

NetFlow: what happens in your network?

by Lorenzo Busatti

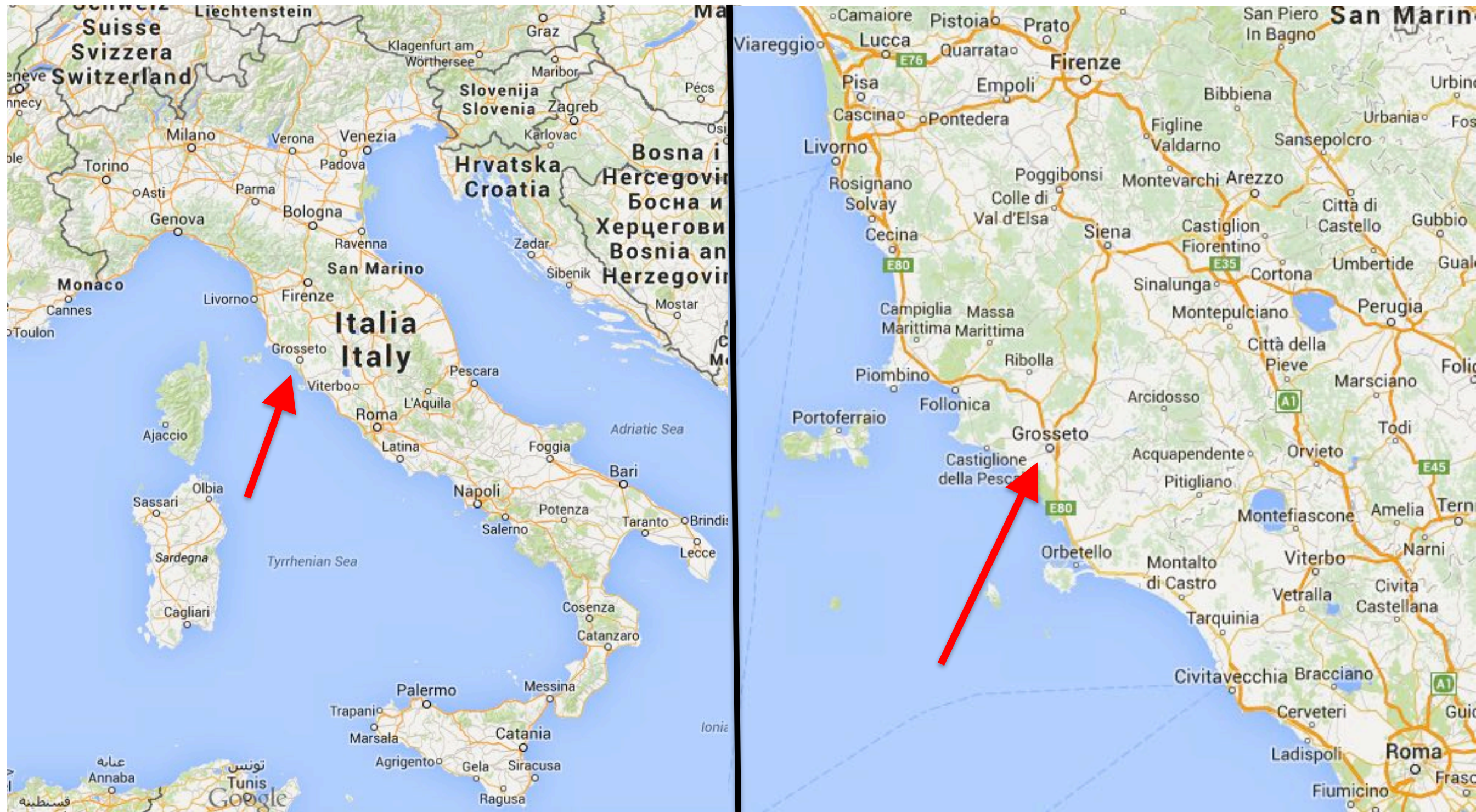
EUROPE ON FEBRUARY 25 - 26, 2016

About me

Lorenzo Busatti

- Founder of Grifonline S.r.l. (1997)
- Founder of Linkwave (2006)
- MikroTik Trainer (2010)
- Member of RIPE, AMS-IX, MIX-IT

About me



I'm a MikroTik *enthusiast*

I'm a MikroTik *enthusiast*

I'm a MikroTik *evangelist*

About me

- Founder (2016) of the



**Non Profit Organization for
High Quality Training Partners**

Advertising time!

My friend Andrew Cox booked too late for this MUM, so the presentations slots was already full.

I promised him to quick advertise his fantastic product (and for free 😊):



Bright WiFi

Cloud based management software
for ISP's and integrators



Bright WiFi

Clever customer connections.

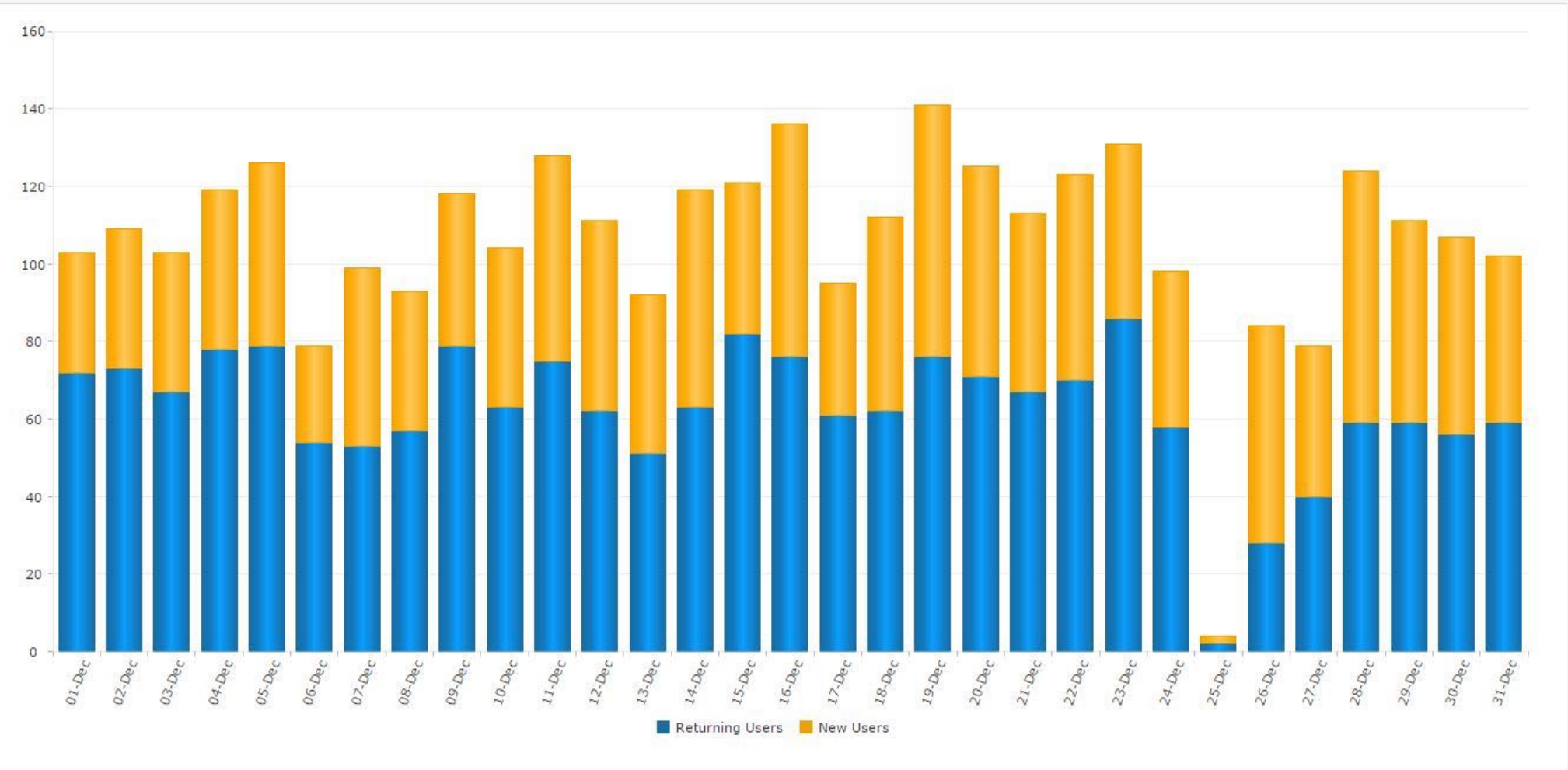
- Dashboard
- Users
- Rooms
- Units
- Settings
- Reports
- Prepaid

Dashboard

All Bright WiFi Hotspots (Paid)

Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan

New vs Returing Users for December 2015



At a Glance

21
Online Now
At 7 Jan 2016

Data Usage

131.73GB Downloads 01-Dec to 31-Dec	28.61GB Uploads 01-Dec to 31-Dec	764.74GB Forecast Downloads 01-Dec to 31-Dec
136.46GB Forecast Uploads 01-Dec to 31-Dec		

Users

1,957 Unique Users 01-Dec to 31-Dec	1,371 New 01-Dec to 31-Dec	586 Returning 01-Dec to 31-Dec
---	----------------------------------	--------------------------------------



Bright WiFi

Clever customer connections.



