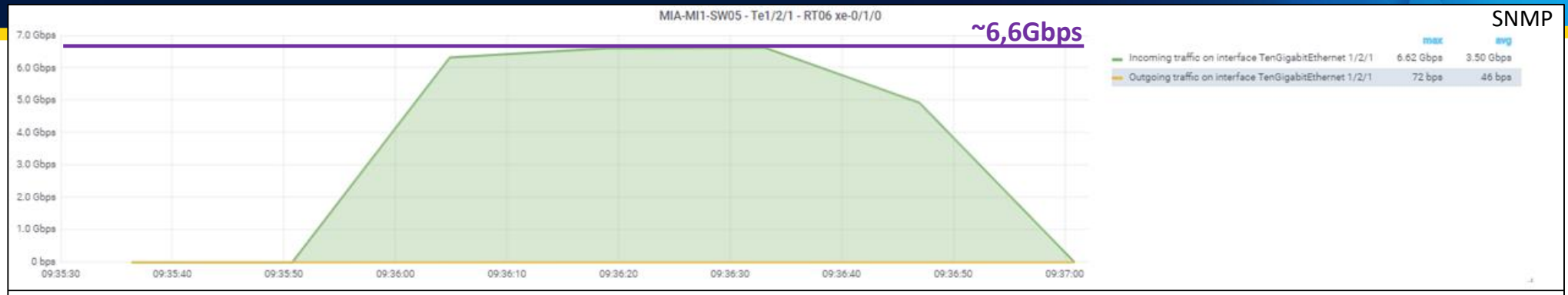


- Gerador de Tráfego EXFO
- Dell (Switch OpenFlow) = Polling SNMP habilitado a cada **14s** (valor mínimo possível do equipamento).
- Juniper (Roteador) = JTI habilitado enviando telemetria a cada **2s**.
- 2x Noviflow (Switch P4 – Data Plane programável) = INT habilitado para todos os pacotes, **real-time**. Visualização do Grafana a cada **500ms**.
- Todos os gráficos da demo foram retirados do Grafana.

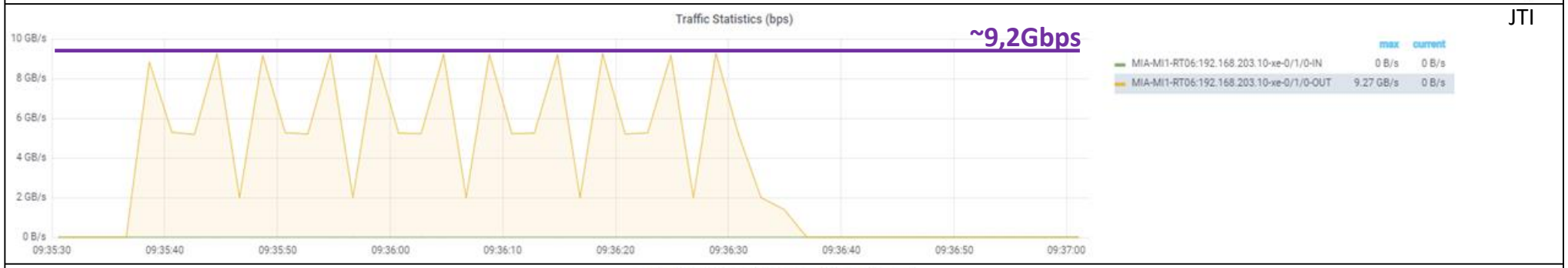
Analisando Bursts: SNMP x JTI x INT [Teste 1]

- Duração: 1 min.
- 2 Streams: Contínuo e Burst.
- Tráfego contínuo: 2Gbps.
- Burst: 11 bursts de 10Gbps.
- Duração de cada burst: 2,5s.
- Intervalo entre bursts: 2,5s.

