

Large Networks Monitoring

Luca Deri <deri@ntop.org>, @lucaderi

Goal of This Presentation

- Explain challenges in monitoring large networks.
- Introduce open source AS traffic observability.
- Present the integration work on BGP/BMP.
- Show you that you will now be able to monitor your AS traffic without costly monthly subscriptions to cloud-based products.

Do I "Own" the Monitored Traffic ?

- Yes

You are monitoring your services (e.g. email. Web etc) so the traffic hitting your servers belongs to you. You can do DPI and store detailed IP information.

Example: service providers, company, individuals.

- No

I provide Internet connectivity to my community and my customers. My goal is to keep the network healthy, I can't store/visualize detailed information.

Example: IXP Network Operators.

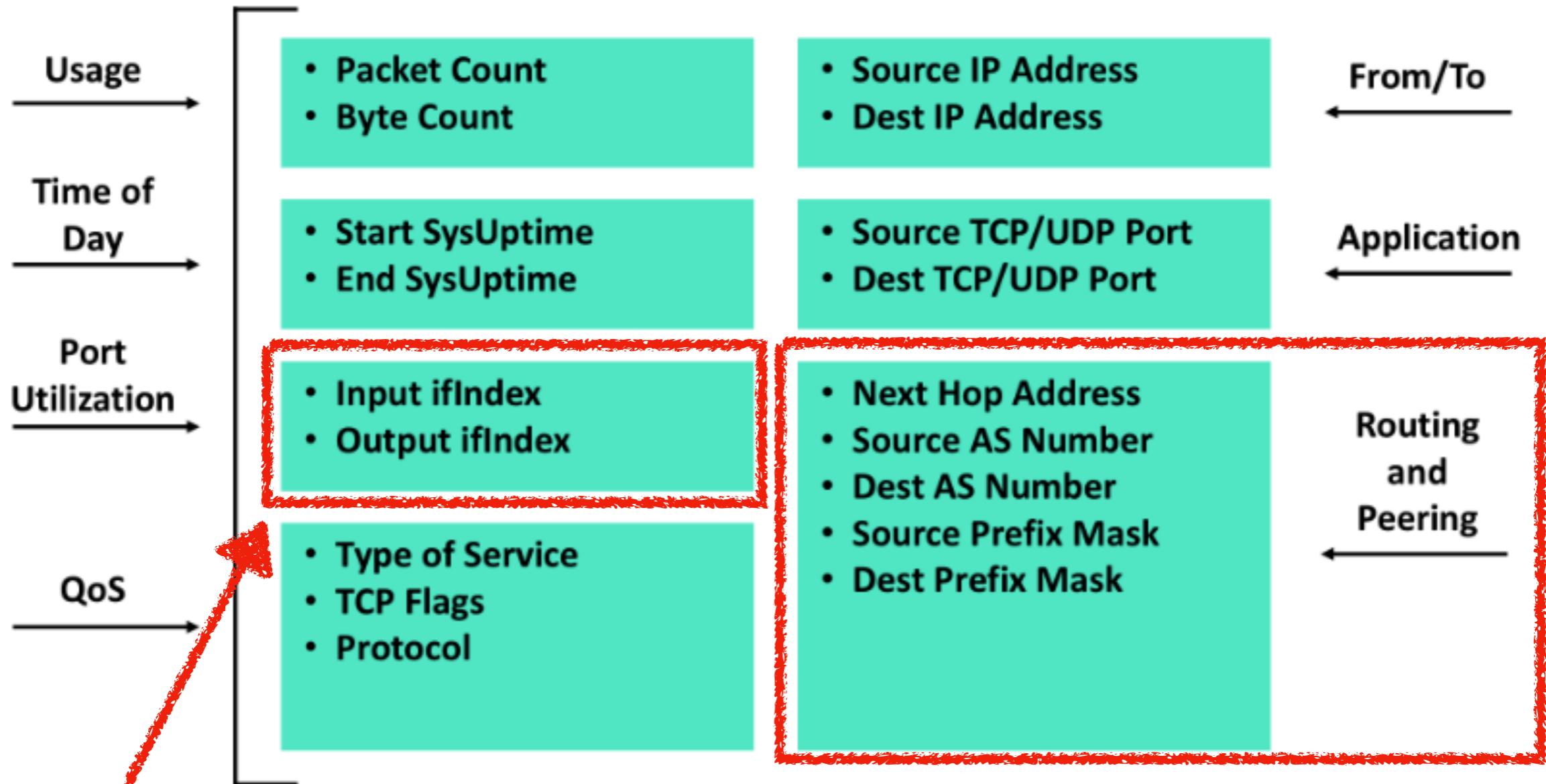


Our use case

- Mixed

You have a large enterprise where only on selected networks you do DPI and the rest is flow-based.

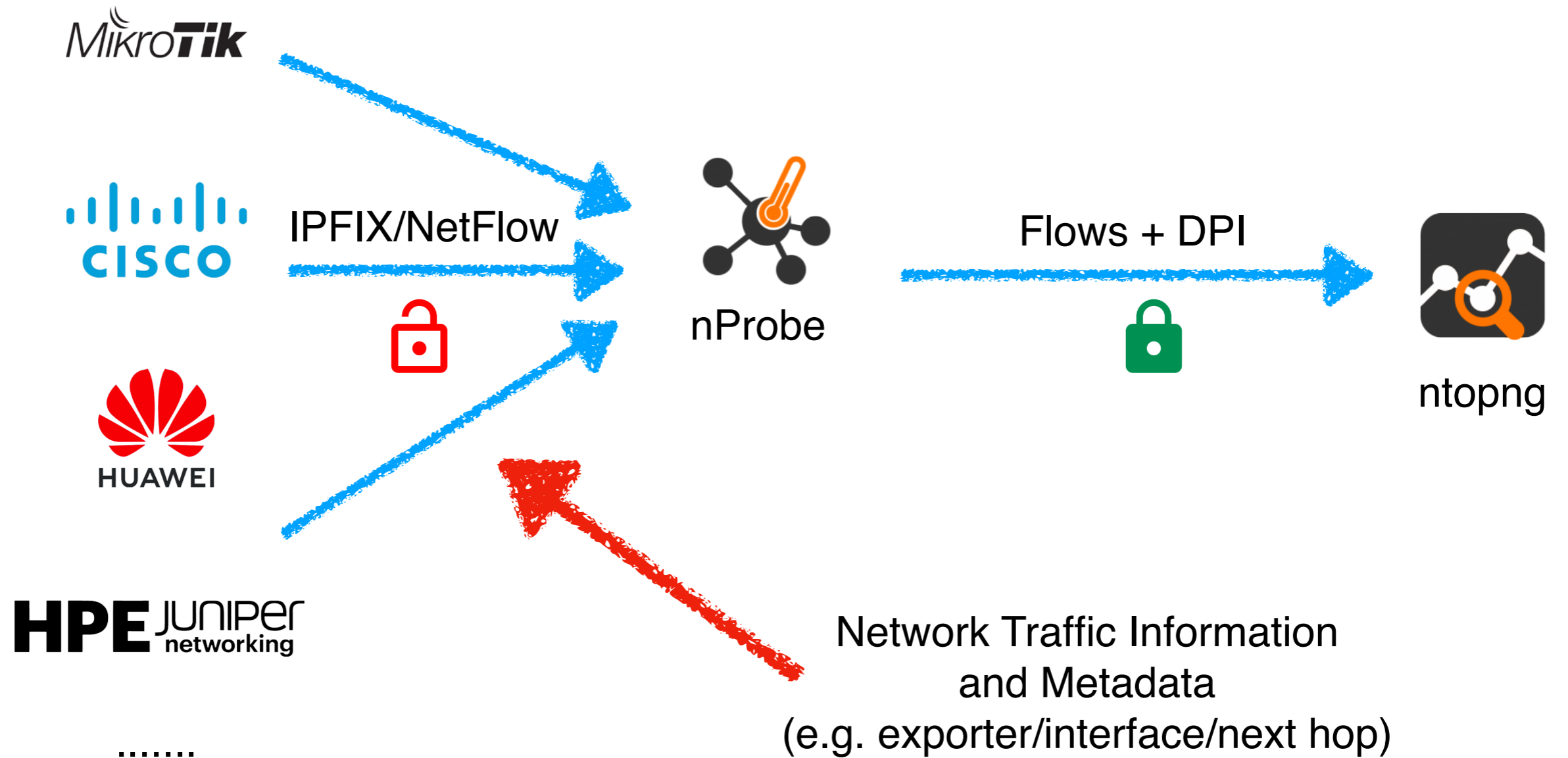
What's Inside a Flow ?



