BENOCS

Performance measurement goes Flow

HOW CORRELATION OF PERFORMANCE- AND FLOW-DATA CAN PROVIDE FULL PROBLEM-CONTEXT

Why combining probe- and flow data?

- Probe based performance monitoring can only display a small focused network problem
- Extrapolating from the probe-problem to the likely fallout-perimeter is required to assess the scope of the problem
- Flow-data can support extrapolation task

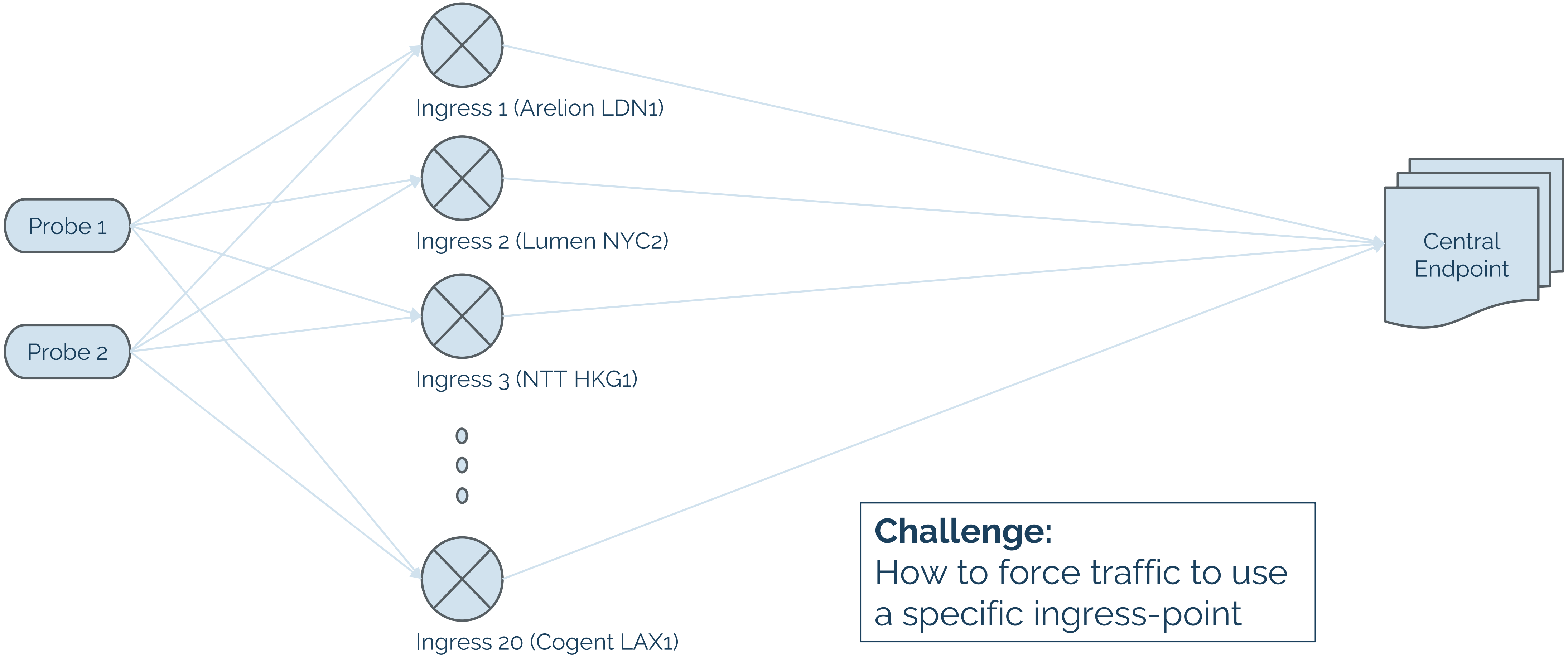
Challenge 1: operate probes

Target: monitor 20 (transit) ingress points

- Solution 1: install 50 probes and hope that each ingress point gets used at least 1x
  (€€€ - costly and unlikely to cover all ingress points)