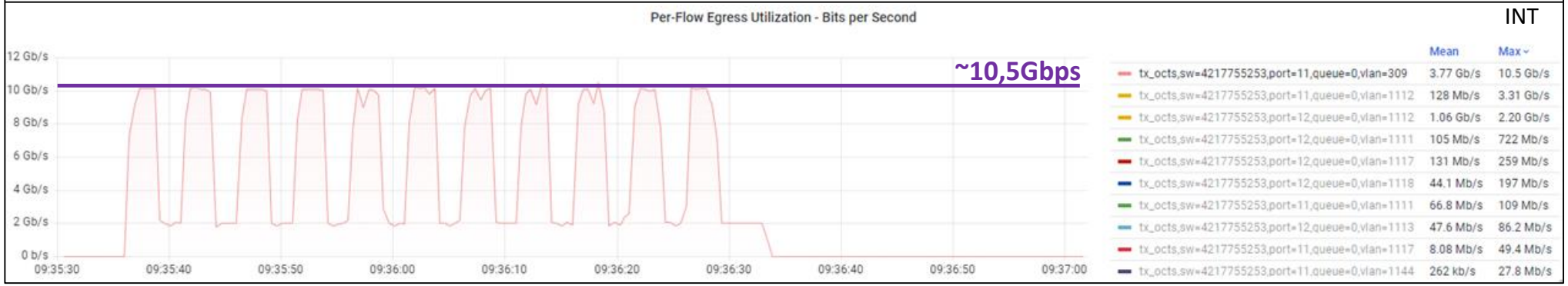
SNMP



JTI



INT



Analisando Bursts: SNMP x JTI x INT [Teste 1]

- Duração: 1 min.
- 2 Streams: Contínuo e Burst.
- Tráfego contínuo: 2Gbps.
- Burst: 11 bursts de 10Gbps.
- Duração de cada burst: 2,5s.
- Intervalo entre bursts: 2,5s.

Resultados do Gerador de Tráfego

Stream 1

	Average	Minimum	Maximum
Throughput (Gbit/s)	1.6017	0.0000	2.1909
Jitter (ms)	0.00185	< 0.00001	0.03606
Latency (ms)	29.93274	0.02690	95.46404
	Seconds	**Count**	**Rate**
Frame Loss	9	311669	1.9E-01
Out-of-Sequence	0	0	0.0E00

Stream 2

	Average	Minimum	Maximum
Throughput (Gbit/s)	4.3947	0.0000	10.0000
Jitter (ms)	0.00059	< 0.00001	95.43156
Latency (ms)	85.55913	0.02702	95.46338
	Seconds	**Count**	**Rate**
Frame Loss	22	305053	8.0E-02
Out-of-Sequence	0	0	0.0E00

Analisando Bursts: SNMP x JTI x INT [Teste 2]

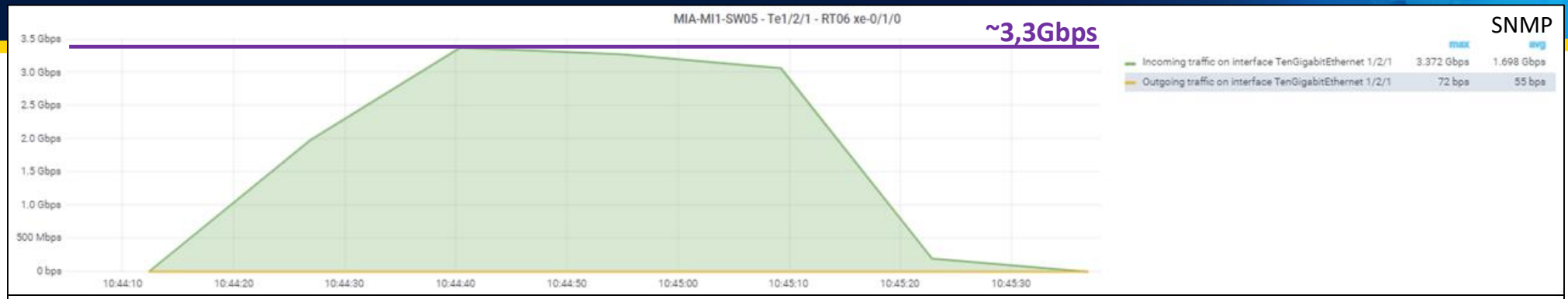
- Duração: 1 min.
- 2 Streams: Contínuo e Burst.
- Tráfego contínuo: 2Gbps.
- Burst: 11 bursts de 10Gbps.
- Duração de cada burst: 1s.
- Intervalo entre bursts: 4s.