Flow Exporter Information

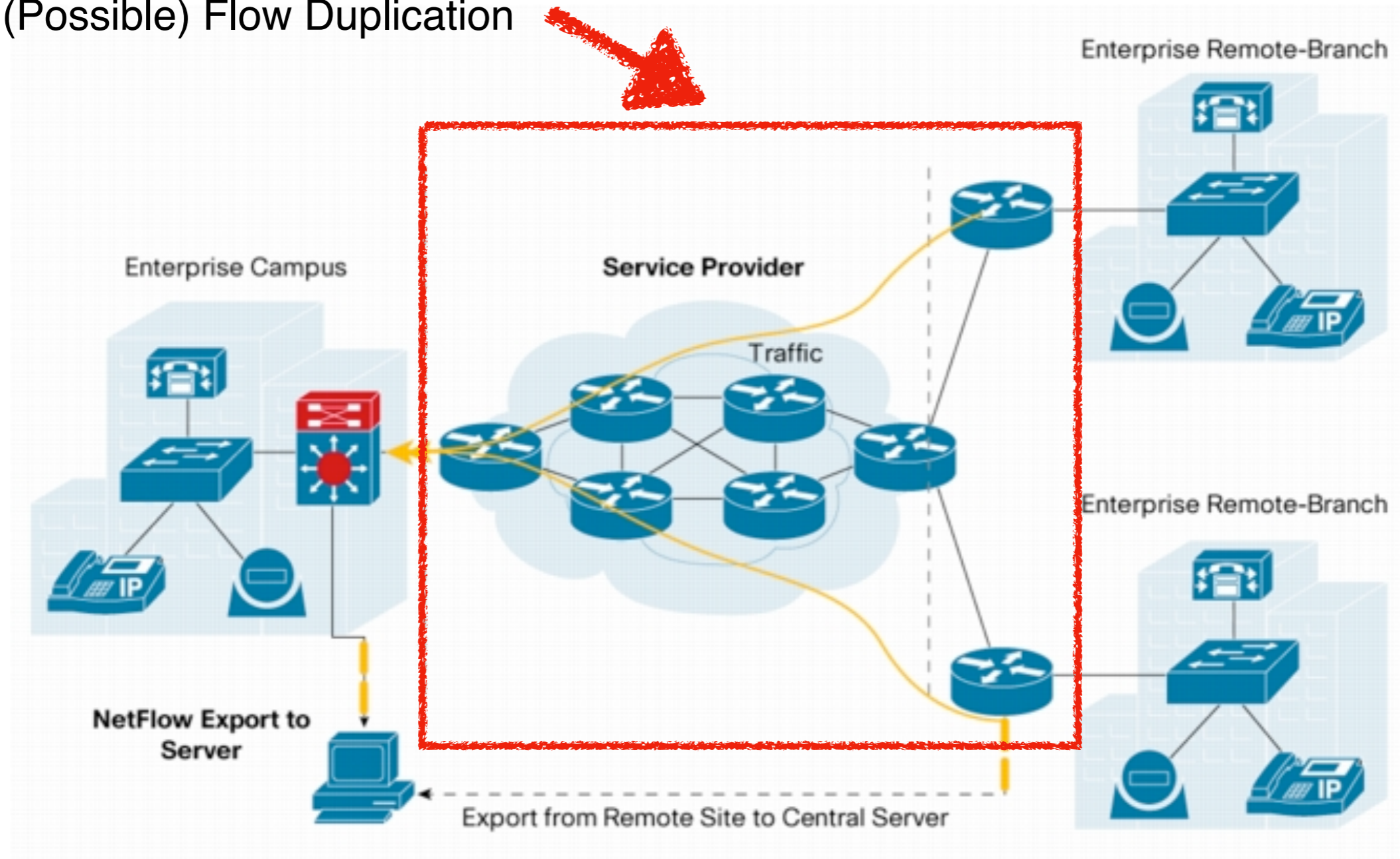


Flow Collection: nProbe and ntopng



Flow Collection in Large Networks

(Possible) Flow Duplication



Flow Duplication: Good or Bad? [1/3]

- What is duplicated flow?
 - Same time window
 - Same 5-tuple (proto, IP/Port src/dst)
 - Different flow exporter.
- Flow duplication can create issues when accounting traffic as the same flow can be accounted once, twice... depending on the network.

Flow Duplication: Good or Bad? [2/3]

The screenshot shows the ntopng interface with a sidebar on the left containing navigation options: Dashboard, Monitoring, Alerts, Views (highlighted), Flow Exp., Maps, Interface, Policies, Settings, Developer, and Help. The main area displays a 'Live Flows' aggregation view for the host 'tcp://127.0.0.1:1234'. It shows a traffic graph and summary statistics: 950.60 Kbps / 931.20 Mbps, 5.3K (1.2K) flows, and 65.5K (16.6K) bytes. Below the graph is a filter bar with dropdowns for Host, Protocol, Application, Status, Traffic Type, Host Pools, and Source AS, all set to 'All'. A table below lists flow actions with columns: Actions, Actual Thpt, Total, and Info. A red box highlights the 'Info' column for several rows, showing '4 Bidir. Exp. Internet eXc...' and '3 Bidir. Exp. Internet eXc...'.

Actions	Actual Thpt	Total ...	Info
[icon]	43.50 Kbps ↓	12.19 GB	4 Bidir. Exp. Internet eXc...
[icon]	549.35 Kbps...	11.93 GB	3 Bidir. Exp. Internet eXc...
[icon]	214.44 Kbps ↓	10.15 GB	5 Bidir. Exp. Transit
[icon]	11.55 Mbps ↑	9.30 GB	3 Bidir. Exp. Internet eXc...
[icon]	42.73 Mbps ↑	7.72 GB	5 Bidir. Exp. Transit
[icon]	12.56 Mbps ↑	7.70 GB	
[icon]	80.89 Kbps ↓	6.35 GB	3 Bidir. Exp. Internet eXc...
[icon]	783.05 Kbps ↓	5.86 GB	6 Bidir. Exp. Internet eXc...
[icon]	1.54 Mbps ↑	4.71 GB	3 Bidir. Exp. Internet eXc...
[icon]	7.47 Mbps ↑	4.07 GB	4 Bidir. Exp. Internet eXc...

Flow Duplication: Good or Bad? [3/3]

Exporters Information	Flow Exporter / Next Hop	Input Interface / Output Interface
	[10.255.255.202] → 10.20.2.10	VLAN1001-edge-01.core-A → VLAN2002-ac101.ac (internal_interface)
	[10.255.255.202] → 10.20.2.25 Return Path	VLAN2002-ac101.ac (internal_interface) → VLAN1001-edge-01.core-A
	[10.255.255.31] → 10.20.2.9 Return Path	pppoe-B-KINEMAXMON → VLAN2002-edge-02.core (internal_interface)
	[10.255.255.31] → 0.0.0.0	VLAN2002-edge-02.core (internal_interface) → pppoe-B-KINEMAXMON
	[10.255.255.201] → 10.20.2.26	VLAN100-IPT-FT (transit) → VLAN1001-edge-02.core-A

Flow Deduplication: nProbe vs ntopng

ntopng

ZMQ Statistics				
Collected Flows 📈	817,147,795 [12.7 Kfps] ↑	Discarded Flows (by ntopng) 📉	400 [0.0 %] —	
Collected ZMQ Messages 📈	136,254,424 ↑	Dropped ZMQ Messages 📉	1,519 [0.0 %] —	Avg Flows/Msg: 6
Interface Updates	18,127 ↑	Counter Updates	0 —	
Traffic Statistics				
Traffic Anomalies 📈	Local Hosts Anomalies	22,241 —	Remote Hosts Anomalies	23,117 ↑
Deduplicated Flows 📈	407,756,411 [49.9 %] ↑			

