

AS Traffic Observability using ntopng

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

Federico Santulli <federico.santulli@nhm.it>

Who am I

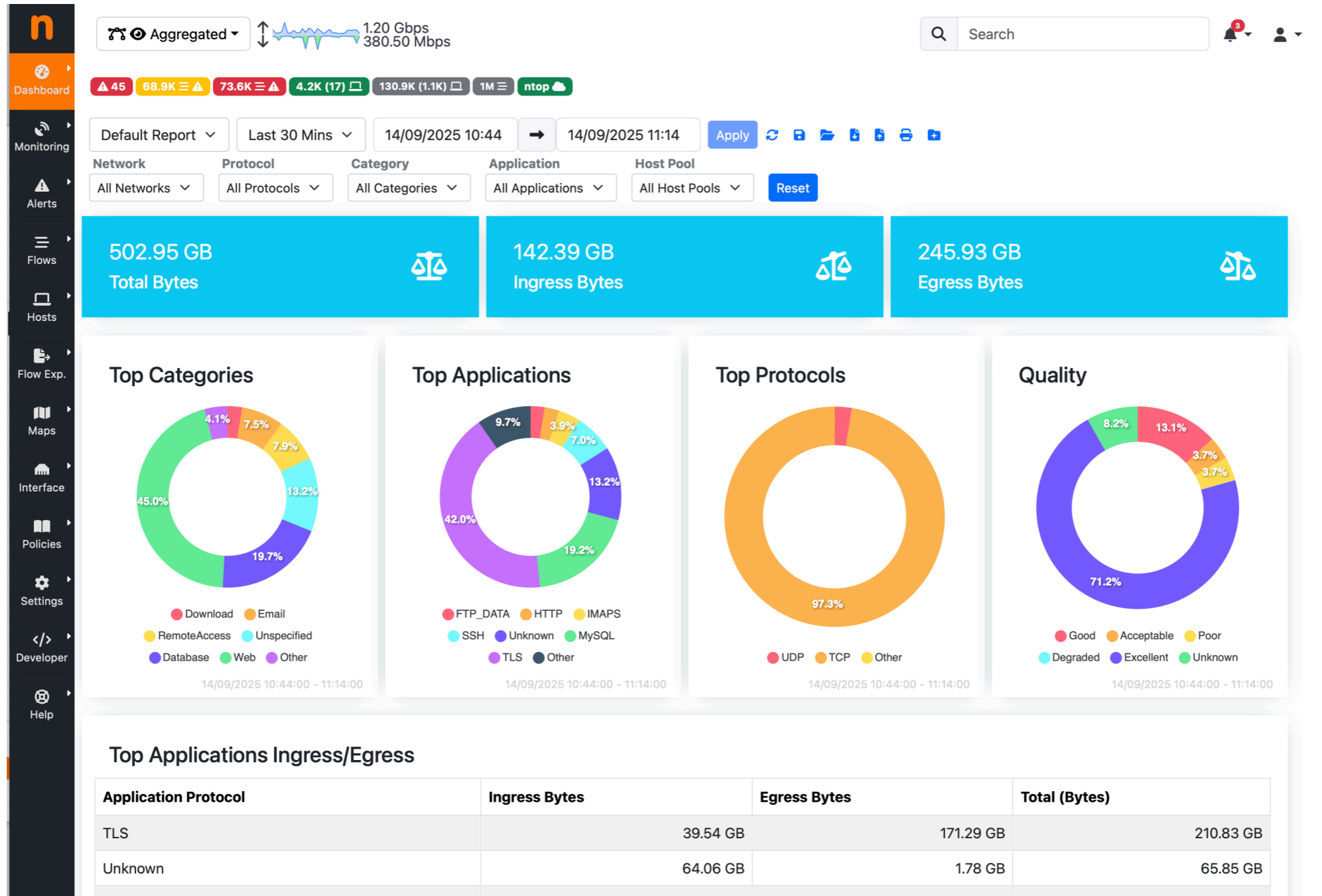
- Luca is the ntop founder, company that develops open-source network security and visibility tools.
- Author of various open source software tools and Lecturer at the Computer Science Department, University of Pisa, Italy.
- Federico, is N.H.M. CEO (AS 62275) and seasoned network expert.



Goal of This Presentation

- Introduce open source AS traffic observability.
- Show you that you will now be able to monitor your AS traffic without costly monthly subscriptions to non-European cloud-based products.
- Know your feedback in order to steer the development.
- See if any of you are willing to help us test/adopt the tool and educate us on this topic (you are the traffic experts, we are the coders).