AmLight ExP
Americas Lightpaths Express & Protect

Analisando Bursts: SNMP x JTI x INT [Teste 3]

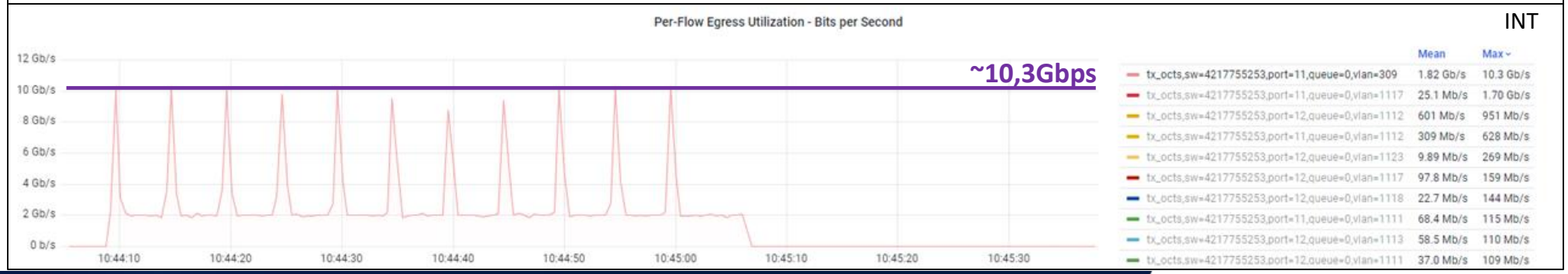
- Duração: 1 min.
- 2 Streams: Contínuo e Burst.
- Tráfego contínuo: 2Gbps.
- Burst: 11 bursts de 10Gbps.
- Duração de cada burst: 500ms.
- Intervalo entre bursts: 4,5s.