nProbe

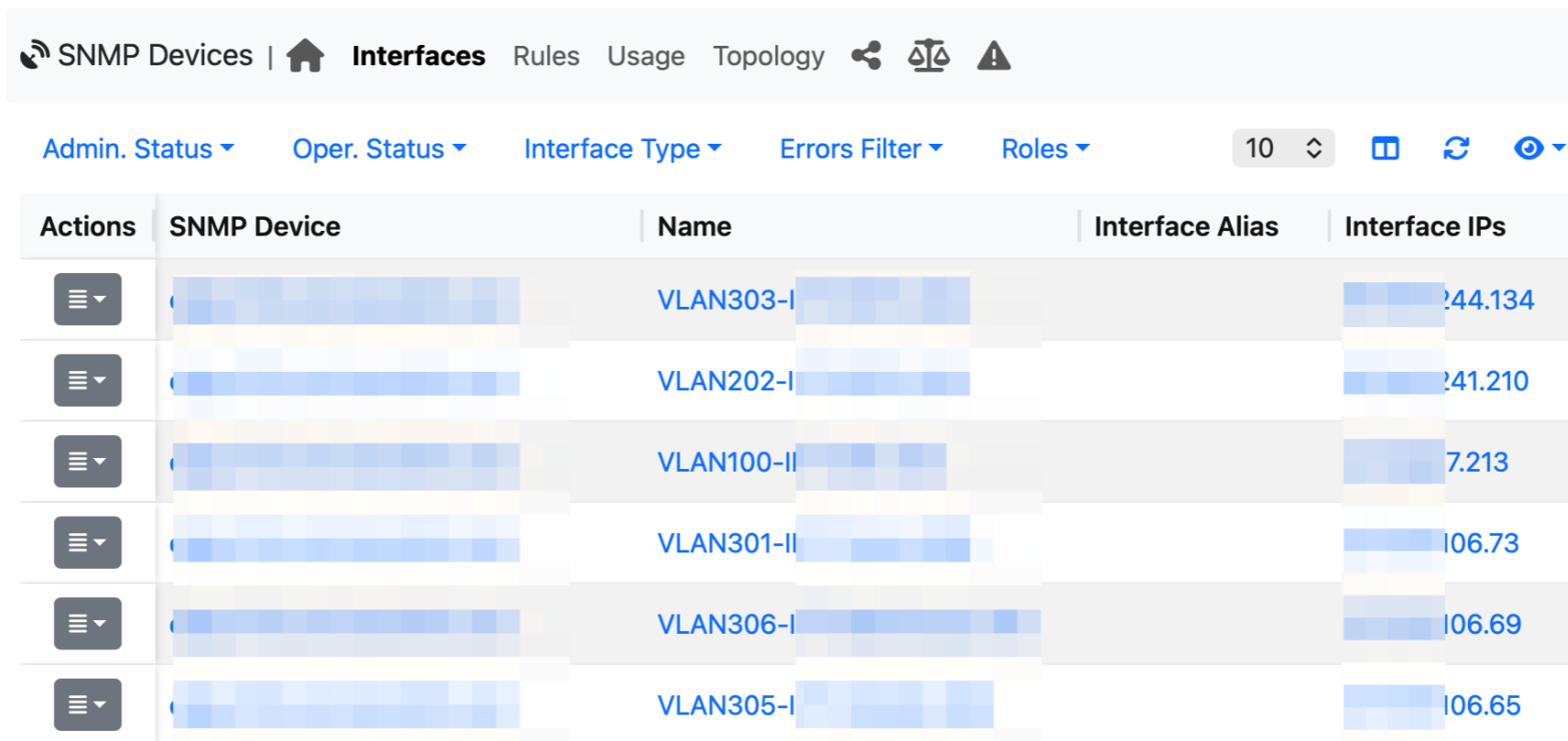
`--flow-collection-deduplication` | Discards duplicated flows (i.e. flows with the same key sent by two different flow exporter IP)

Best Practices

- Most people can deploy monitoring devices at the edge of the network:
 - No duplication
 - Visibility of north/south traffic.
- You can also monitor internal routers if you want to study the traffic trajectory but this can put significant load on large networks.
- In short: it depends on your monitoring goals and your use case.

Handling Exporters IPs

- Flow exporters often export flows from multiple interfaces hence with multiple IP addresses.
- In order to bind all IPs to the same exporter, we have enhanced SNMP to poll IPv4/v6 addresses.



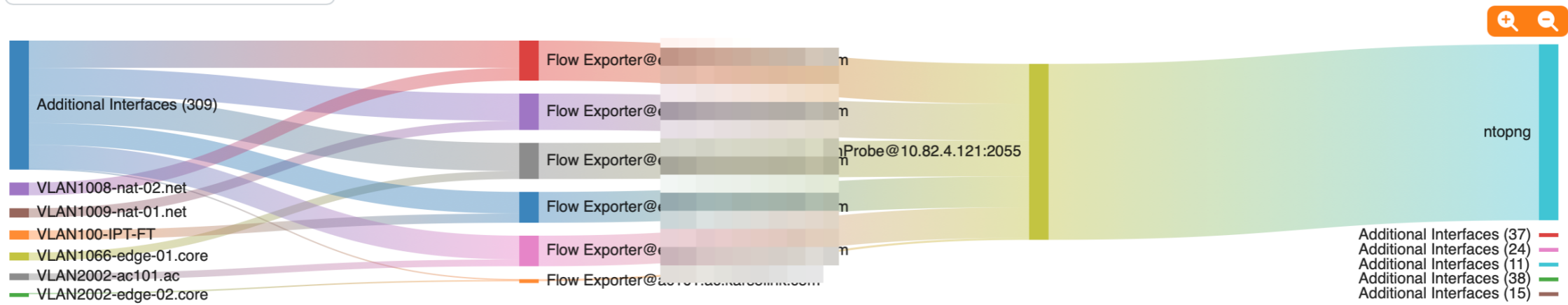
The screenshot shows the ntopng web interface. At the top, there is a navigation bar with 'SNMP Devices' selected, and other options like 'Interfaces', 'Rules', 'Usage', and 'Topology'. Below the navigation bar, there are filter options for 'Admin. Status', 'Oper. Status', 'Interface Type', 'Errors Filter', and 'Roles'. A table displays the following data:

Actions	SNMP Device	Name	Interface Alias	Interface IPs
⋮	[blurred]	VLAN303-I	[blurred]	194.134
⋮	[blurred]	VLAN202-I	[blurred]	194.210
⋮	[blurred]	VLAN100-II	[blurred]	197.213
⋮	[blurred]	VLAN301-II	[blurred]	1906.73
⋮	[blurred]	VLAN306-I	[blurred]	1906.69
⋮	[blurred]	VLAN305-I	[blurred]	1906.65

nProbe vs Exporters

Criteria:

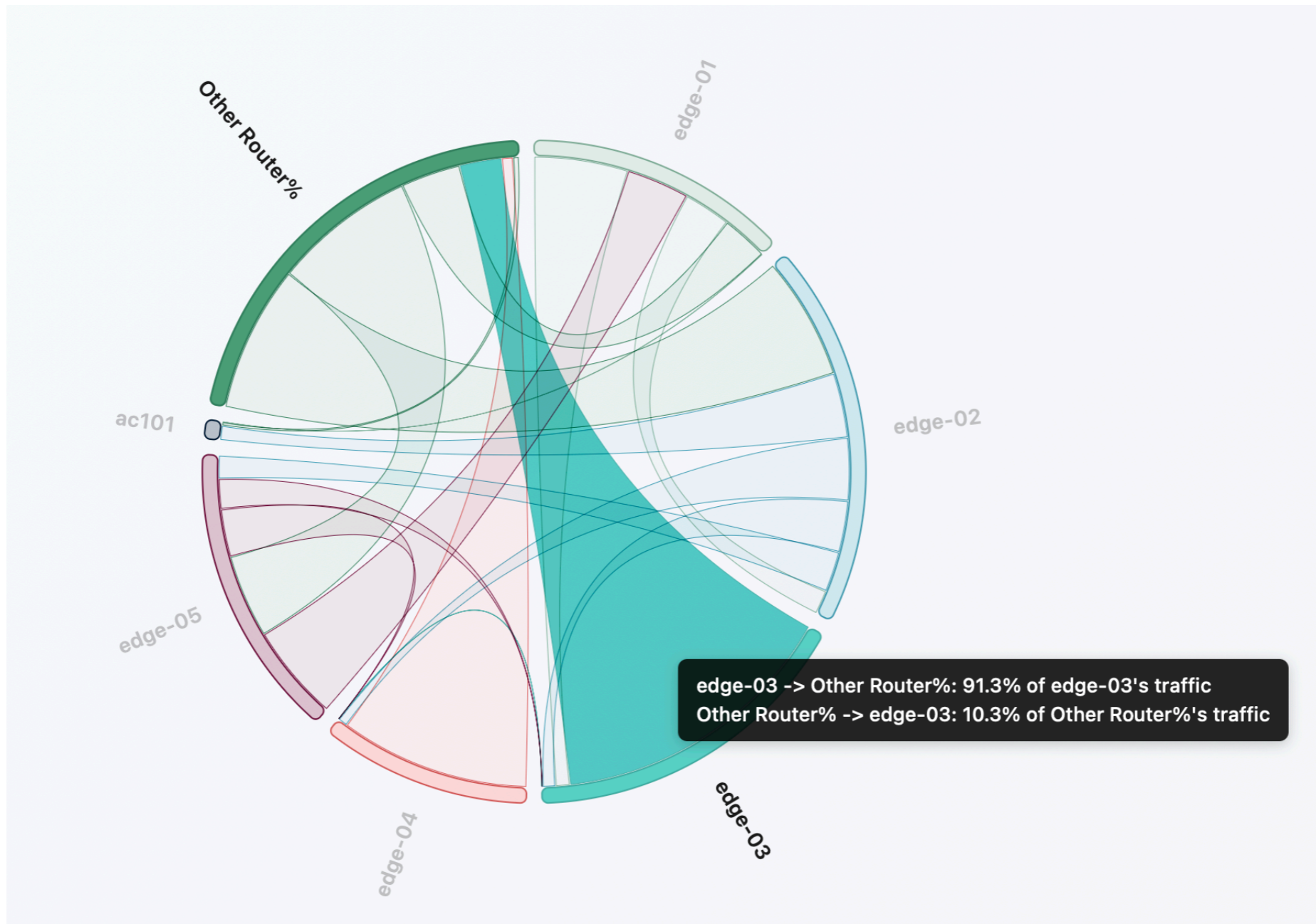
Total Flows



10 [grid] [refresh] [eye] Search:

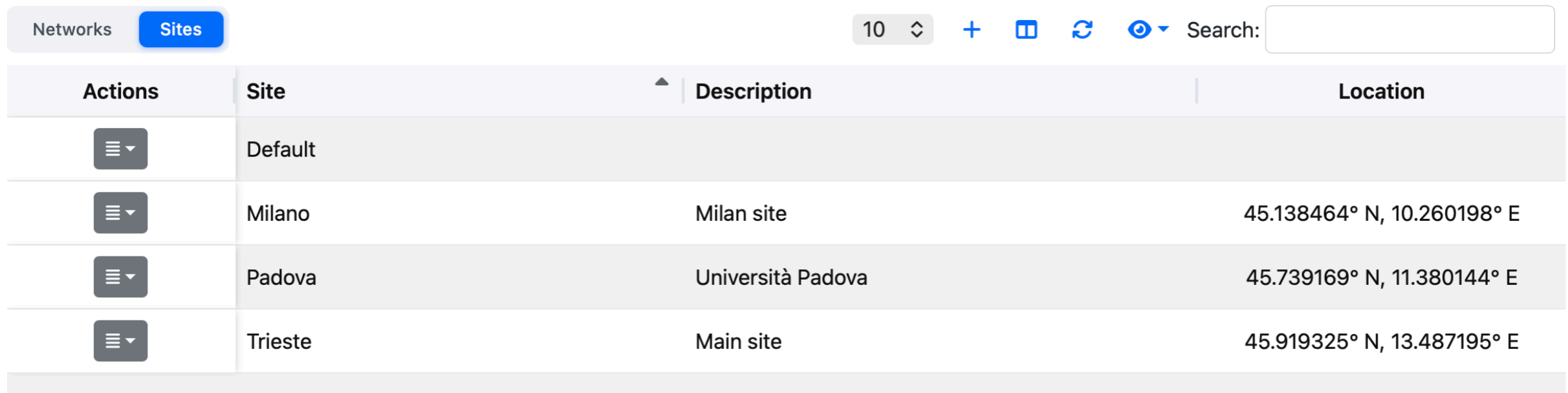
Actions	Flow Exporter	IfName (ntopng)	S...	Flow Exporter IP	Export Type	Interfaces	Last Flow Col
[dropdown]	[blurred]	tcp://127.0.0.1:1234		10.255.255.31	NetFlow/IPFIX (Port: 20...	310	00:04 ago
[dropdown]	[blurred]	tcp://127.0.0.1:1234		10.255.255.203	NetFlow/IPFIX (Port: 20...	38	00:04 ago
[dropdown]	[blurred]	tcp://127.0.0.1:1234		10.255.255.205	NetFlow/IPFIX (Port: 20...	25	00:04 ago
[dropdown]	[blurred]	tcp://127.0.0.1:1234		10.255.255.201	NetFlow/IPFIX (Port: 20...	12	00:04 ago
[dropdown]	[blurred]	tcp://127.0.0.1:1234		10.255.255.204	NetFlow/IPFIX (Port: 20...	39	00:04 ago
[dropdown]	[blurred]	tcp://127.0.0.1:1234		10.255.255.202	NetFlow/IPFIX (Port: 20...	16	00:04 ago

Combining Exporters with Flow NextHop







Networks vs Sites [1/2]

- On large networks, IPs might be physically deployed across multiple locations.
- Sites allow you to cluster IPs across locations.



The screenshot shows a web interface with a 'Sites' tab selected. At the top, there are navigation buttons for 'Networks' and 'Sites', a page size selector set to '10', and a search bar. Below the navigation is a table with four columns: 'Actions', 'Site', 'Description', and 'Location'. The table contains four rows of site data.

Actions	Site	Description	Location
	Default		
	Milano	Milan site	45.138464° N, 10.260198° E
	Padova	Università Padova	45.739169° N, 11.380144° E
	Trieste	Main site	45.919325° N, 13.487195° E

Networks vs Sites [2/2]

Networks | Networks

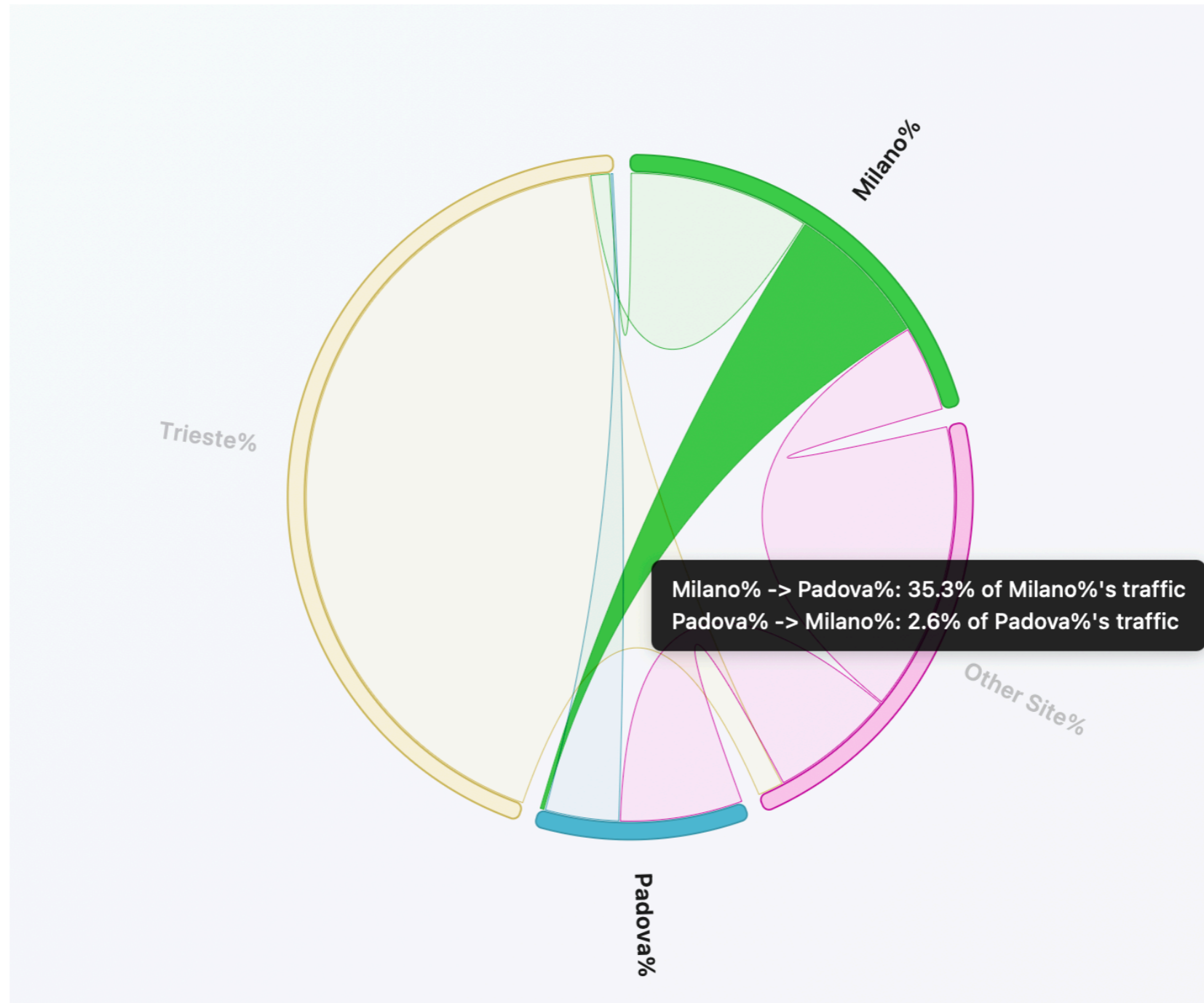
Networks Score

Networks Sites

10 [Refresh] [Filter] [Search]

Actions	Network Name	Site	Hosts	Score	Host/Score ...	Alerted Fl...	Traffic	Throughput	Traffic
⋮	edge-03 · 10.255.255.0/24	Trieste	1	0	0	0	Sent 55% Rcvd 45%	0.00 bps	163.56 KB
⋮	edge-04 · 10.255.255.0/24	Trieste	1	0	0	0	Sent 44% Rcvd 56%	0.00 bps	260.44 KB
⋮	edge-05 · 10.255.255.0/24	Padova	1	0	0	0	Sent 77% Rcvd 23%	20.34 Kbps	67.09 MB
⋮	ac101 · 10.255.255.0/24	Milano	1	0	0	0	Sent 12% Rcvd 88%	0.00 bps	147.71 KB
⋮	edge-01 · 10.255.255.0/24	Milano	1	0	0	0	Sent 100% Rcvd 0%	0.00 bps	28.49 MB
⋮	edge-02 · 10.255.255.0/24	Milano	1	0	0	0	Sent 100% Rcvd 0%	0.00 bps	20.22 MB
⋮	10.0.0.0/8	Default	1.4 K	379	0	72	Sent 98% Rcvd 2%	1.06 Gbps	5.80 GB

Sites Traffic Distribution



Binding Interfaces to Roles

SNMP Devices / [redacted] | Home Alert [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