Dashboard



Users



Units



Settings



Reports

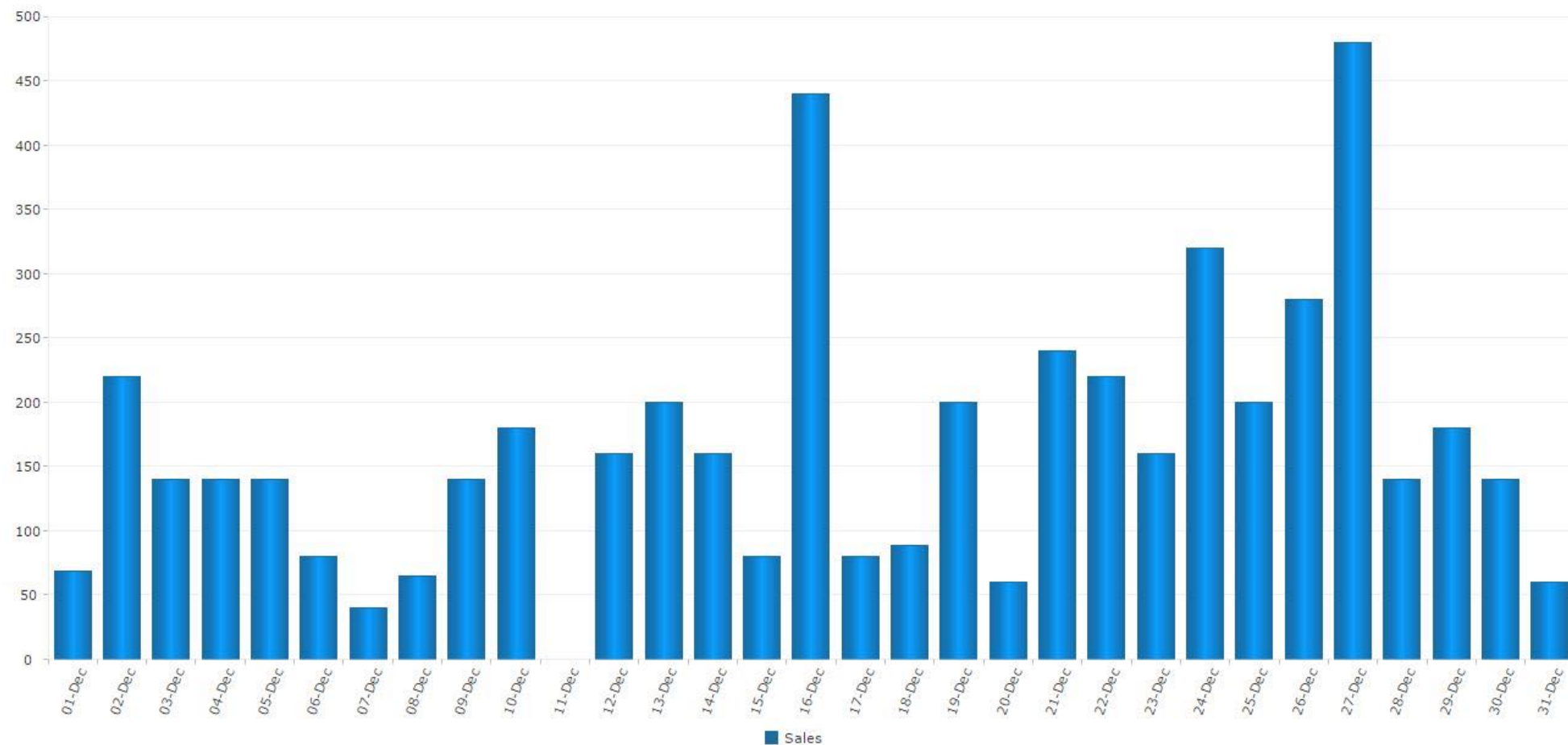


Prepaid

Dashboard

Demo Residential

Daily Sales for December 2015



Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan

At a Glance

67 %

Take up Rate

At 7 Jan 2016

113

Connected Units

At 7 Jan 2016

\$7,459.40

Contracted Value

At 7 Jan 2016

Connections

7

Activated

01-Dec to 31-Dec

0

Cancelled

01-Dec to 31-Dec

7

User Gain

01-Dec to 31-Dec

Data Usage

7,859.31GB

Downloads

01-Dec to 31-Dec

2,008.62GB

Uploads

01-Dec to 31-Dec

9,867.94GB

Total Usage

01-Dec to 31-Dec

Sales

\$5,099.20

Total Sales

01-Dec to 31-Dec

Add to Page

Drag or double-click to add a control to your page.

Paid Login

- Standard Login (+ Social)
- Standard Login
- Signup

Free Login

- One Click Button
- Ask a Question
- Mobile Phone (SMS)
- Social Account
- Demographics
- Passcode
- External Login

Page Elements

- Text
- Link
- Line

Terms & Conditions

- Terms & Conditions

Halcyon House



Click Here for FREE WiFi

Access FREE WiFi with your favourite social network login.



Background Colour Margin
 Padding Border options

Time & Data After Login

Free Login

How do you want to limit the user?

Data ☒ 100 MB

Time ☐ 30 minutes

How long does the user have to wait for a refill?

1 days

Restrict the speed of the connection?

☐ Full
☐ Full

Dedicated to Max

The traffic of your network

The traffic of your network

Is one of the most
important “things”.

The traffic of your network

What do you know
about it ?

The traffic of your network

What is the growth of your customer traffic to Netflix?

The traffic of your network

What are the top AS you should peer with?

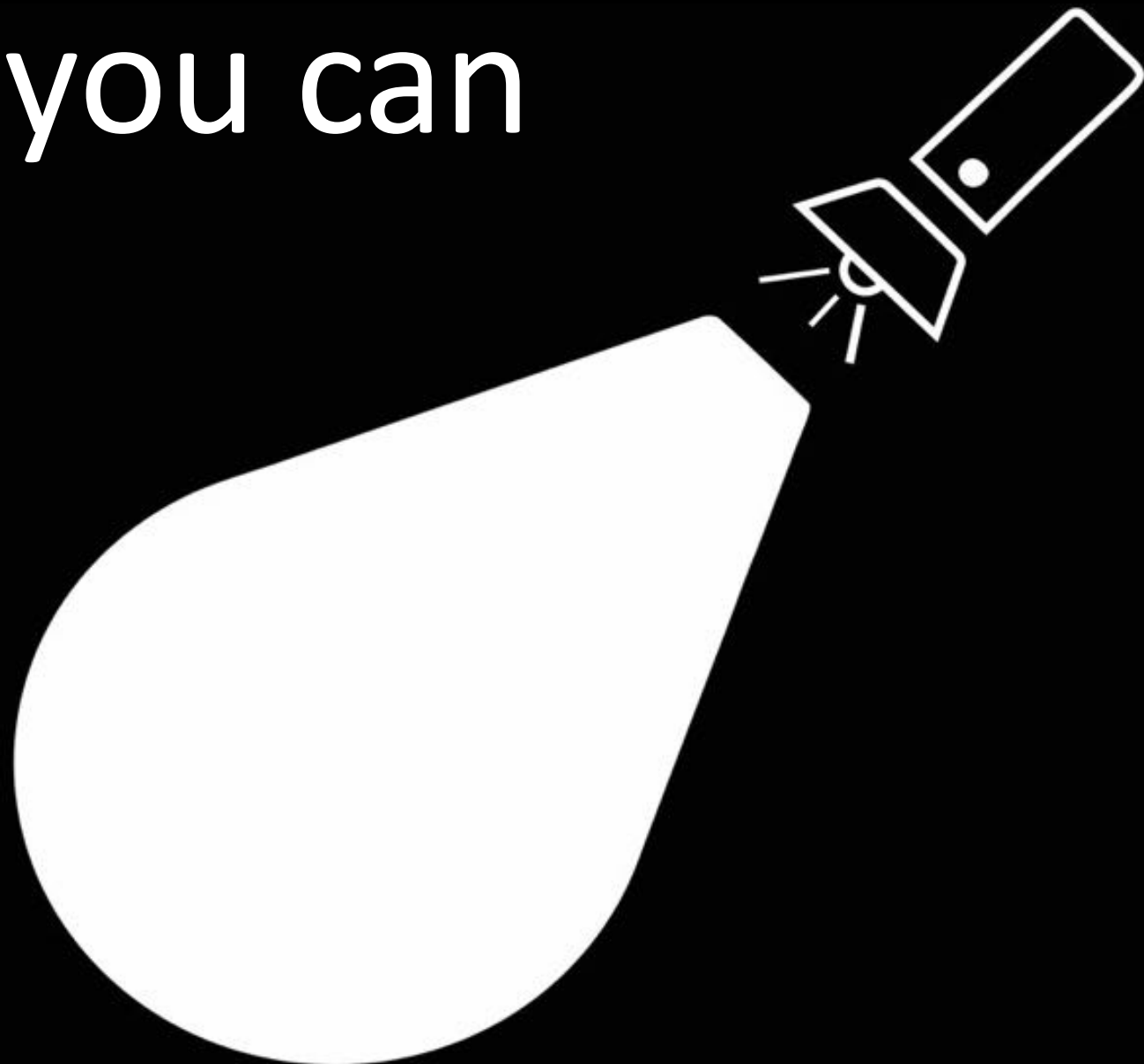
The traffic of your network

Who is the top
bandwidth drawer?