What is ntopng ? [1/2]



What is ntopng ? [2/2]

- Open source (<https://github.com/ntop/ntopng>) traffic monitoring application able to also collect NetFlow/IPFIX/sFlow flows (~100k flows/sec).
- Ability to generate behavioral metrics, traffic alert, DPI-based traffic analysis.
- ETA (Encrypted Traffic Analysis) based on nDPI.
- High-capacity historical flow database.
- Data export to Elasticsearch, Kafka, InfluxDB, Grafana.
- Integration with SIEM and security applications/IDS (Suricata).
- Enterprise edition available at no cost for research and educational users.

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. Note: they also have portion of the overall traffic they "own". 

Monitoring a Network Operator

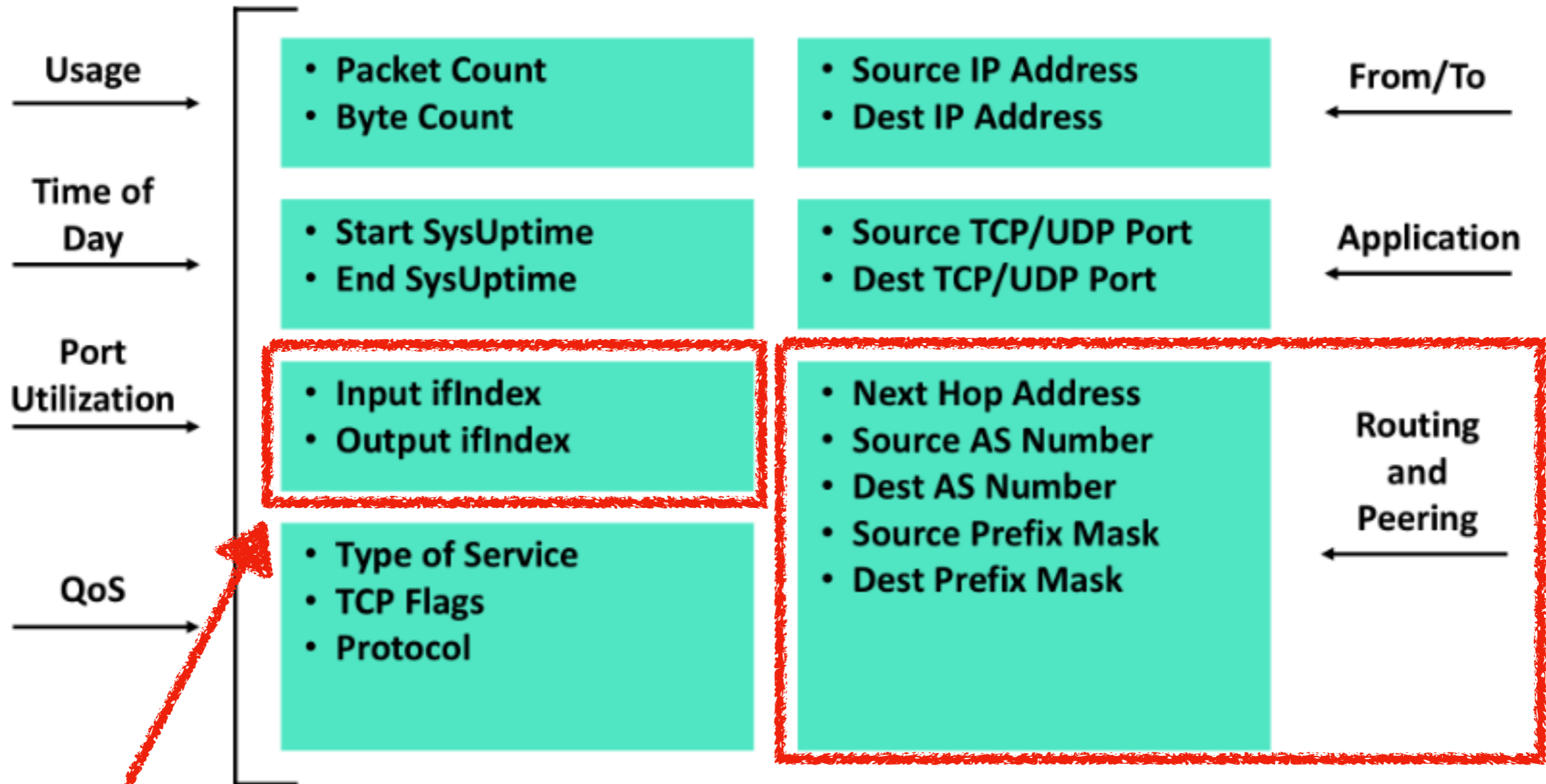
- Data Source

Usually routers (NetFlow/IPFIX) and switches (sFlow). Packets would be the best but they carry too many details, and often they are too many to analyze.