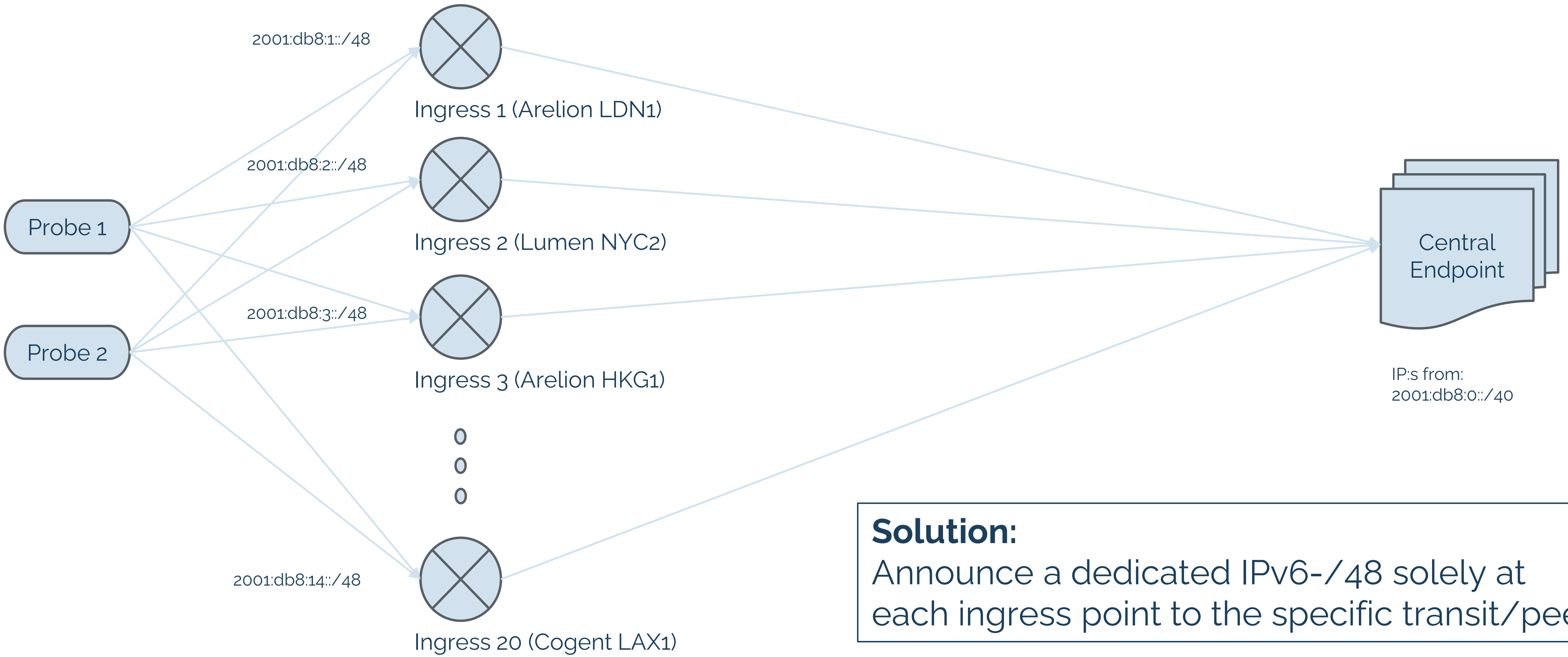
- Solution 2: install 2 probes and announce target-host with dedicated IPv6-/48:
  (efficient, requires complex config)