The traffic of your network

With few tools you can know
more than you can

Imagine 😊



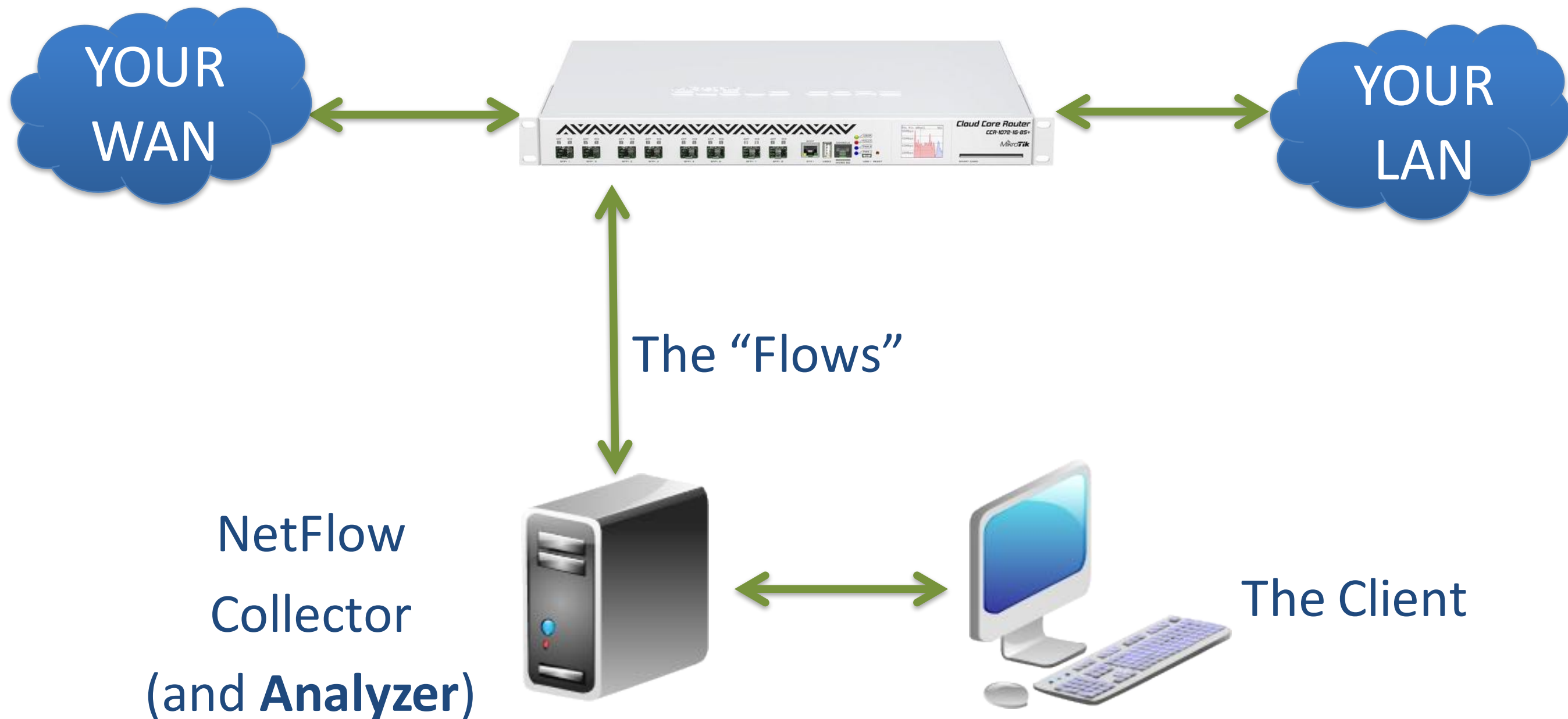
NetFlow in pills

- Is a “common” router’s feature
- **Collect IP traffic statistics**
- Later will **export** them to a **NetFlow Collector**
- They’re called: **flow record**
- The format is template based (since the **Version 9**): expandable for the future

NetFlow in RouterOS

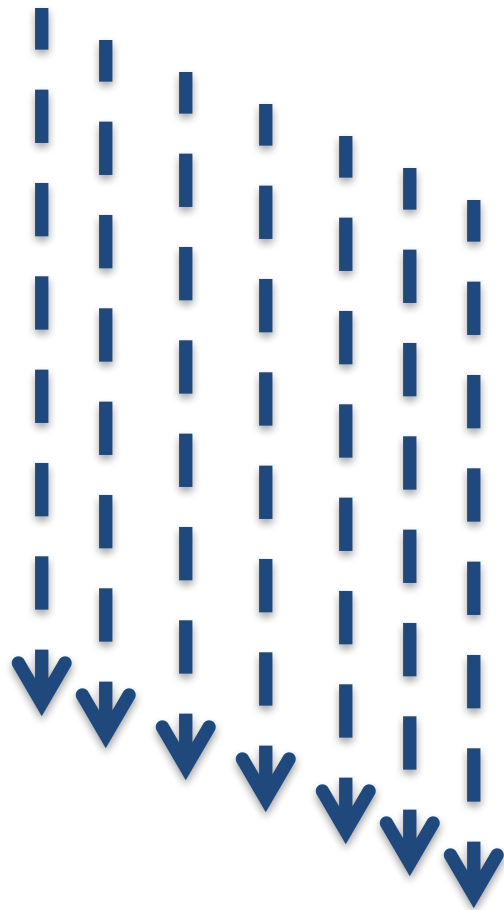
- Yes, is supported!
- Is called: **Traffic Flow** (NetFlow it's a Cisco naming....)
- He's "living" there: **/ip traffic-flow**
- Exist since ROS v. 2.9
- Today support the **Versions 1, 5, 9**
- Check the wiki for the differences 😊

Traffic Flow in action



Two Ingredients

The “Flows”



A NetFlow
Collector
(and Analyzer)



Traffic Flow limitations

- Up to RouterOS v. 6.0 will export **only** RX traffic of an interface
- Currently RouterOS does not export BGP AS numbers ☹️
- Hope to see implemented soon 😊

The “boring” part

(but very short)

Packet transport protocol

- The records are exported using UDP
- The standard port is the 2055 (user defined)
- The router does not keep track of flow records already exported
- If a NetFlow packet is dropped all contained records are lost forever
- Doesn't export the "payloads"
- The content isn't encrypted

General structure (v9)

NetFlow Packet header

— Template

- NetFlow **Record 1**
- NetFlow **Record 2**
- NetFlow **Record n**

— Template

- NetFlow **Record $n + 1$**
- NetFlow **Record $n + 2$**
- NetFlow **Record $n + n$**

The packet header

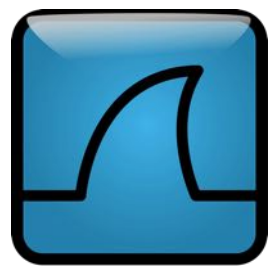
- Version number (v1, v5, v7, v8, v9)
- Sequence number
- Timestamp
- Number of records (v5 or v8) or list of templates and records (v9)

The Template format

- ID
- length
- Field Count
- Field 1 Type
- Field 1 Length
- Field 2 Type
- Field 2 Length
- Field N Type
- Field N Length

(some) v9 Fields

IN_BYTES	DIRECTION	SRC_AS
OUT_BYTES	IPV4_NEXT_HOP	DST_AS
IN_PKTS	IPV6_SRC_ADDR	BGP_IPV4_NEXT_HOP
OUT_PKTS	IPV6_DST_ADDR	IP_PROTOCOL_VERSION
PROTOCOL	ICMP_TYPE	MPLS_LABEL_(1-10)
SRC_TOS	IN_SRC_MAC	IF_NAME
TCP_FLAGS	IN_DST_MAC	IF_DESC
L4_SRC_PORT	OUT_DST_MAC	
L4_DST_PORT	OUT_SRC_MAC	FORWARDING STATUS (lots of subcodes!!!)
IPV4_SRC_ADDR	SRC_VLAN	
IPV4_DST_ADDR	DST_VLAN	

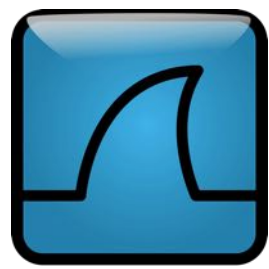


Live view

The packet Header

731 1... 3 CFLOW 1446 total: 20 (v9) records Obs-Doma

- ▶ Frame 731: 1446 bytes on wire (11568 bits), 1446 bytes captured (11568 bits)
- ▶ Ethernet II, Src: AxiomTec_52:93:bc (00:60:e0:52:93:bc), Dst: Routerbo_cf:4c:74 (00:0c:42:cf:4c:74)
- ▶ Internet Protocol Version 4, Src: 91.200.120.33, Dst: 91.200.120.1
- ▶ User Datagram Protocol, Src Port: 2055 (2055), Dst Port: 2055 (2055)
- ▼ Cisco NetFlow/IPFIX
 - Version: 9
 - Count: 20
 - SysUptime: -854209.489001904 seconds
 - ▶ Timestamp: Feb 23, 2016 12:49:08.000000000 CET
 - FlowSequence: 45665169
 - SourceId: 0
 - ▶ FlowSet 1 [id=256] (20 flows)



Live view

The Template

▼ Cisco NetFlow/IPFIX

Version: 9

Count: 20

SysUptime: -854209.489001904 seconds

► Timestamp: Feb 23, 2016 12:49:08.000000000 CET

FlowSequence: 45665169

SourceId: 0

▼ FlowSet 1 [id=256] (20 flows)

FlowSet Id: (Data) (256)

FlowSet Length: 1384

[\[Template Frame: 19\]](#)