- Routing Information

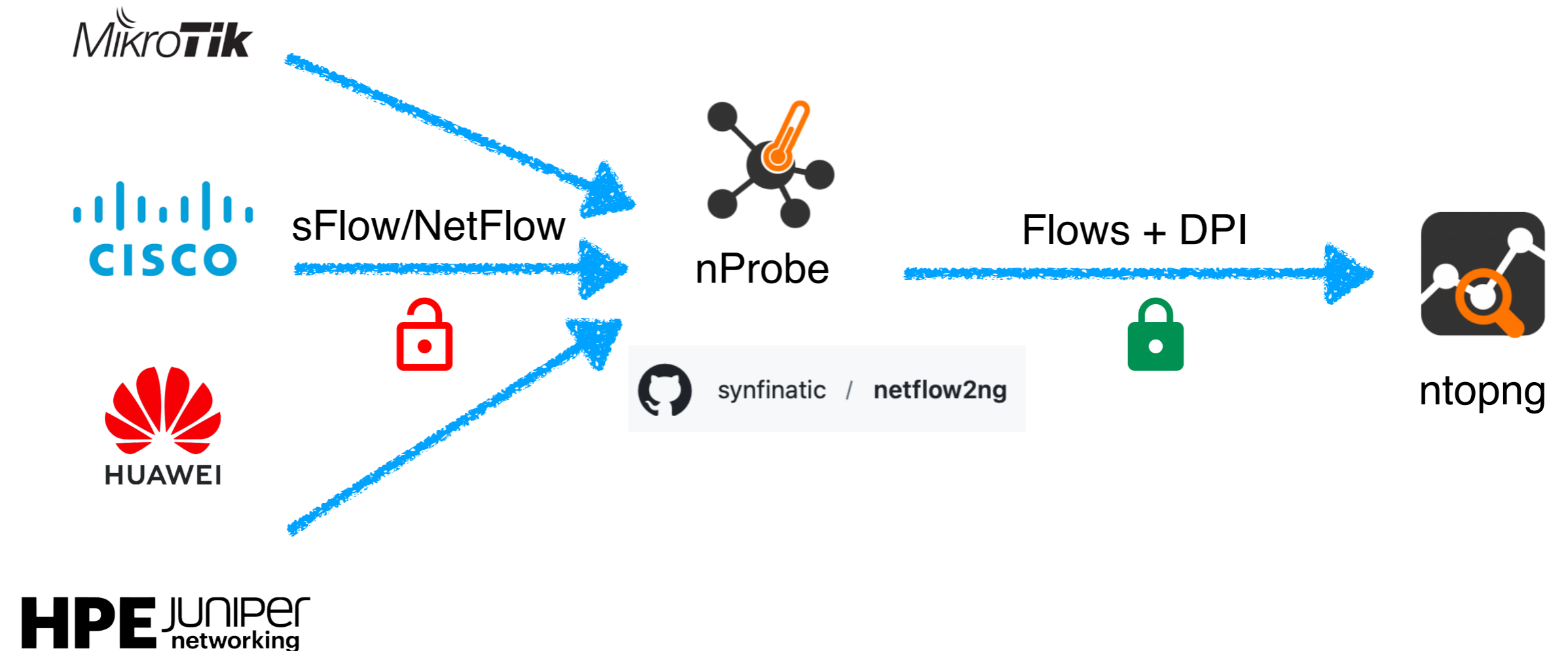
Flow contain "mild" routing information that is enough for basic traffic analysis. More advanced BGP data access would be desirable.

What's Inside a Flow ?