Challenge 1: Solution 2



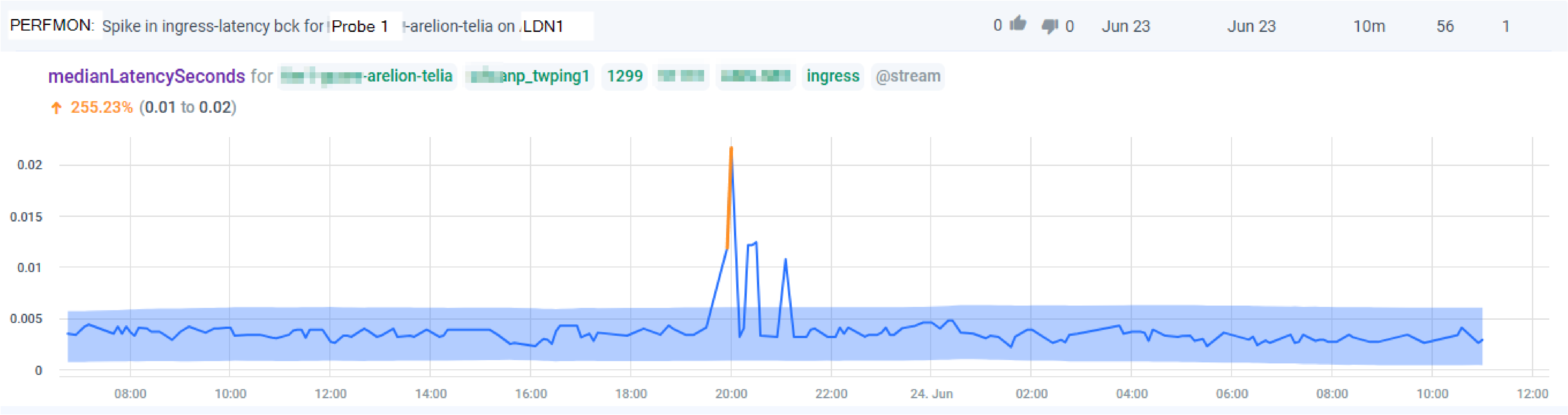
Challenge:
How to force traffic to use a specific ingress-point

Challenge 1: Solution 2



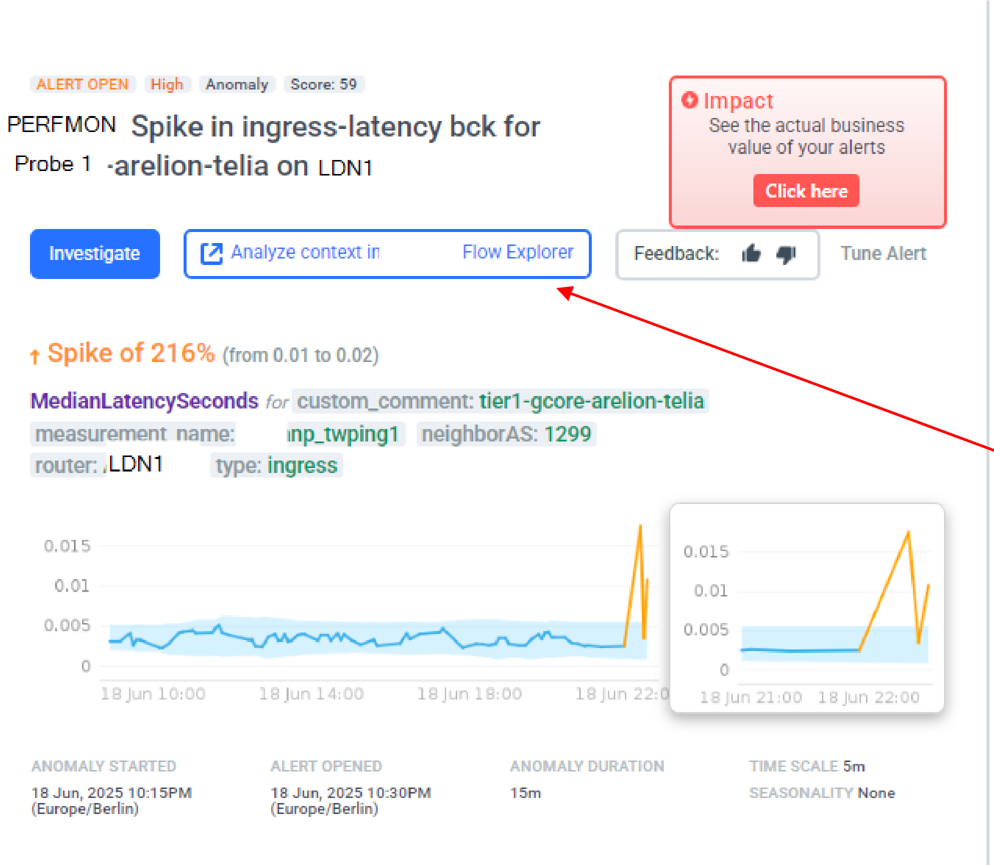
Solution:
Announce a dedicated IPv6-/48 solely at each ingress point to the specific transit/peer