► Flow 1

► Flow 2

► Flow 3

► Flow 4

► Flow 5

► Flow 6

► Flow 7

► Flow 8

► Flow 9

► Flow 10

► Flow 11

► Flow 12

► Flow 13

► Flow 14

► Flow 15

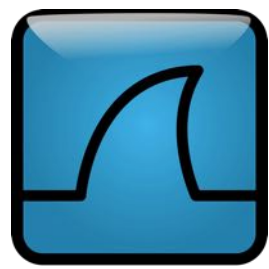
► Flow 16

► Flow 17

► Flow 18

► Flow 19

► Flow 20



Live view

One Flow

▼ Flow 1

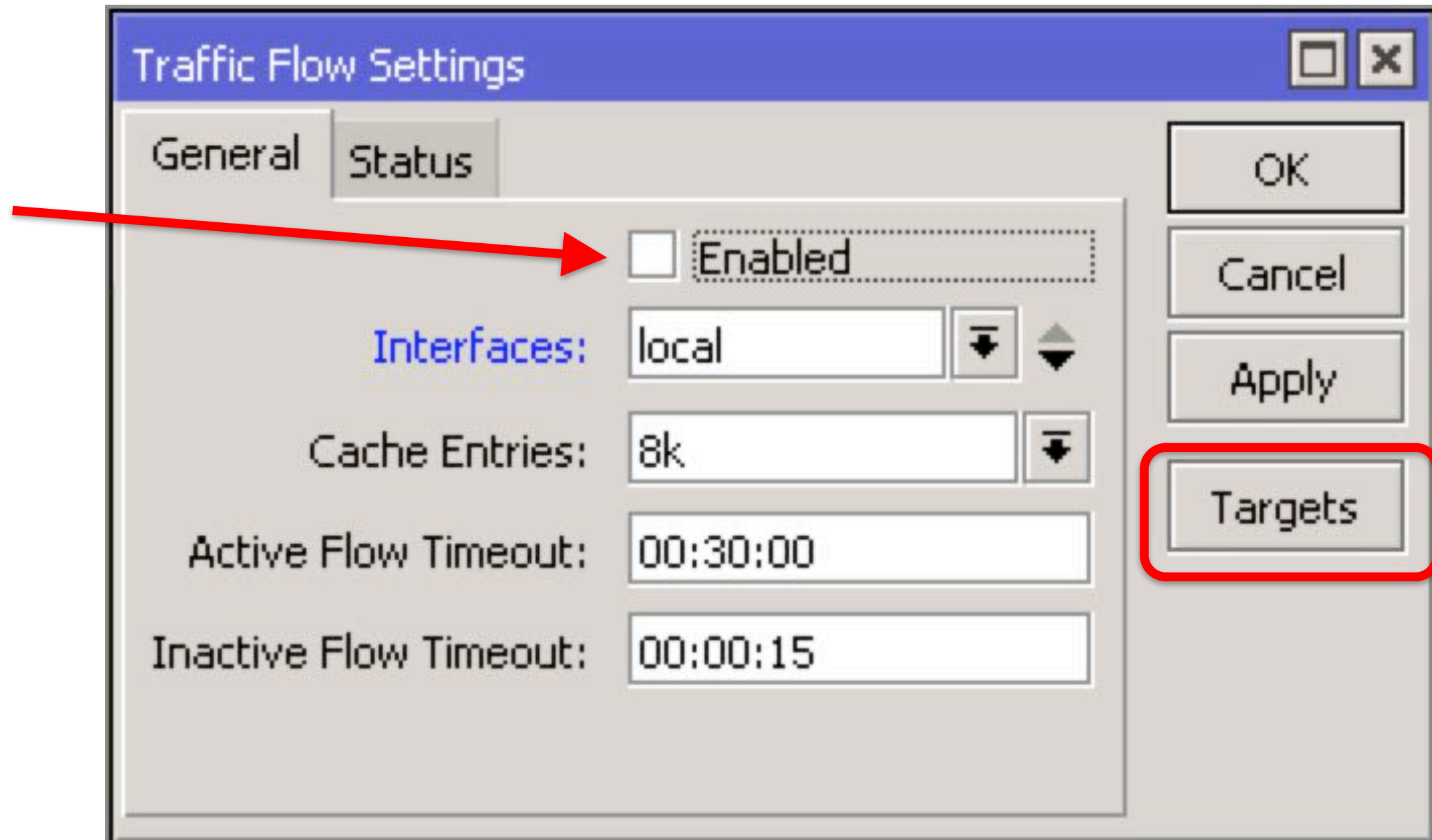
- ▼ [Duration: 1.290000000 seconds (switched)]
 - StartTime: 854193.160000000 seconds
 - EndTime: 854194.450000000 seconds
 - Packets: 4
 - Octets: 160
 - InputInt: 8
 - OutputInt: 3
 - SrcAddr: 51.200.120.12
 - DstAddr: 85.73.239.223
 - Protocol: TCP (6)
 - IP ToS: 0x00
 - SrcPort: 64866 (64866)
 - DstPort: 61053 (61053)
 - NextHop: 80.249.208.179
 - DstMask: 0
 - SrcMask: 0
 - TCP Flags: 0x14
 - Destination Mac Address: AxiomTec_52:93:bc (00:60:e0:52:93:bc)
 - Post Source Mac Address: AxiomTec_06:02:d4 (00:60:e0:06:02:d4)
 - Post NAT Source IPv4 Address: 51.200.120.12
 - Post NAT Destination IPv4 Address: 85.73.239.223
 - Post NAT Source Transport Port: 0
 - Post NAT Destination Transport Port: 0

Summary

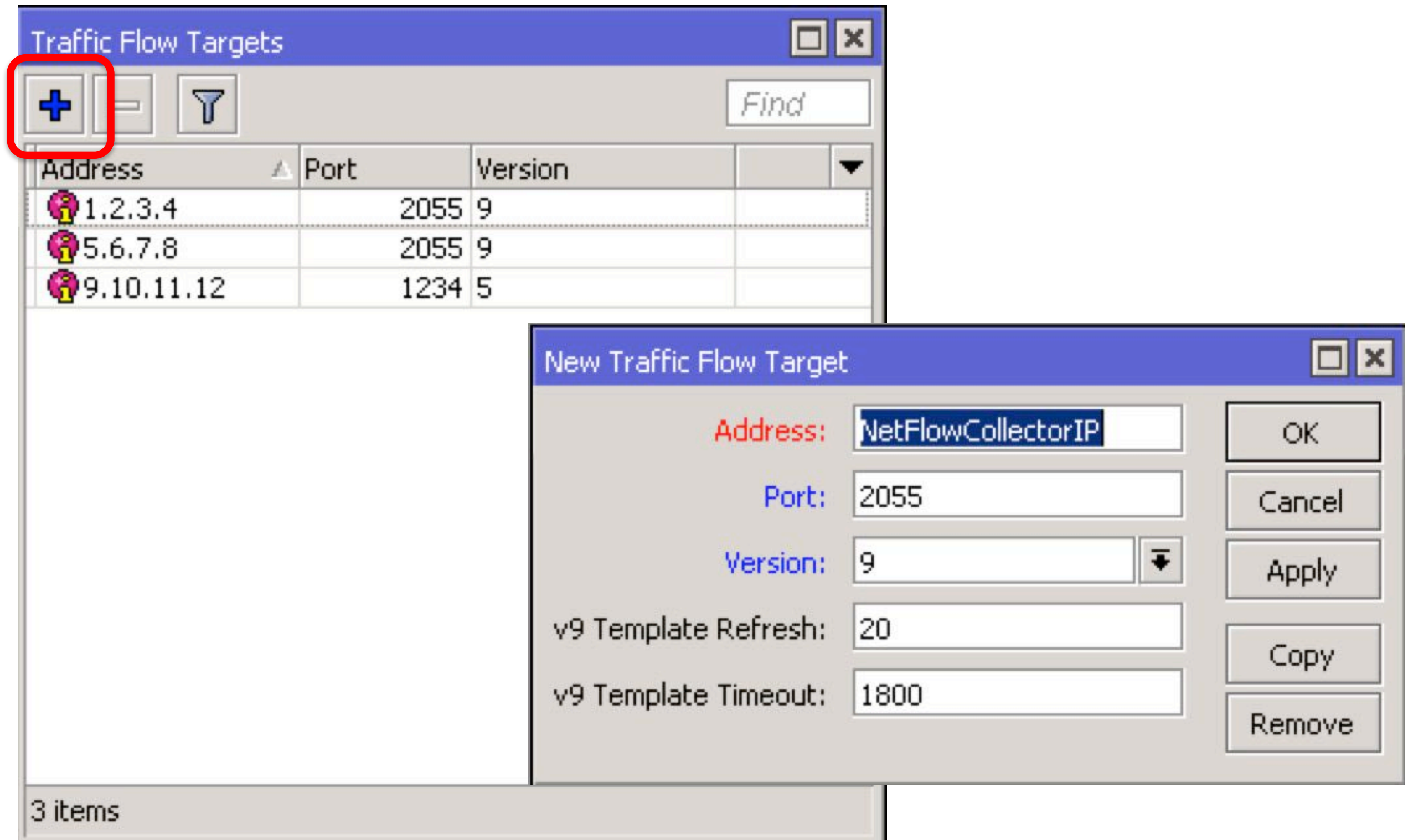
The Traffic Flow will “export” almost “everything” except the effective “payload”

Setting up (the router)