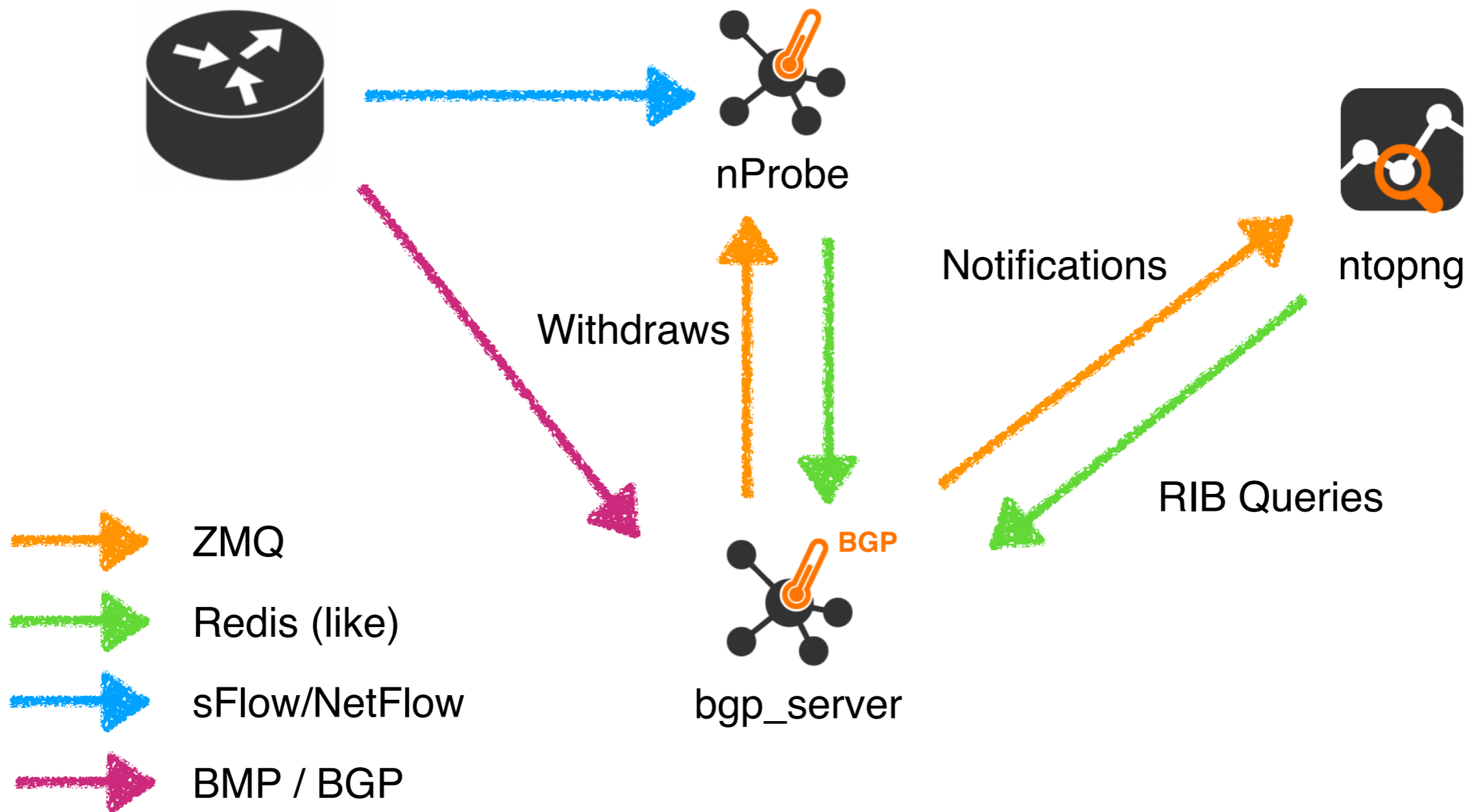


Flow Exporter Information

Flow Collection in ntopng



BGP/BMP Collection [1/2]



BGP/BMP Collection [2/2]