SNMP



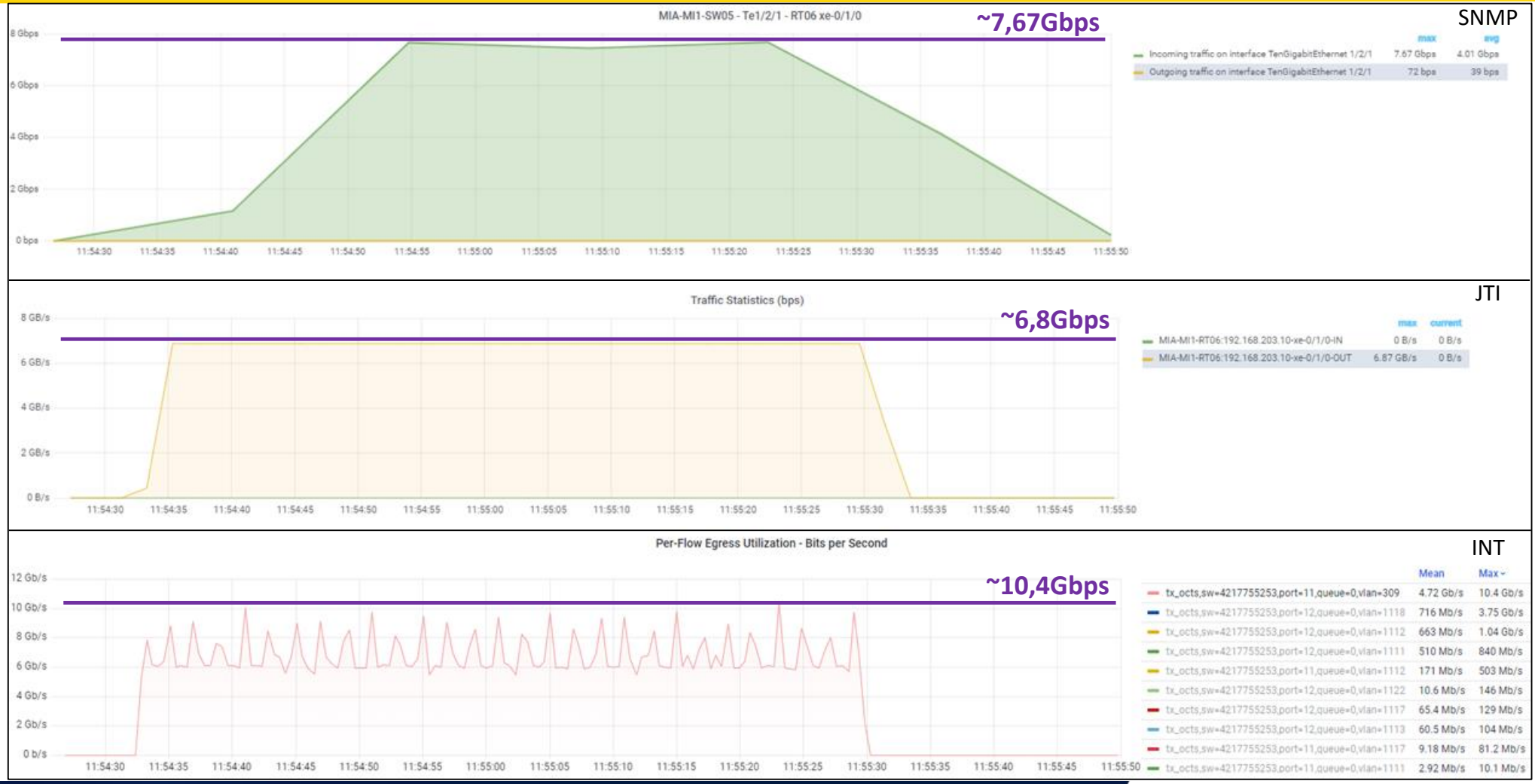
JTI

INT



Analisando Bursts: SNMP x JTI x INT [Teste 4]

- Duração: 1 min.
- 2 Streams: Contínuo e Burst.
- Tráfego contínuo: 6Gbps.
- Burst: 30 bursts de 10Gbps.
- Duração de cada burst: 200ms.
- Intervalo entre bursts: 1,8s.



AmLight ExP
Americas Lightpaths Express & Protect

Ok, muitas ferramentas…
E agora? Como usar todas?

Futuro: Redes Autonômicas

- A Autonomic Networking Architecture (ANA) cria as definições e metas de design para uma rede autogerenciada.
- Padronizado via Internet Engineering Task Force (IETF) RFC 7575.
- O autogerenciamento é composto por várias propriedade “self-x”:
  - **Self-configuration**: Funções autonômicas não necessitam de configuração, seja por um administrador ou um sistema de gerência. São configuradas por si mesmas baseando-se em conhecimentos próprios.
  - **Self-healing**: Funções autonômicas adaptam-se por si mesmas à mudanças no ambiente e recuperam-se automaticamente.
  - **Self-optimizing**: Funções autonômicas determinam automaticamente formas de otimizar seu comportamento em relação ao um conjunto de objetivos bem definidos.
  - **Self-protection**: Funções autonômicas protegem-se automaticamente contra potenciais ataques.