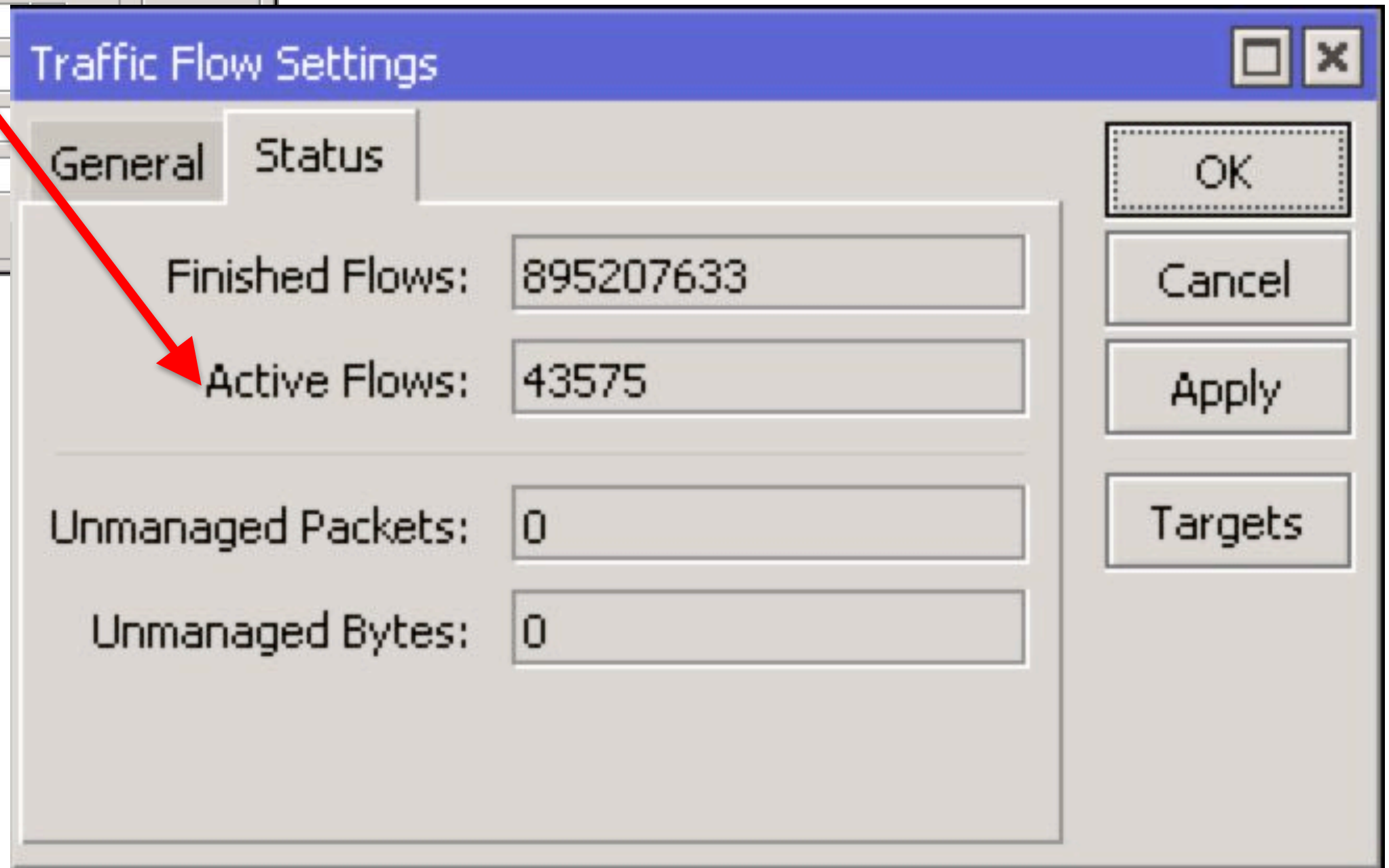
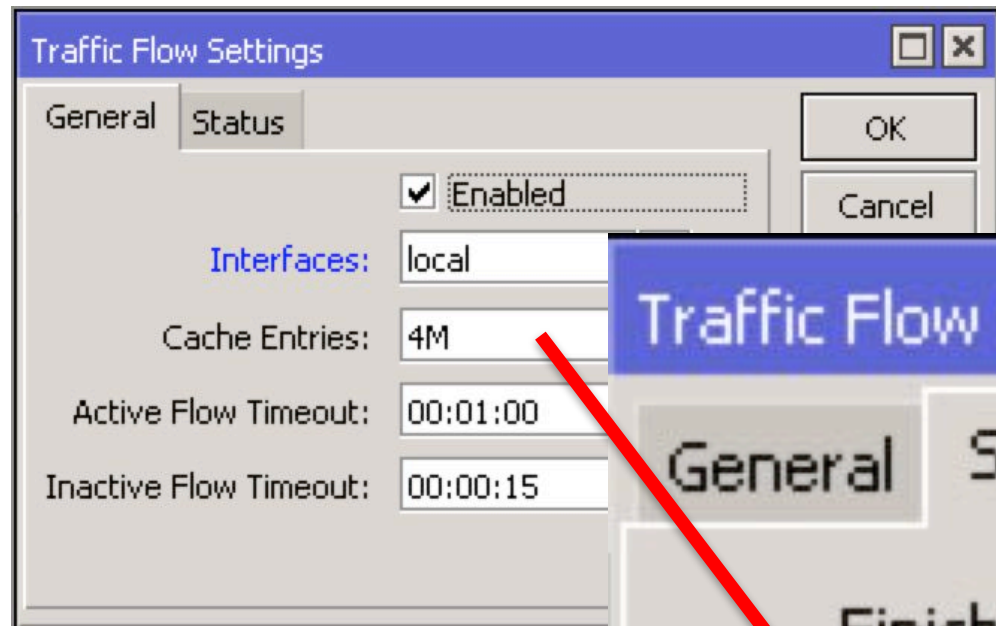
IP → Traffic Flow



IP → Traffic Flow - Targets



IP → Traffic Flow → Status



How much resources
will take (the flows) ?

Traffic Flow “traffic”

There is not an exact formula to calculate the exported “flows”, but I’ll show you a “live” example.

Traffic Flow “traffic”

The router traffic

Interface <ether8>			
General	Ethernet	Status	Traffic
Tx/Rx Rate:		297.9 Mbps	/ 39.8 Mbps
Tx/Rx Packet Rate:		33 166 p/s	/ 25 196 p/s

The sessions

2050 items out of 89656

The “Flows”

Eth. P... ▲	Pro...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate
800 (ip)	17 ...	91.222.122.33:2055	91.222.122.33:2055			0 bps	1130.3 kbps

The NetFlow Collectors (and Analyzer)

What I need now?

- A **Collector** will collect the flows exported by your router.
- An **Analyzer** will make these data readable and usable to you.
- Most of the Collectors are Analyzer also.

Which one?

- Open source;
- Closed source;
- For Windows;
- For Linux;
- On the Cloud;
- Paid Vs Free;

Examples



ManageEngine
NetFlow Analyzer

PRTG
NETWORK
MONITOR

 **POLYGRAPH.io**

 **Scrutinizer**TM
NetFlow & sFlow Analyzer

 **Colasoft**[®]
Get to Know Your Network

Which one?

I'm not a reseller or a sales representative of these brands.

Search on the web and “try before buy” (when possible).

Which one?

In this presentation I'll show you an example using the cloud services provided by:



<http://polygraph.io>

The most interesting part:
What can I see?????

Which traffic?

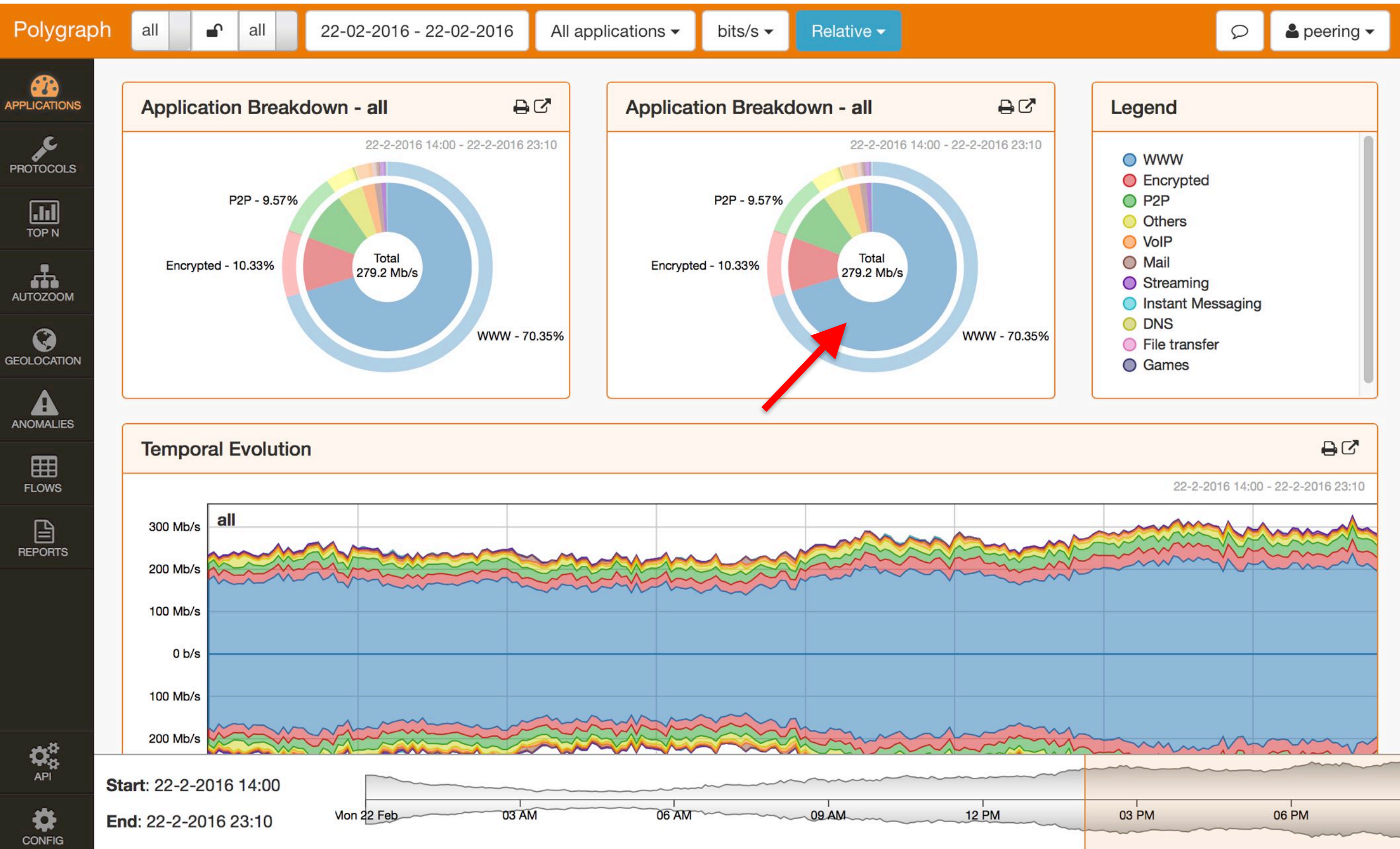
Just few examples:

- Bandwidth monitoring
- Applications Used
- Identify visited domains
- Top talkers (customers and host)
- Geolocate traffic.
- Attacks detection.