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 ASN to be notified
-v           Verbose: print every parsed message
```

Example:

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

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

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

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 the navigation bar, a status bar shows a 'view:all' dropdown, a traffic graph, and several data points: 1.20 Gbps / 9.10 Gbps, 2 alerts, 11 warnings, 39 errors, 6.7K (4.2K) flows, 59.2K (17K) flows, 215K flows, and ntopng status.

Runtime Preferences

Search Preferences

- Active Scan
- Active Monitoring
- Alerts
- Applications
- Assets
- Behaviour Analysis
- Cache Settings
- ClickHouse
- Flows Dump
- ASN Mode**
- LLM Providers

ASN Mode

Enable ASN Mode

Implement ASN traffic analysis and data aggregation capabilities. Optimal outcomes are attainable when utilizing nProbe to collect NetFlow flows.

BGP Server Configuration

Server Address
Network address of the BGP server

Server Port
BGP server port

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.

Configure Your ASNs

Network Configuration | Policies **ASN Configuration** ←

My ASNs

62275,58113

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

Customer ASNs

[Blurred text]

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

Relevant Remote ASNs

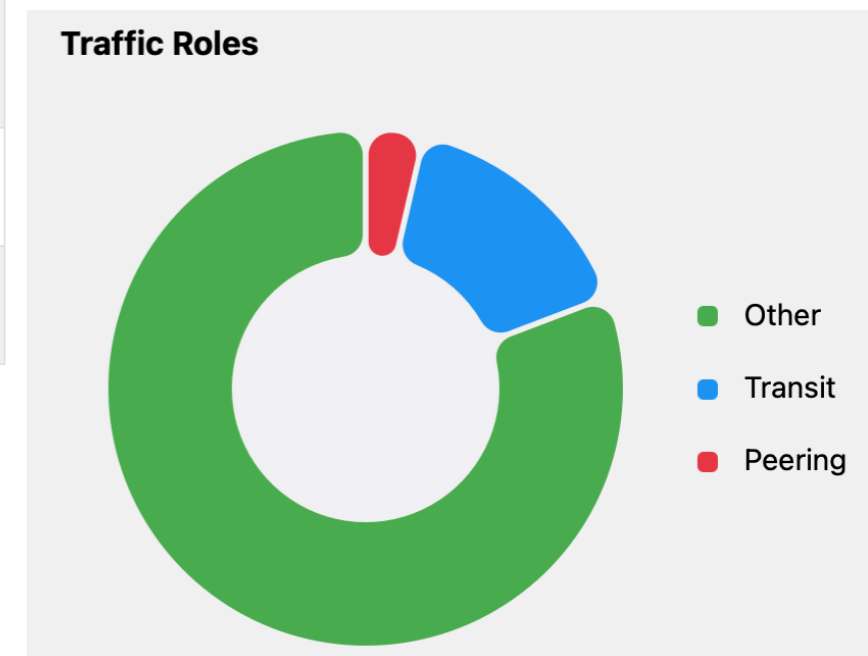
16509,396982,13335,19551,8075,14618,54113,15169,54994,209242,40509,139341,15967,60068,21859,16625,16276,24429,47583,14061,202492,199524,31898,45102,132203,32934,2906,40027,8234,48634,5400,8968,11251,22604,23344,23258