Futuro: Redes Autonômicas – Proposta da AmLight

Application

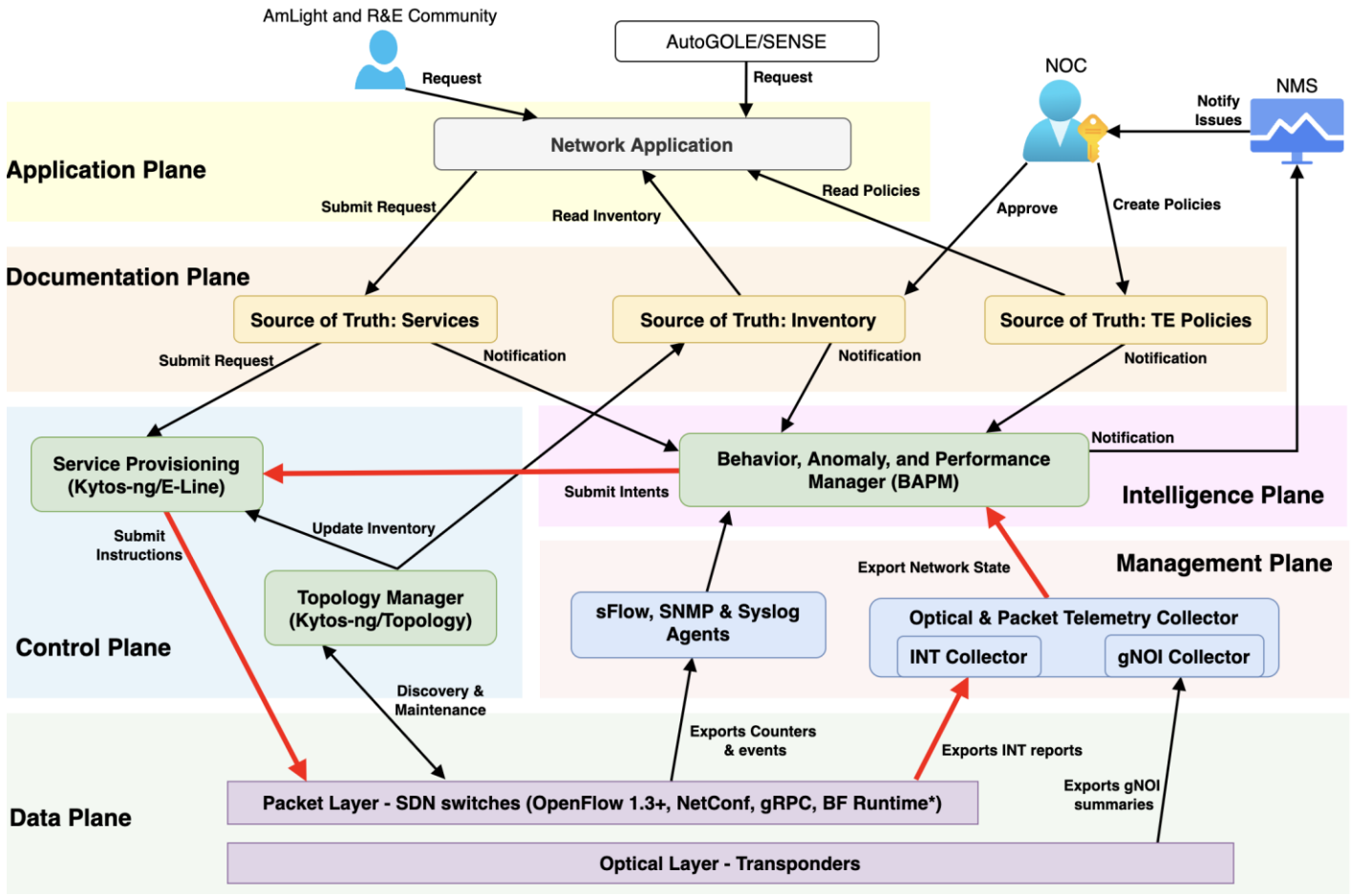
Documentation Plane

Control Plane

Intelligence Plane

Management Plane

Data Plane



Comentários Finais

- Monitorar todos os pacotes é possível com o In-Band Network Telemetry!
- O INT e o JTI aumentaram a visibilidade da rede além das nossas expectativas.
- A combinação de todas as ferramentas/técnicas possibilita a AmLight acompanhar qualquer problema de performance ou reclamação dos usuários.
- Combinar o INT com ferramentas de Machine Learning habilitará a AmLight a criar tendências confiáveis e avançar para uma rede orquestrada autonômica criando uma camada de inteligência adicional ao SDN.
- Ferramentas e técnicas legadas continuam sendo muito importantes para determinadas funções!

Obrigada! / Perguntas? / Comentários?

Como Obter o Melhor do Monitoramento via Syslog, SNMP, Flows e Telemetria? Caso de uso da AmLight

Renata Frez - RNP/AmLight <renata@amlight.net>