Interface Admin Status Toggle interface admin status. Toggle is immediate but actual status shown is refreshed during the next poll.	<input checked="" type="checkbox"/>
Interface Operational Status Change Alerts Toggle alerts generated when an interface operational state changes	<input checked="" type="checkbox"/>
Interface Duplex Status Change Alerts Toggle alerts generated when an interface duplex status changes	<input type="checkbox"/>
Interface Discards/Errors Alerts Toggle alerts generated when the discards or errors counters on an interface increase	<input type="checkbox"/>
Port Role SNMP Interface Port Role	<div style="border: 2px solid red; padding: 5px;"><ul style="list-style-type: none">CustomerInternal LANInternet Connectivity (Uplink)Internet eXchangeOtherPeering<input checked="" type="checkbox"/> Transit</div>
Exclude From Usage By default, all the devices/interfaces are included in the SNMP Usage Page, if the user is not interested in analyzing this device/interface, enable this preference to remove it from the Usage Page	<input type="checkbox"/>
Uplink (Out) Speed Advertised Interface Speed: 0.00 Gbit	10.00 Gbit <input type="button" value="Reset Speed"/>
Downlink (In) Speed Advertised Interface Speed: 0.00 Gbit	10.00 Gbit <input type="button" value="Reset Speed"/>

Binding Exporters to Sites

- Step 1: define a site name
- Step 2: bind the exporter network to the site

Networks | Networks

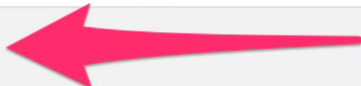










Networks Score

10.20.3.26 10.20.4.2 10.20.3.122

Networks Sites 10 + [grid] [refresh] [eye] Search:

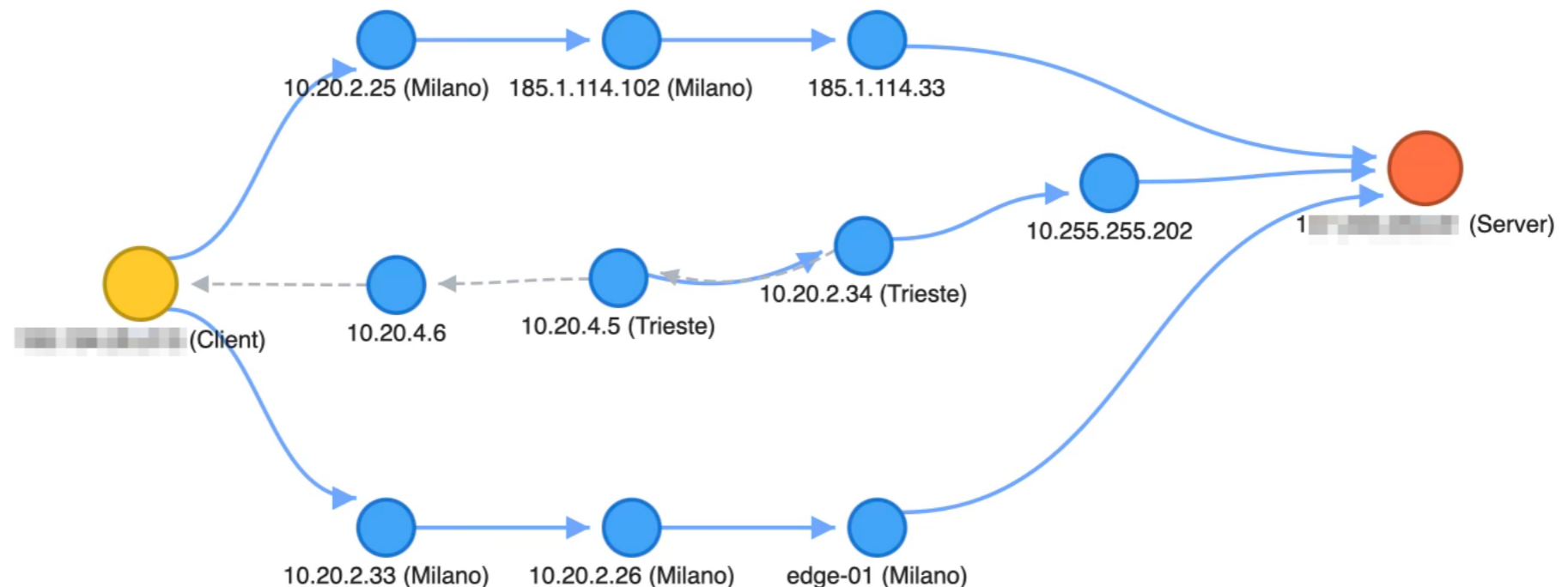
Actions	Site	Description	Location
⋮	Default		
⋮	Milano		45.138464° N, 10.260198° E
⋮	Padova		45.739169° N, 11.380144° E
⋮	Trieste		45.919325° N, 13.487195° E

Merging All Together

Role	Internet eXchange 	
CommunityId 	1:A92Wj45BN9euVc6bRY+bJ1ciby8= 	
Actual / Peak / Average Throughput	402.18 kbps / 9.97 Mbps / 6.64 Mbps	
ASN [Client / Server]		
Exporters Information	Flow Exporter / Next Hop	Input Interface / Output Interface
	 (Default) [10.255.255.203] → 10.20.4.21 	VLAN1062-edge-02.core (internal_interface) → VLAN1007-nat-02.net 
	 (Default) [10.255.255.202] → 217.29.67.15 	VLAN1063-edge-04.core (internal_interface) → VLAN100-IPT-MK (ix)  

Exploring Traffic Flow Paths

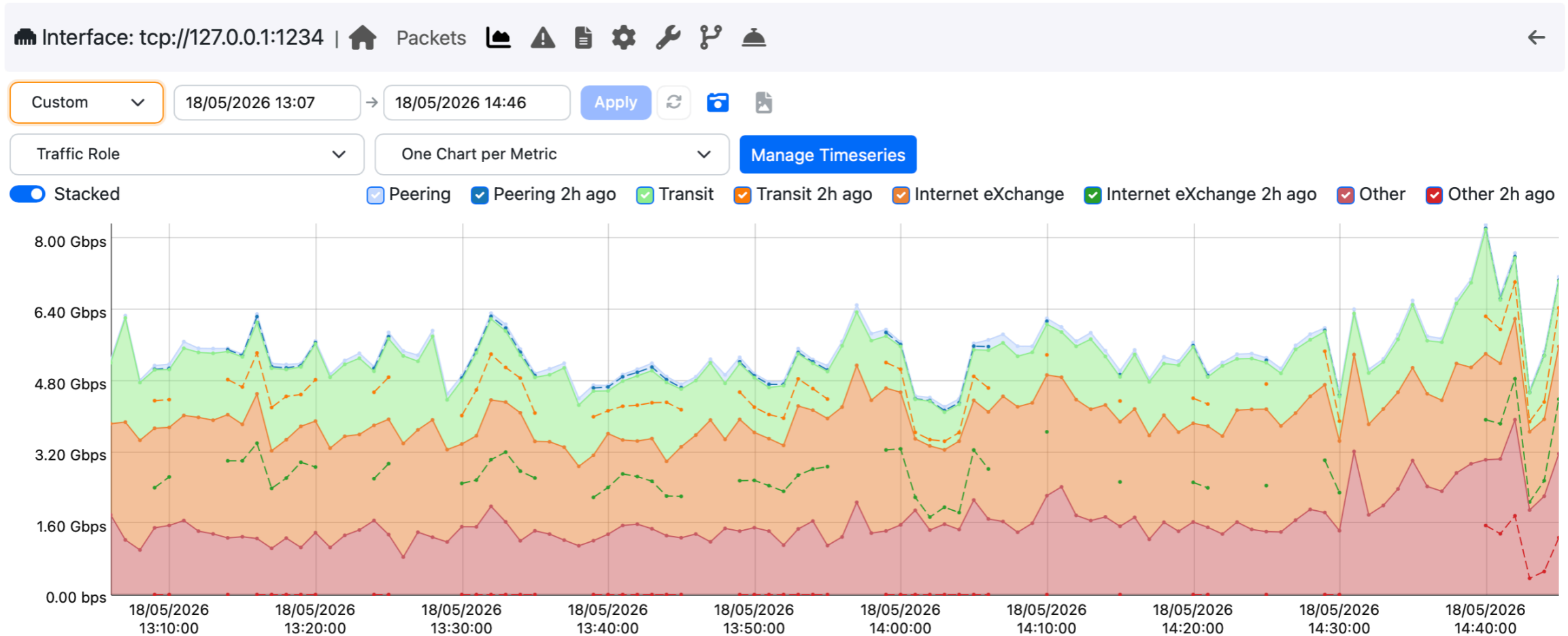
● Client ● Server ● Hop / Exporter - - - - Return Path



Note

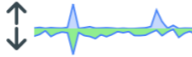
Paths are depicted based on (duplicated) collected flows.