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

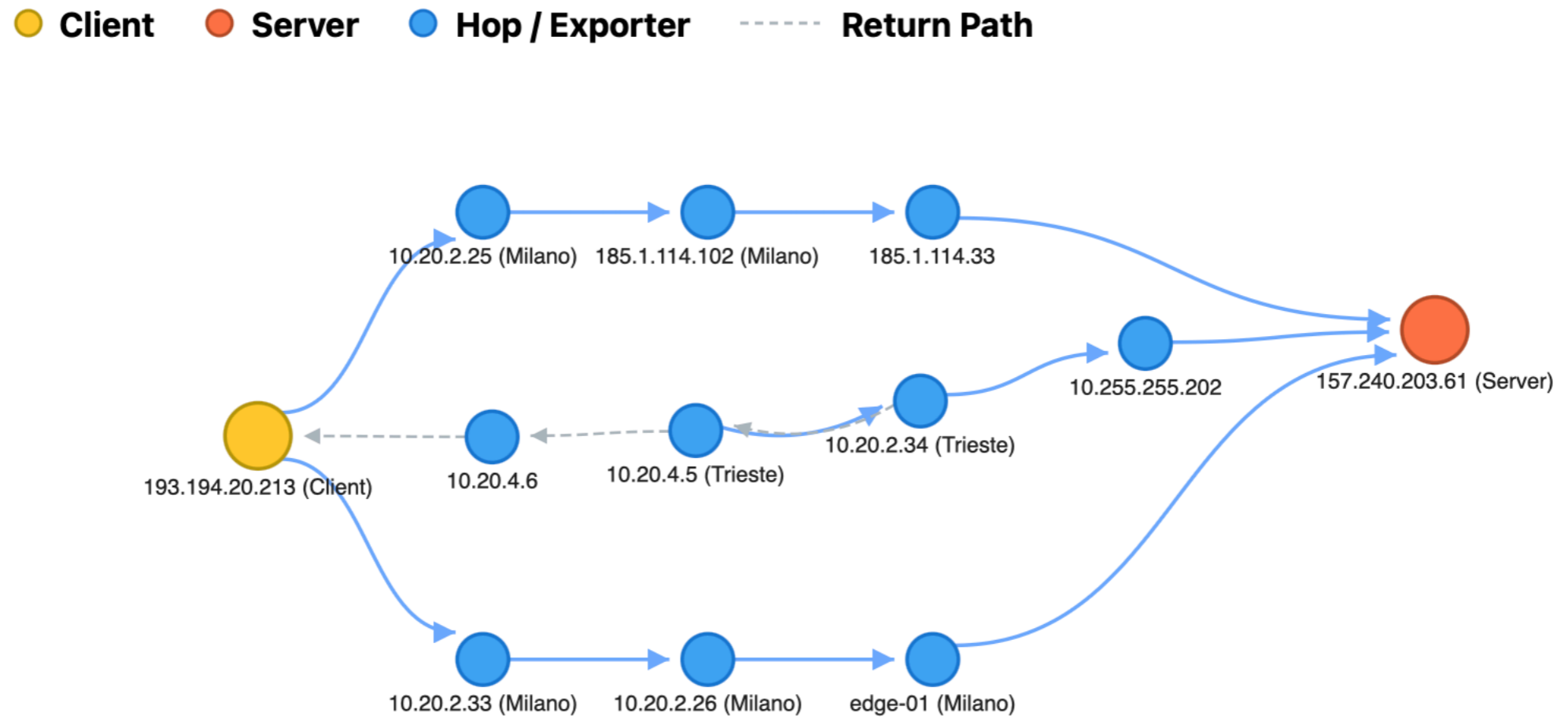
Save Settings

Configure Your Interfaces

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 checked="" 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: 1px solid #ccc; padding: 5px;"><ul style="list-style-type: none">CustomerIX (Internet Exchange)Internal LANInternet Connectivity (Uplink)Other<li style="background-color: #007bff; color: white;">✓ PeeringTransit</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	<input type="text" value="1.00"/> Gbit Reset Speed
Downlink (In) Speed Advertised Interface Speed: 0.00 Gbit	<input type="text" value="1.00"/> Gbit Reset Speed



Explore Traffic Flows



AS View

view:all 1.70 Gbps 9.90 Gbps 2 3 39 6.8K (4.2K) 57.1K (15.9K) 216.3K ntop

Autonomous Systems

ASN Filter: All ASNs Time: Live Interface Role: All Roles

Stacked Top Active ASN

Facebook, Inc. Amazon.com, Inc. Akamai International B.V. Google LLC

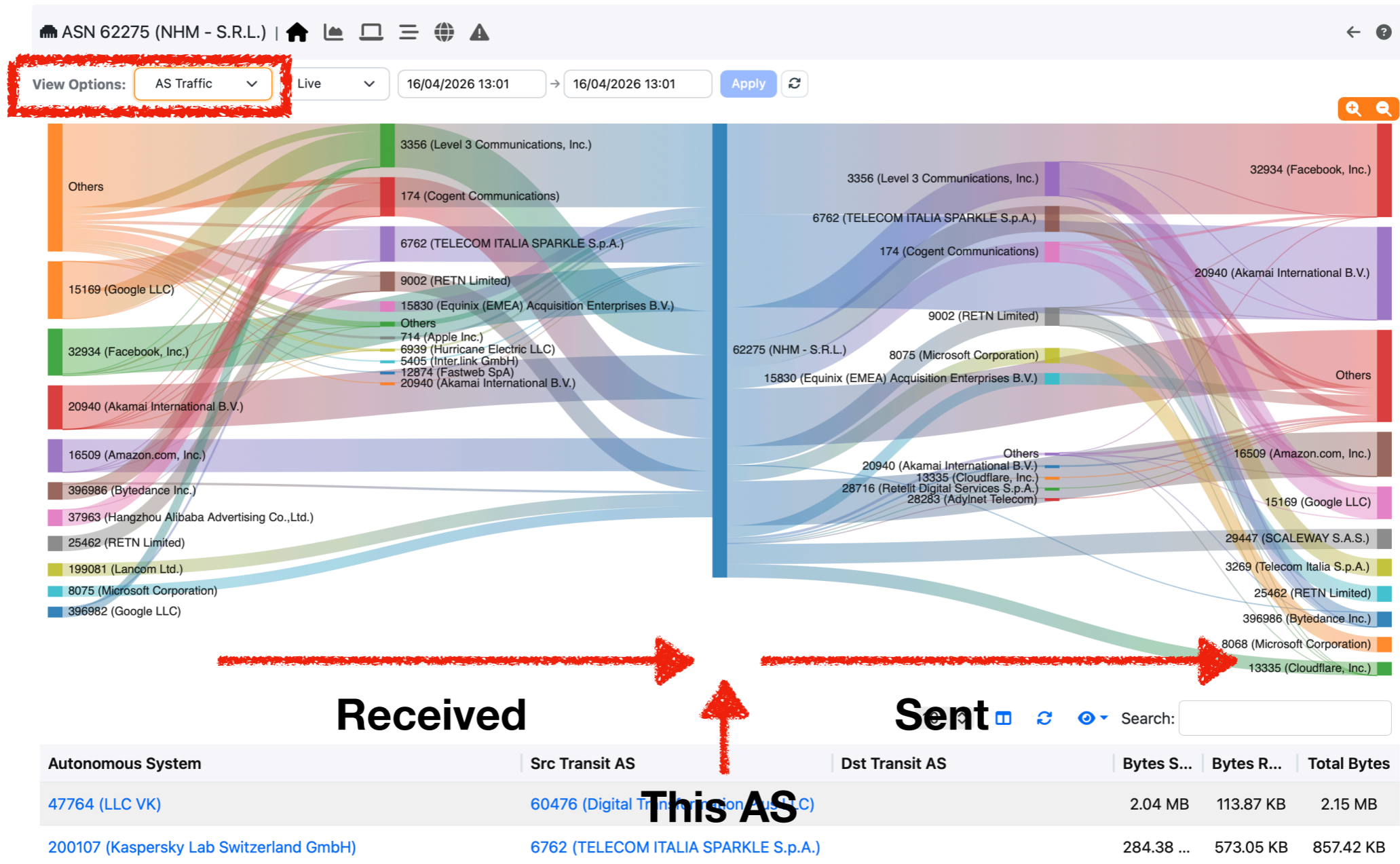
12.00 Gbps
8.00 Gbps
4.00 Gbps
0.00 bps

16/04/2026 12:06:00 16/04/2026 12:08:00 16/04/2026 12:10:00 16/04/2026 12:12:00 16/04/2026 12:14:00 16/04/2026 12:16:00 16/04/2026 12:18:00

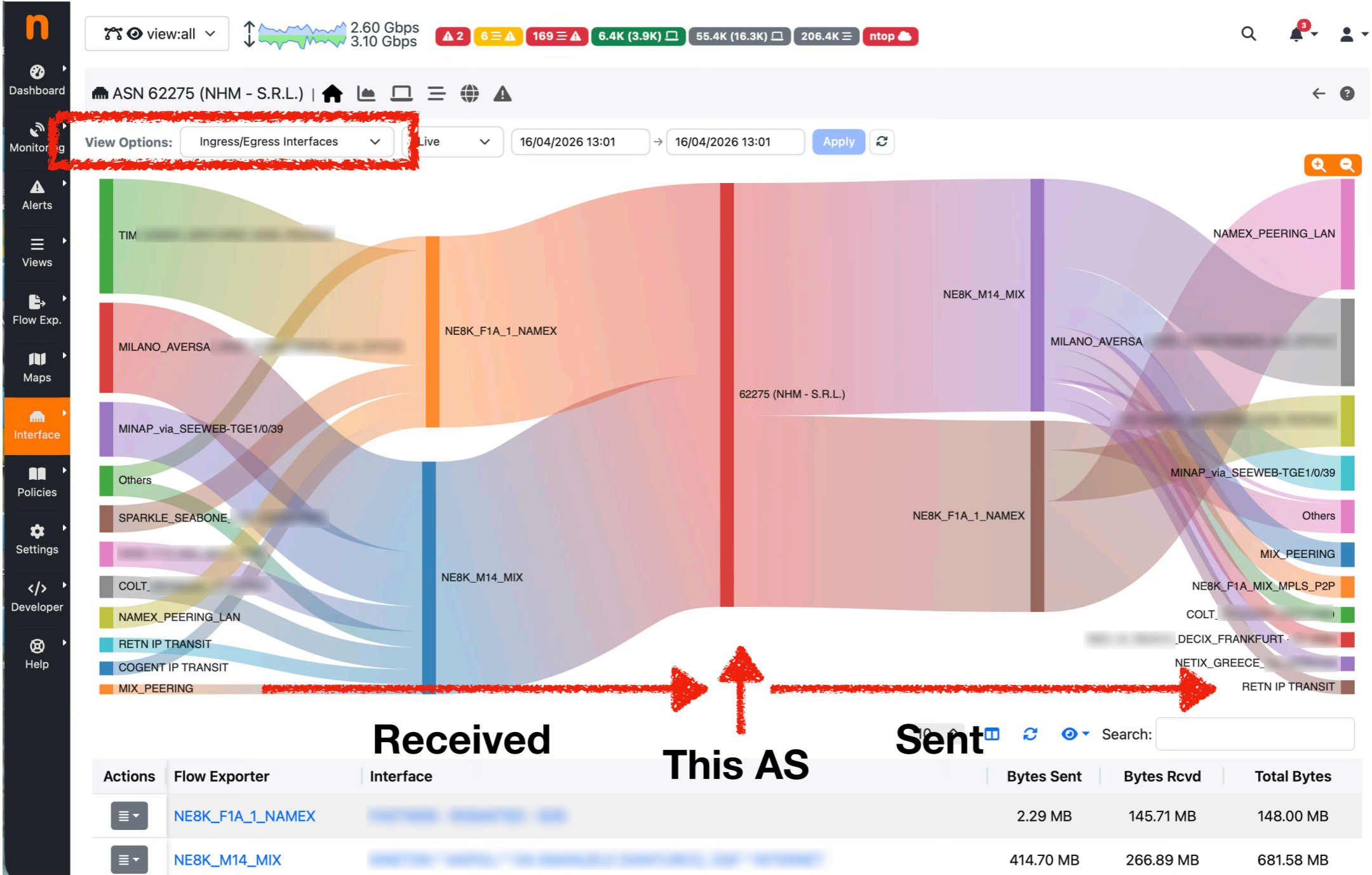
10 [Refresh] [Fullscreen] [Search]

Acti...	ASN	Name	Seen Since	Breakdown	Throughput	Traffic
<input type="checkbox"/>	62275	NHM - S.R.L. [RIPEstat PeeringDB]	11:29:43	Sent 13% Rcvd 86%	3.53 Gbps	60.41 GB