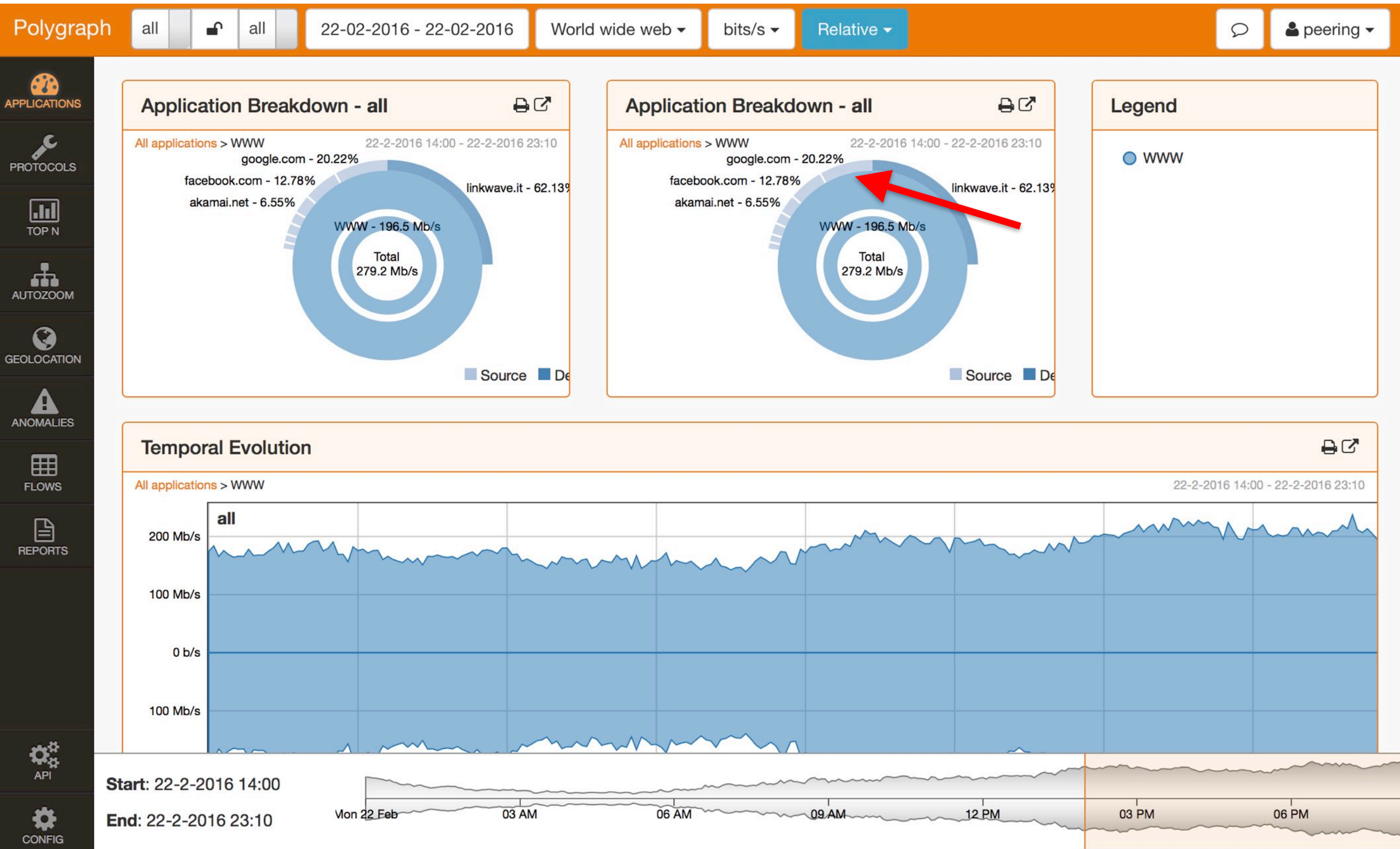
Which traffic?