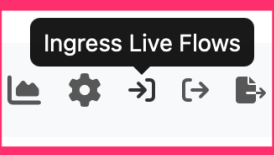
Role Traffic Breakdown






Metric	Average	95th Percentile	Max	Min	Total
Peering	68.37 Mbps	99.56 Mbps	151.46 Mbps	27.19 Mbps	47.76 GB
Transit	714.27 Mbps	1.08 Gbps	1.95 Gbps	417.46 Mbps	498.91 GB
Internet eXchange	1.23 Gbps	1.61 Gbps	1.75 Gbps	758.23 Mbps	855.90 GB
Other	1.52 Gbps	2.07 Gbps	3.06 Gbps	843.53 Mbps	1.04 TB

Interface Traffic Breakdown

tcp://127.0.0.1:1234  52.90 Kbps
1.80 Gbps 2.1K (309) 67.5K (19.9K) 18 487.9K

SNMP Devices / e (10.255.255.205) / VLAN303   

Interface Index	35
Name	VLAN303-
Role	Transit 
Interface Type	I2vlan (135)
Interface IPs	<ul style="list-style-type: none">
Uplink (Out) Speed	10 Gbit 
Downlink (In) Speed	10 Gbit 
Administrative Status	Up
Operational Status	Up
In Discards	0
In Errors	0
Out Errors	0
Last Change	182 Days, 12:48:12
In Bytes	46.25 TB
Out Bytes	5.71 TB
Last In Usage	1 % (100 Mbit)
Last Out Usage	0 %

Enhanced Flow Filtering

- In addition to the "legacy" host/protocol/etc. filters it is now possible to filter flows according to:
 - ASN
 - Exporter
 - Exporter Interfaces (id and roles).

The screenshot shows the ntop Live Flows interface with the following elements:

- Header: Live Flows | Aggregation
- Filtering controls: Host (All), Protocol (All), Application (All), Status (All), Traffic Type (All), Host Pools (All), Networks (All), Source AS (All), Destination AS (All), Flow Exporter (All), Interface Role (All). A search bar is also present.
- Table columns: Actions, First Seen, Last Seen, Duration, Protocol, Score, Cli ASN, Srv ASN, Flow.
- Table row: 01:27, 01:25, 00:03, TCP:SSH, Guess, [blurred], [blurred], 4, [blurred].

A red box highlights the filtering controls for Networks, Source AS, Destination AS, Flow Exporter, and Interface Role, along with the search bar and a Reset button.

ASN Classification



My ASNs

204471

Comma separated list of ASNs, that belong to this organization.

My Customers ASNs

200036,8038,208449,205493

Comma separated list of Customer ASNs, interconnected to the Internet via my ASNs.

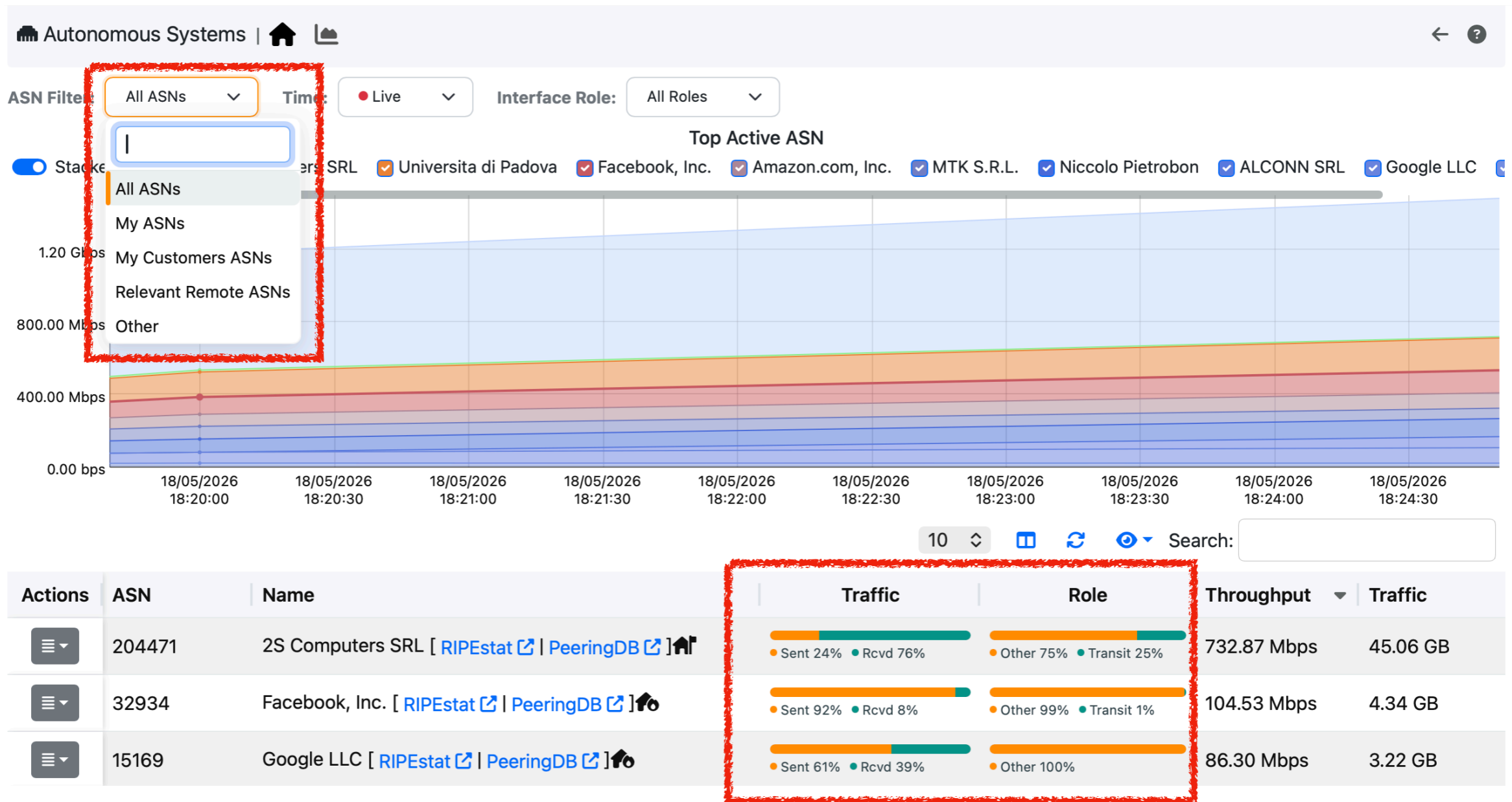
Relevant Remote ASNs

16509,2593,32934,41327,54113,15169,63949,9002

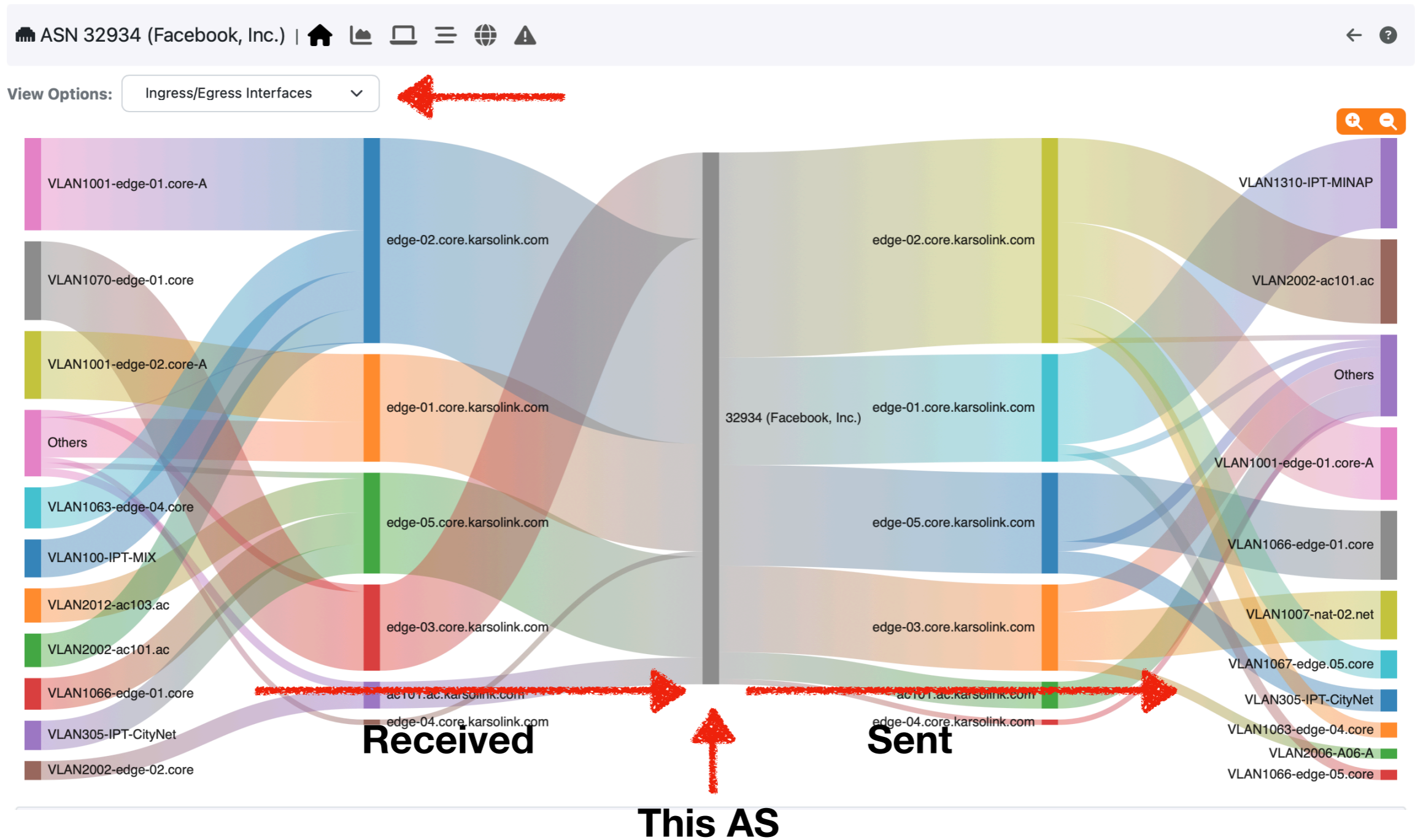
Comma separated list of Remote ASNs that are relevant for the monitoring standpoint.