<input type="checkbox"/>		[RIPEstat PeeringDB]	11:29:43	Sent 15% Rcvd 84%	2.10 Gbps	35.11 GB
<input type="checkbox"/>	32934	Facebook, Inc. [RIPEstat PeeringDB]	11:29:43	Sent 93% Rcvd 6%	1.45 Gbps	20.68 GB
<input type="checkbox"/>		[RIPEstat PeeringDB]	11:29:43	Sent 15% Rcvd 84%	1.40 Gbps	22.02 GB
<input type="checkbox"/>	3269	Telecom Italia S.p.A. [RIPEstat PeeringDB]	11:29:43	Sent 4% Rcvd 95%	1.31 Gbps	5.13 GB

AS View: Traffic View



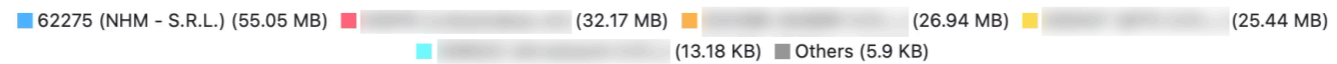
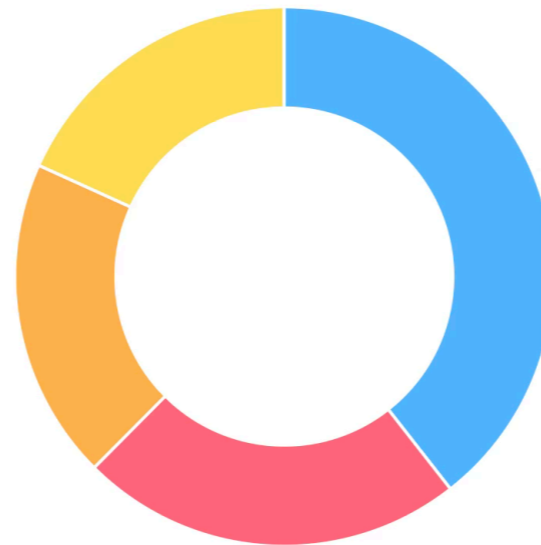
AS View: Router/Interfaces View



AS View: My Customers Breakdown

ASN 14618 (Amazon.com, Inc.) | Home | Settings | Refresh | Help

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



10 | Search:

Customer ASNs	Bytes Sent	Bytes Rcvd	Total
62275 (NHM - S.R.L.)	31.18 MB	23.52 MB	
	23.38 MB	7.81 MB	

BGP Looking Glass

The screenshot displays the ntop BGP Looking Glass interface. At the top, there is a navigation bar with a search icon, a notification bell with a red '3', and a user profile icon. Below the navigation bar, a summary section shows traffic statistics: 6.10 Gbps (up) and 8.50 Gbps (down). A series of colored status indicators follows: 1 red triangle, 14 yellow triangles, 108 red triangles, 6K (3.6K) green squares, 48.7K (13.6K) grey squares, 279.9K yellow squares, and the ntop logo.

The main content area features a search bar with the IP address '2a01:4f8:1c1a:bd58::1' and a search icon. To the right, the prefix '2a01:4f8::/32' is displayed with an 'RPKI: Valid' status. Below the search bar, there are controls for page size (set to 10), refresh, and search input.