- And since RouterOS 6.33 the **fastpath**

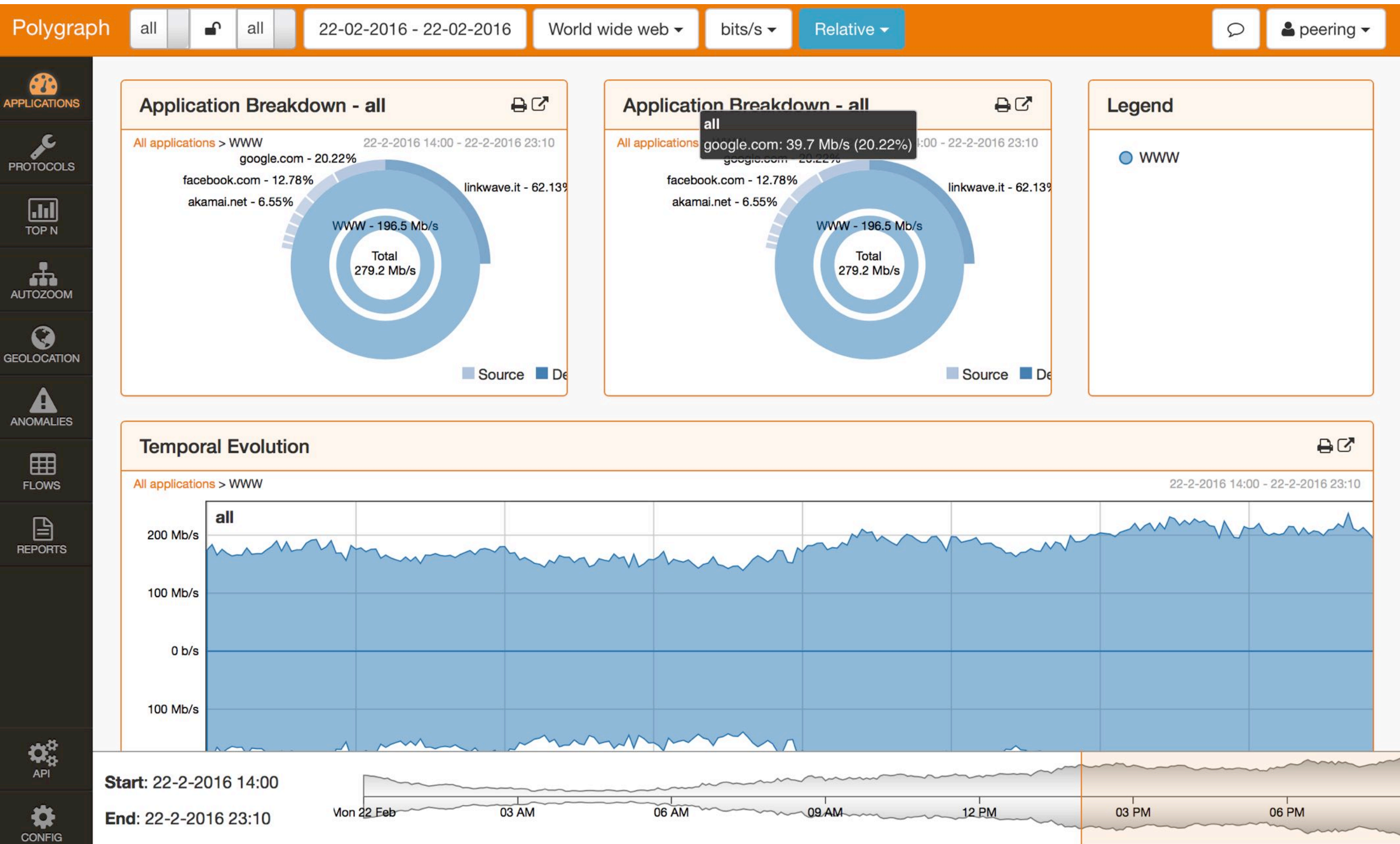
“Live” demo



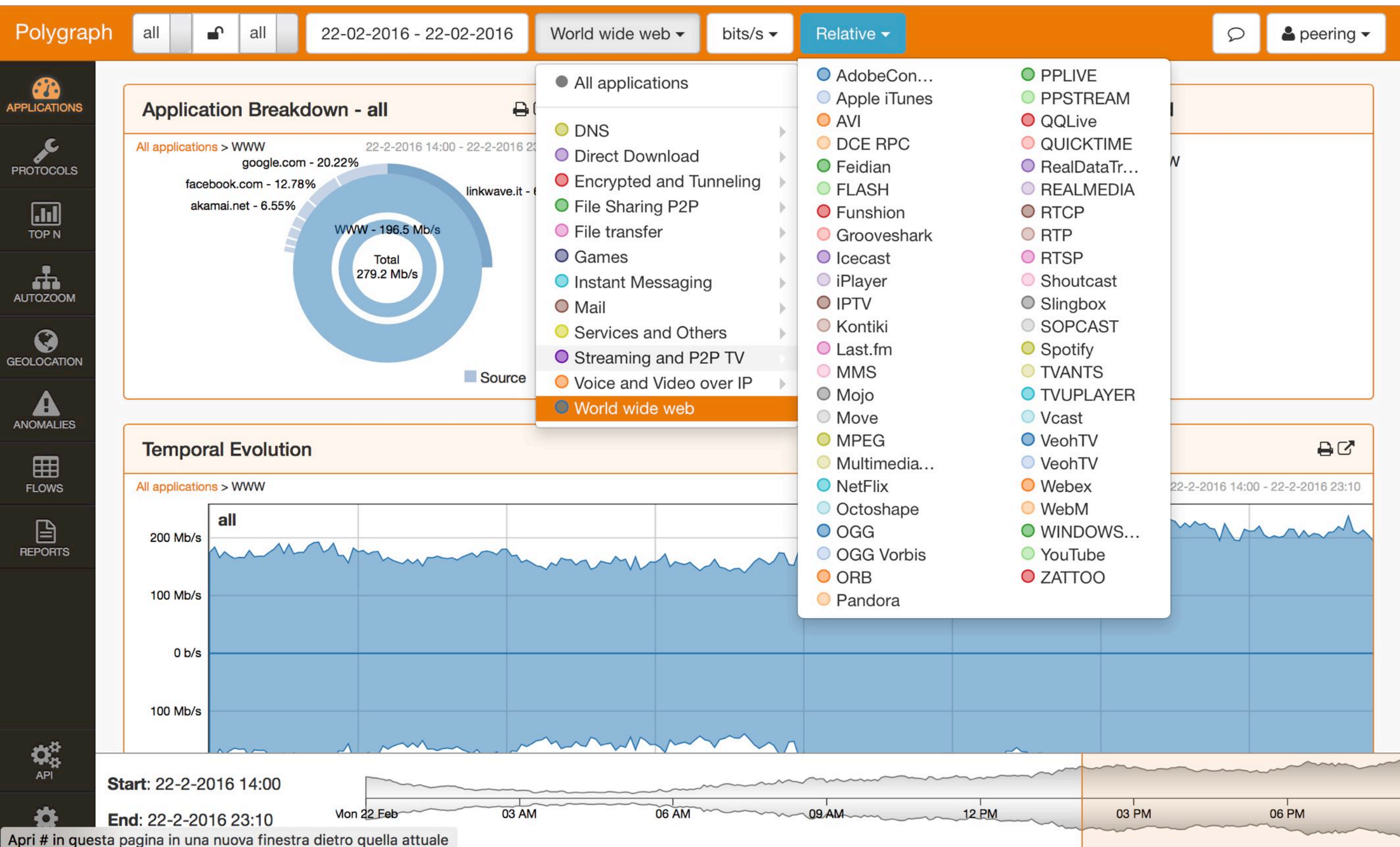
“Live” demo



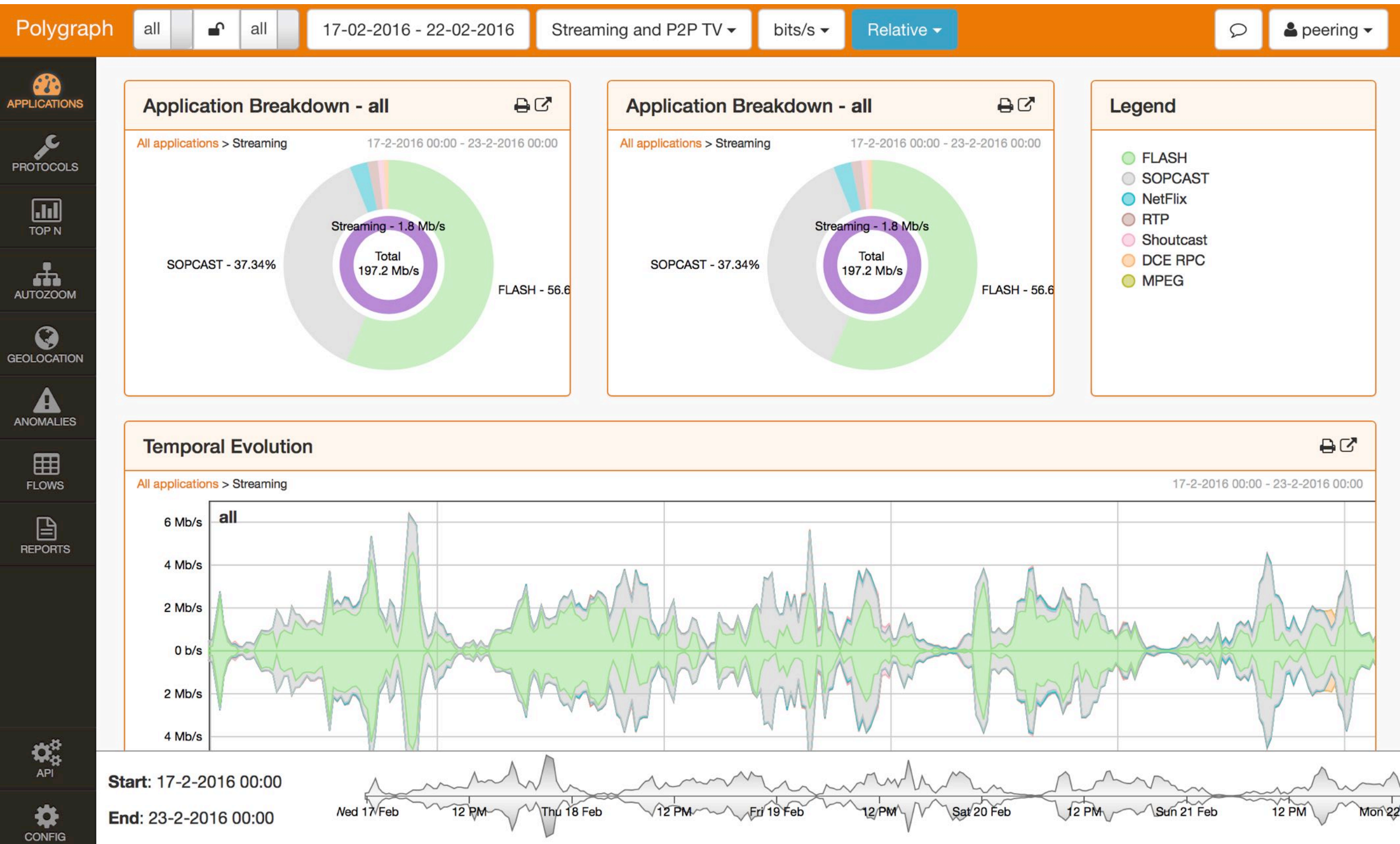
“Live” demo



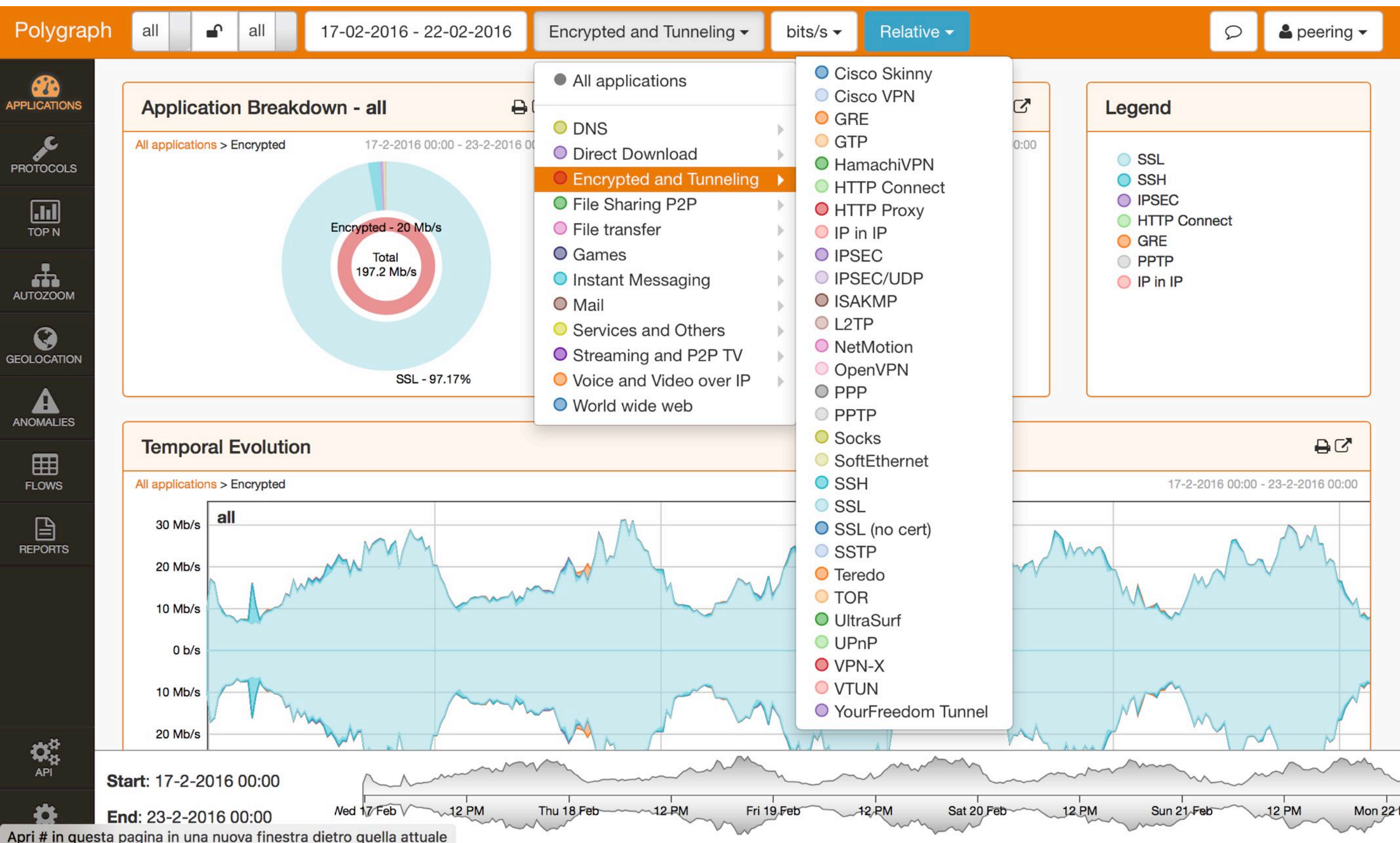
“Live” demo



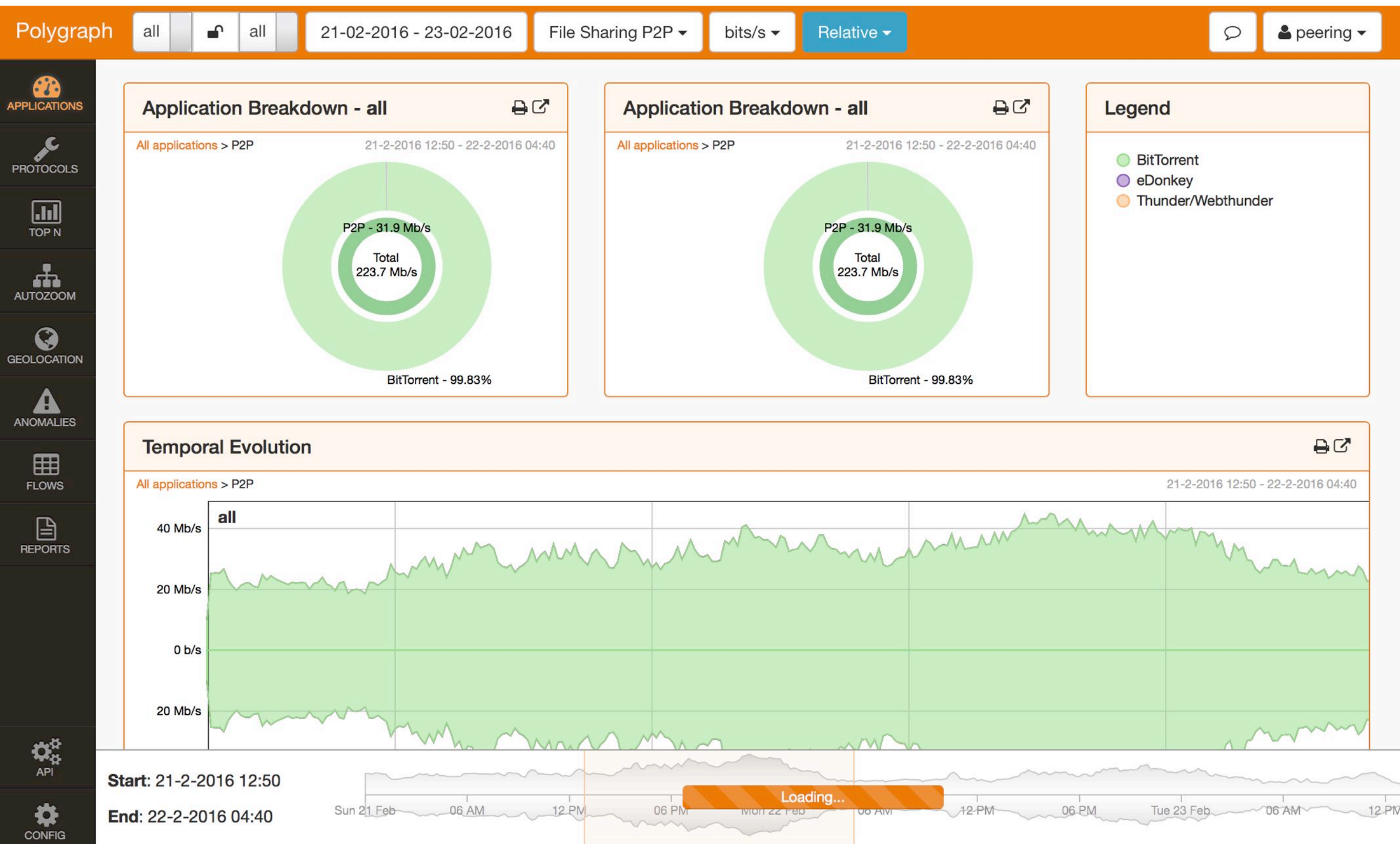
“Live” demo



“Live” demo



“Live” demo



“Live” demo

- CitrixOnline GotoMeeting
- FiCall
- Generic Voice
- H323
- IAX
- Iskoot
- Lync
- MGCP
- MyPeople
- NOE
- ooVoo
- Scydo
- SIP
- Skype
- Tango
- TeamSpeak
- Truphone
- Ventrilo
- Viber
- VoipSwitch VoIP Tunnel

- AdobeCon...
- Apple iTunes
- AVI
- DCE RPC
- Feidian
- FLASH
- Funshion
- Grooveshark
- Icecast
- iPlayer
- IPTV
- Kontiki
- Last.fm
- MMS
- Mojo
- Move
- MPEG
- Multimedia...
- NetFlix
- Octoshape
- OGG
- OGG Vorbis
- ORB
- Pandora

- PPLIVE
- PPSTREAM
- QQLive
- QUICKTIME
- RealDataTr...
- REALMEDIA
- RTCP
- RTP
- RTSP
- Shoutcast
- Slingbox
- SOPCAST
- Spotify
- TVANTS
- TVUPLAYER
- Vcast
- VeohTV
- VeohTV
- Webex
- WebM
- WINDOWS...
- YouTube
- ZATTOO

- Gmail
- IMAP
- IMAPs
- Lotus Notes
- POP
- POPS
- SMTP
- SMTPs

“Live” demo