Save Settings

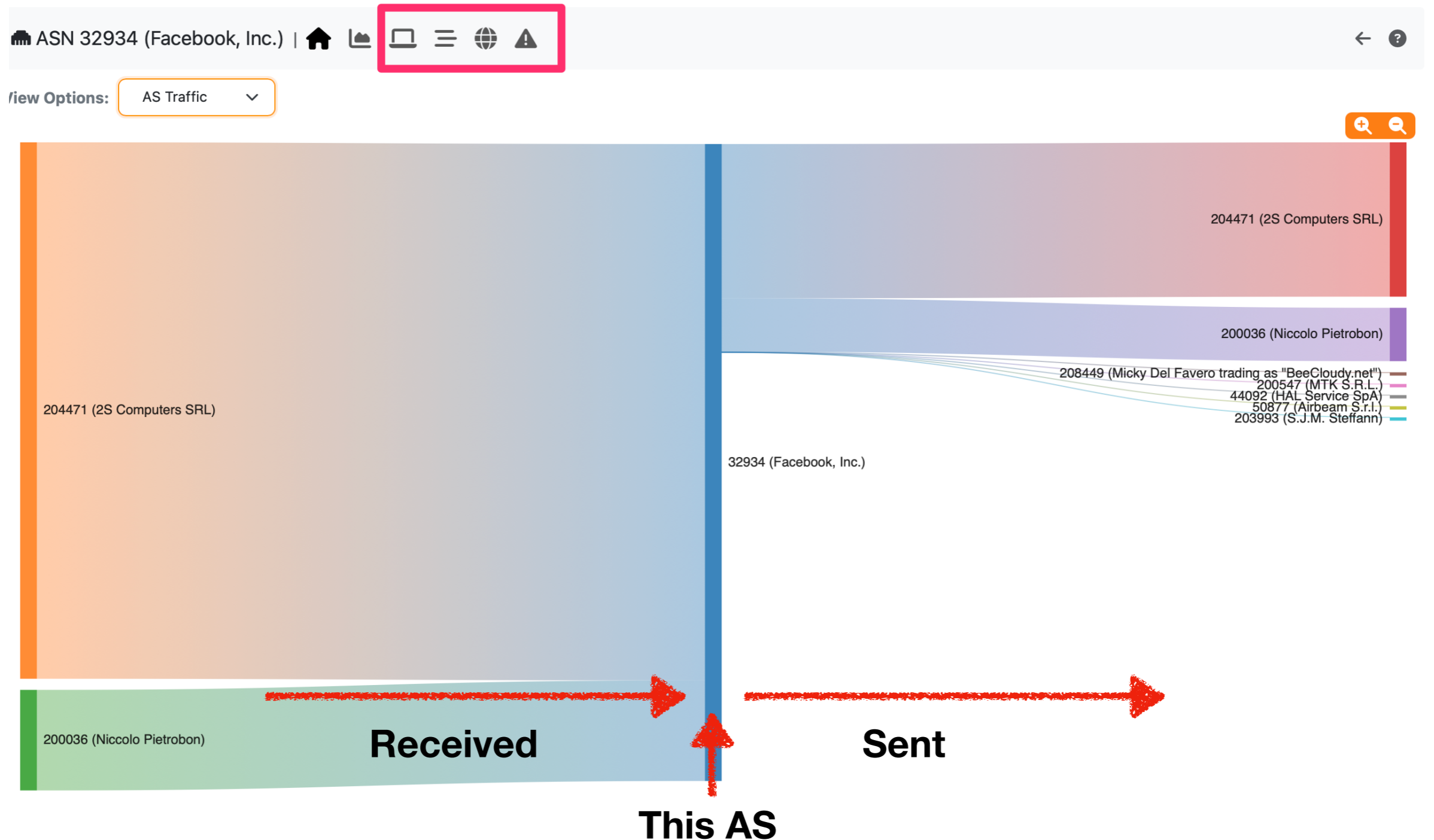
ASN Page Revamped



ASN: Ingress/Egress Interfaces



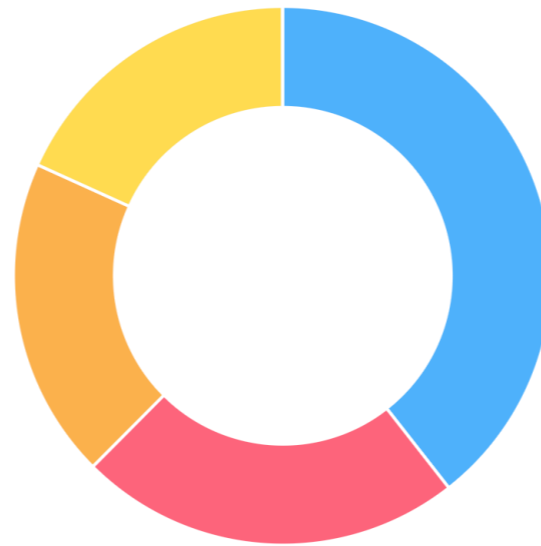
ASN Traffic View



AS View: My Customers Breakdown

ASN 14618 (Amazon.com, Inc.) | Home | Settings | Menu | Search

View Options: **Customer Breakdown** | Live | 14/09/2025 19:56 | 14/09/2025 19:56 | Apply



62275 (NHM - S.R.L.) (55.05 MB) | 34978 (Linkwireless srl) (32.17 MB) | 204386 (NABIRI S.R.L.) (26.94 MB) | 200547 (MTK S.R.L.) (25.44 MB) | 206022 (Airnetwork S.R.L.) (13.18 KB) | Others (5.9 KB)

10 | Search:

Customer ASNs	Bytes Sent	Bytes Rcvd	Tot:
62275 (NHM - S.R.L.)	31.18 MB	23.52 MB	
34978 (Linkwireless srl)	23.38 MB	7.81 MB	

Enabling ASN Mode: ntopng

The screenshot displays the ntopng web interface. At the top, there is a navigation bar with a search icon, a notification bell with a red '3' badge, and a user profile icon. Below this, a status bar shows network traffic: 1.20 Gbps (up) and 9.10 Gbps (down). A row of colored status indicators includes: 2 red triangles, 11 yellow triangles, 39 red triangles, 6.7K (4.2K) green squares, 59.2K (17K) grey squares, 215K grey squares, and an ntop logo.

The main content area is titled 'Runtime Preferences' and features a search bar labeled 'Search Preferences'. A sidebar on the left lists various settings categories: Active Scan, Active Monitoring, Alerts, Applications, Assets, Behaviour Analysis, Cache Settings, ClickHouse, Flows Dump, **ASN Mode** (highlighted in blue), and LLM Providers. The 'Settings' category in the sidebar is also highlighted in orange.

The 'ASN Mode' section is expanded, showing a toggle switch labeled 'Enable ASN Mode' which is turned on. Below this, the 'BGP Server Configuration' section is visible, containing two input fields: 'Server Address' with the value '127.0.0.1' and 'Server Port' with the value '63799'. A blue 'Save' button is located at the bottom right of the configuration area.