The central part of the interface is a table with the following columns: BGP Peer Id, BGP Peer ASN, Origin, AS Path, Next Hop, and Local Pref. The table contains five rows of data:

BGP Peer Id	BGP Peer ASN	Origin	AS Path	Next Hop	Local Pref.
217.197.106.202	204471 (KARSOLINK - 2S Co...)	IGP	• 62275 (NHM - NHM - S...) • 24940 (HETZNER-AS -	2a04:8640:cafe:ba...	100
185.40.212.1	62275 (NHM - NHM - S.R.L.)	IGP	• 24940 (HETZNER-AS -	fd00::10:80:6:13	198
185.40.212.2 (NE8K_M14_MIX - Milano) Best 🏆	62275 (NHM - NHM - S.R.L.)	IGP	• 24940 (HETZNER-AS -	fd00::10:80:6:a	198
185.40.212.5	62275 (NHM - NHM - S.R.L.)	IGP	• 24940 (HETZNER-AS - • 24940 (HETZNER-AS -	fd00::10:80:6:5	101

On the left side, a vertical sidebar contains navigation icons and labels: Dashboard, Monitoring, Alerts, Views, Flow Exp., Maps, Interface, Policies, and Settings.

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 (944.45 MB)[rank 3] NE8K_M14_MIX:MIX_PEERING (125.9 MB)[rank 4] NE8K_M14_MIX:DECIX_FRANKFURT (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:DECIX_FRANKFURT (515.33 KB)

Future Work Items

- Additional alerts (e.g. DDoS, BGP peers state...).
- Detection of traffic spikes not due to a DDoS (e.g. soccer match).
- Add new traffic analysis tools to provide hints about new peering agreements that could improve your costs.
- 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/ntopng>

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

Credits

- Vasja Krizmancic - Karsolink (AS 204471)
- Paolo Caparrelli - Goline (AS 202032)