Challenge 2: Alert performance degradation



Solution:
Use generic alert system with
a) thresholds (good enough)
b) anomaly detection (reduces noise)

Challenge 3: Correlate with flow

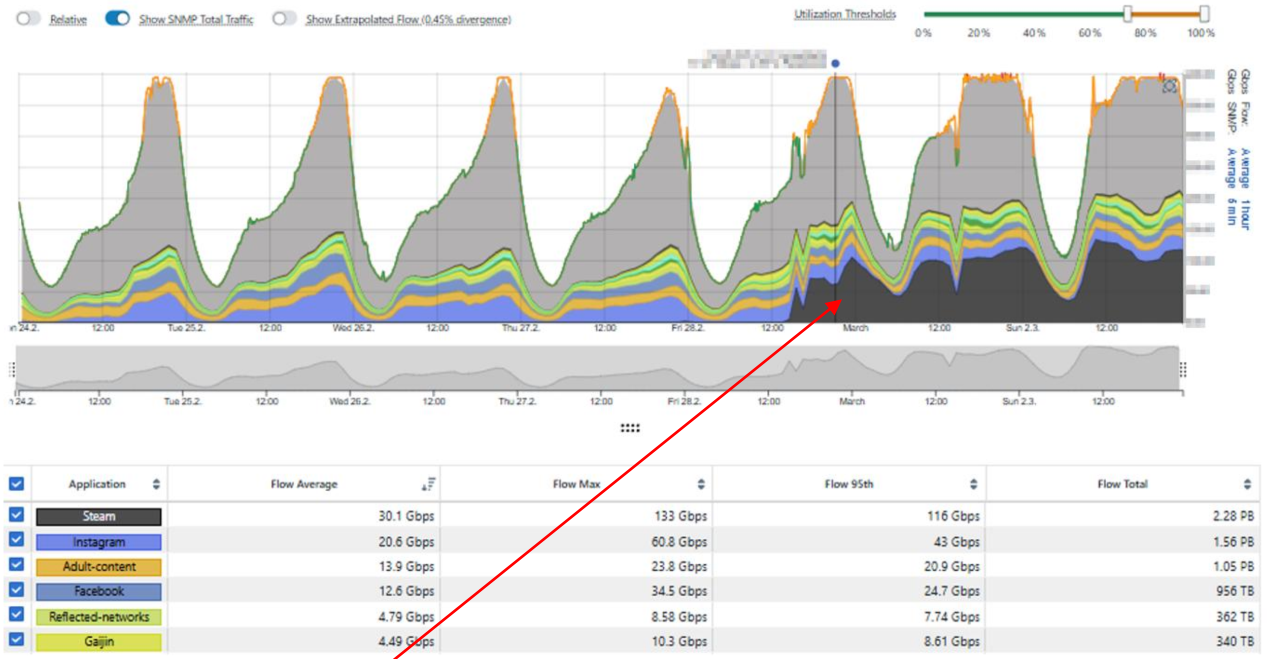


Peer and ingress-router are known from the IPv6-prefix

- That gives as the key identifiers to correlate with flow data
- All traffic of the alerted ingress-point can be displayed to show full context