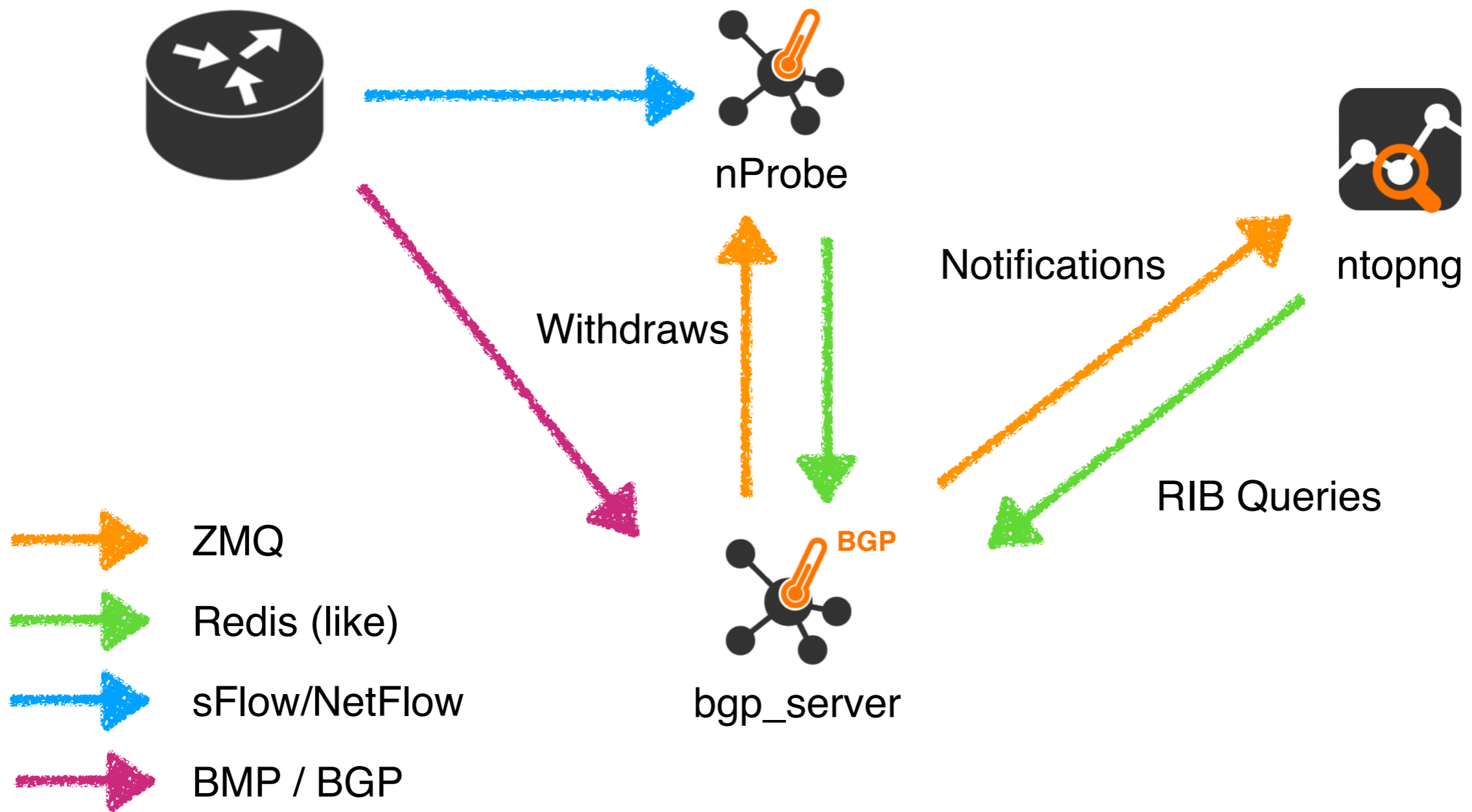
Enabling ASN Mode: nProbe

- You have the option to:
 - Collect flows as they are received (i.e. with full IP information).
 - [Optional] Mask IP addresses (according to the flow netmask) in order to hide the exact IP address.

```
--asn-mode          | Collect flows and optimize export for AS traffic analysis.  
                    | This CLI option has no effect in packet mode
```

- Note: DPI in flow collection operates partially (no packets) using IP addresses (e.g. the Office365 IP range) and protocol+ports.

BGP/BMP Collection [1/2]



BGP/BMP Collection [2/2]

```
Welcome to bgp_server v.11.1.260406 for macOS 26.4
Copyright 2026 - ntop.org
```

```
Usage: bgp_server -z <URL> [-p <BMP port>] [-r <redis port>]
        [-b <BGP port>] [-a <local ASN>] [-i <BGP router-ID>]
        [-n <path>] [-v]
```



```
-z <URL>      ZMQ publish URL
-p <port>     BMP listen port           (default 11019)
-r <port>     Redis query port         (default 63799)
-b <port>     BGP passive listen port   (0 = disabled, default BGP port is 179)
-a <ASN>      Local AS number for BGP OPEN (default 65000)
-i <IP>       Local BGP router-ID (dotted decimal, default 1.1.1.1)
-n <path>     List of IPv4/v6 prefixes to be notified (add/withdraw)
-v           Verbose: print every parsed message
```

Example:


```
[BMP] bgp_server -z tcp://127.0.0.1:11059 -p 11019 -n prefixes.txt
```

```
[BGP] bgp_server -z tcp://127.0.0.1:11059 -i 10.82.4.121 -p 179 -a 65000 -n prefixes.txt
```


Merging Routing with Flows

Flow: [blurred] → [blurred] |  **BGP** 

BGP Client Info


Prefix	45.159.195.0/24 
BGP Peer Id	217.197.106.201
BGP Peer ASN	204471 (KARSOLINK - 2S Computers SRL)
Origin	IGP
Next Hop	10.255.255.201
AS Path	204471 (KARSOLINK - 2S Computers SRL) 200036 (CITYNET - Niccolo Pietrobon)
MED (Multi-Exit Discri...	
Local Pref.	
Communities	

BGP Server Info

Prefix	209.99.184.0/21 
BGP Peer Id	217.197.106.201
BGP Peer ASN	204471 (KARSOLINK - 2S Computers SRL)
Origin	IGP
Next Hop	10.255.255.201
AS Path	204471 (KARSOLINK - 2S Computers SRL) 9002 (RETN-AS - RETN Limited) 3257 (GTT-BACKBONE GTT Communications Inc.) 30823 (AUROLOGIC - aurologic GmbH) 402253 (SKN-NETWORK-1 - SKN Subnet & Teleco...
MED (Multi-Exit Discri...	
Local Pref.	
Communities	9002:9002 9002:64641


BGP Looking Glass

☰ BGP Looking Glass | 🏠 ← ?

1.1.1.1 🔍 1.1.1.0/24 RPKI: Valid 

10 📄 ↻ 🔍 Search:

BGP Peer Id	BGP Peer ASN	Origin	AS Path	Next Hop	Local Pref.
185.54.80.4 (MIX-IT - Default)	202032 (GOLINE - GOLINE ...)	IGP	• 13335 (CLOUDFL/	185.54.80.4	305
193.221.216.30	5398 (INTERNETONE - Inte...)	IGP	• 5398 (INTERNETC • 13335 (CLOUDFL/	77.220.74.109	200
185.54.80.5 (MINAP - Default)	202032 (GOLINE - GOLINE ...)	IGP	• 13335 (CLOUDFL/	185.54.80.5	305
38.28.1.11	174 (COGENT-174 - Cogent...)	IGP	• 174 (COGENT-174 • 13335 (CLOUDFL/	149.11.89.168	200
212.74.82.15	8220 (COLT - COLT Techno...)	IGP	• 8220 (COLT - COL • 13335 (CLOUDFL/	87.241.16.133	200
185.54.80.3 (SWISS-IX - Default) Best 🏆	202032 (GOLINE - GOLINE ...)	IGP	• 13335 (CLOUDFL/	185.54.80.3	305



Alerts [1/2]

⚠ Alert | 🏠



AS	15169 (Google LLC)
Date / Time	09:06:19
Alert	Threshold Crossed
Description	[Metric: Traffic (RX + TX)] [Condition: 409.37 Mbps > 400 Mbps] [Check Frequency: 5 Minutes]

Alerts [2/2]

Alert | 



AS	23344 (Disney Worldwide Services, Inc.)
Date / Time	20:00:35
Alert	AS Exporter Ranking Changed
Description	<p>Ingress ranking changed to</p> <ul style="list-style-type: none">[rank 1] NE8K_F1A_1_NAMEX:NAMEX_PEERING_LAN (17.72 GB)[rank 2] NE8K_M14_MIX:MINAP_via_SEEWEB-TGE1/0/39 (944.45 MB)[rank 3] NE8K_M14_MIX:MIX_PEERING (125.9 MB)[rank 4] NE8K_M14_MIX:BSO_IX_REACH_DECIX_FRANKFURT - ID_2288 (1.5 MB) <p>from</p> <ul style="list-style-type: none">[rank 1] NE8K_F1A_1_NAMEX:NAMEX_PEERING_LAN (18.32 GB)[rank 2] NE8K_M14_MIX:BSO_IX_REACH_DECIX_FRANKFURT - ID_2288 (515.33 KB)

Availability

- What presented today is available in the dev branch. They will be included in the next stable.
- The `bgp_server` does not require an additional license other than nProbe (M and above), and it is based on open source software we developed (URL at the end of this presentation).
- AS/Routing information is available in all ntopng versions if available.

Future Work Items

- AI will be integrated into ntopng to ease data analysis.
- Additional alerts (e.g. DDoS, BGP peers state...).
- Detection of traffic spikes not due to a DDoS (e.g. soccer match).
- Provide more insight about billing costs per customer (peering exposed), in order to better tune the monthly fees based on the current usage.
- What else ?



<https://github.com/ntop/ntop.png>

<https://github.com/ntop/nProbe/tree/master/bgp>

Credits

- Federico Santulli - NHM (AS 62275)
- Vasja Krizmancic - Karsolink (AS 204471)
- Paolo Caparrelli - Goline (AS 202032)