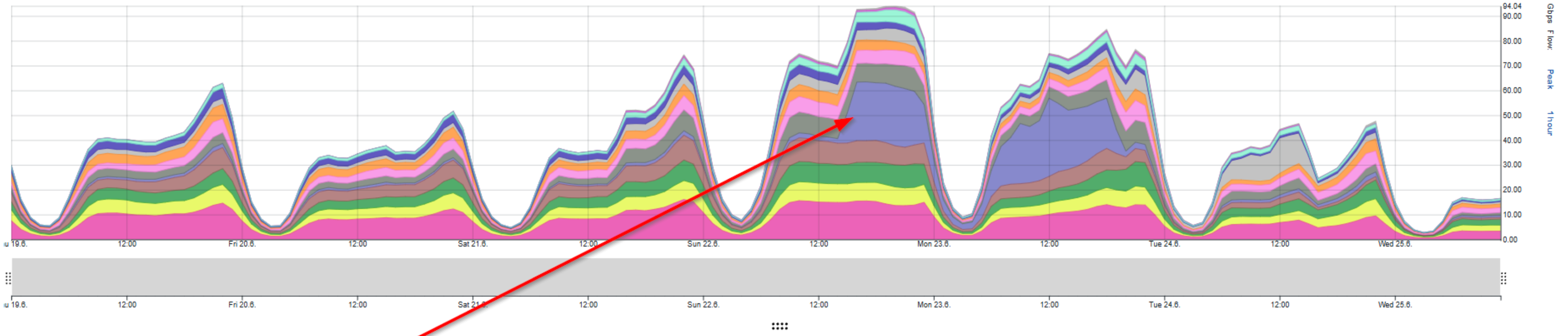
https://xyz.com/asflows?asFilters=%7B%22HND%22%3A%5B%22**1299**%22%5D%2C%22INROUTER%22%3A%5B%22**LDN1**%22%5D%7D&customDimension=%22AS_APPLICATION%2CAS_SRC_INGRESS%2CAS_HND_INGRESS%2CROUTER_IN_INGRESS%2CROUTER_OUT_INGRESS%2CAS_NXT_INGRESS%2CAS_DST_INGRESS%22&dateRange=LAST_7_DAYS&disaggregations=%7B%7D&tagAggregations=%5B%7B%22dimension%22%3A%22ROUTER_OUT_INGRESS%22%2C%22id%22%3A4%7D%5D&tags=%5B%5D&tsDimension=AS_APPLICATION

Challenge 3: Correlate with flow / Application



Traffic on the affected ingress-point was jammed by Steam/Valve traffic (game release)

Challenge 3: Correlate with flow / Regions



Router	Name	Flow Average	Flow Max	Flow 95th	Flow Total
Region 1		7.87 Gbps	16.1 Gbps	15 Gbps	552 TB
Region 2		4.14 Gbps	7.77 Gbps	7.54 Gbps	291 TB
Region 3		4.11 Gbps	9.88 Gbps	8.27 Gbps	288 TB
Region 4		4.09 Gbps	9.98 Gbps	8.86 Gbps	287 TB
Region 5		4.07 Gbps	31.5 Gbps	23.7 Gbps	286 TB
Region 6		3.37 Gbps	9.44 Gbps	8.11 Gbps	237 TB
Region 7		3.03 Gbps	7.97 Gbps	6.07 Gbps	213 TB
Region 8		2.57 Gbps	5.79 Gbps	4.61 Gbps	181 TB
Region 9		2.56 Gbps	14.3 Gbps	8.13 Gbps	180 TB
Region 10		1.74 Gbps	4.06 Gbps	3.49 Gbps	122 TB
Region 11		1.51 Gbps	5.36 Gbps	4.01 Gbps	106 TB
RoW		221 Mbps	964 Mbps	750 Mbps	15.5 TB
Others	.	227 Mbps	949 Mbps	698 Mbps	16 TB
Total		39.5 Gbps		99.3 Gbps	2.77 PB

Additional traffic on the affected ingress-point was mainly targeted at Region 5

Thank you

Questions?

pgyoergy@benocs.com