● Activesync	● LDP	● SNMP	● eBuddy
● AFP	● LPD	● Socrates	● Fring
● Apple	● Mapi	● SSDP	● Gadu-Gadu
● BGP	● msSQL	● STUN	● Goober
● Blackberry	● MySQL	● Syslog	● Google Talk
● Citrix	● NETBIOS	● TDS	● IMO
● CitrixGoTo	● NetFlow/IP...	● TeamViewer	● IMplus
● collectd	● NFS	● Telnet	● IRC
● ComodoUnite	● NTP	● Tunnelvoice	● Jabber
● Corba	● Oracle	● Ubuntu ONE	● MEEBO
● DHCP	● OSPF	● UltraBac	● MSN
● DHCPv6	● PCAnywhere	● Usenet	● MSRP
● EGP	● PostgreSQL	● VMWare	● NIMBUZZ
● I23V5	● RADIUS	● VNC	● Oscar
● ICMP	● RDP	● VRRP	● Paltalk
● ICMPv6	● RemoteScan	● WAP-WSP	● POPO
● IGMP	● RSync	● WAP-WTLS	● QQ
● IPP	● SAP	● WAP-WTP-...	● Unencrypted Jabber
● JAP	● SCTP	● WebDAV	● WhatsApp
● JBK3000	● sFlow	● Whois-DAS	● XDCC
● Kerberos	● Skinny	● WindowsU...	
● LDAP	● SMB/CIFS	● XDMCP	

“Live” demo

- Armagetron
- Battlefield
- ClubPenguin
- CrossFire
- Dofus
- Fiesta
- Florensia
- GameKit
- Guild Wars
- Halflife2
- MapleStory
- PS3
- QQGame
- Quake
- rFactor
- Second Life
- SplashFighter
- Steam
- Warcraft III
- Wii
- World of Kung Fu
- World of Warcraft
- XBOX

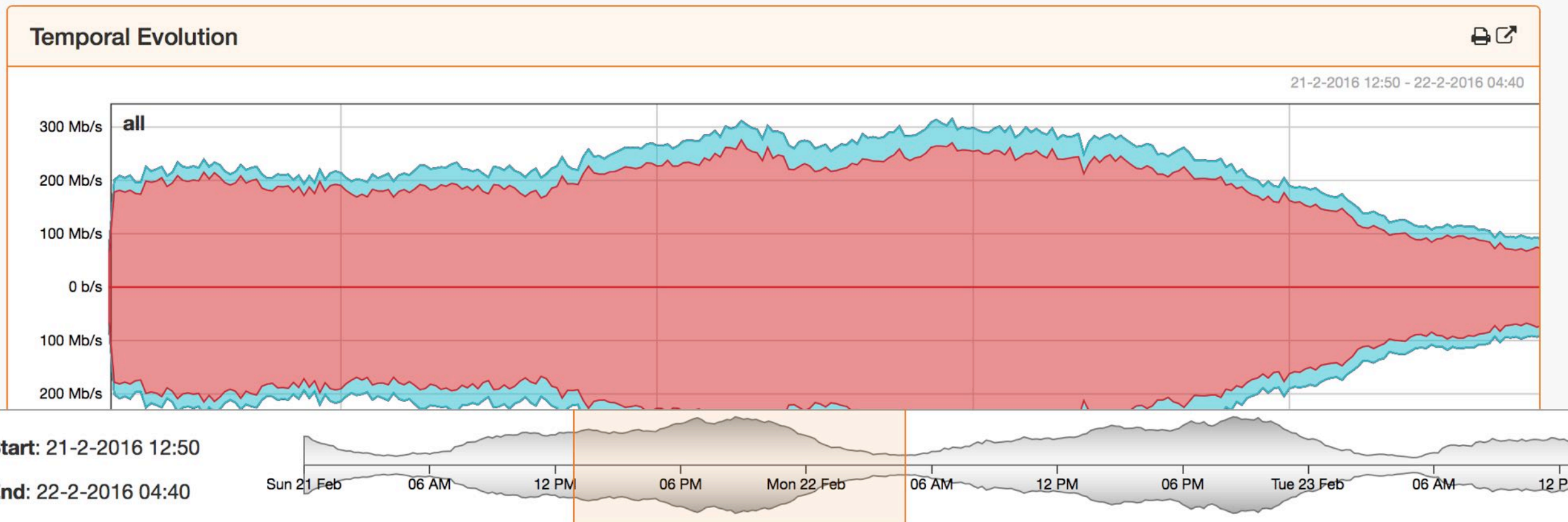
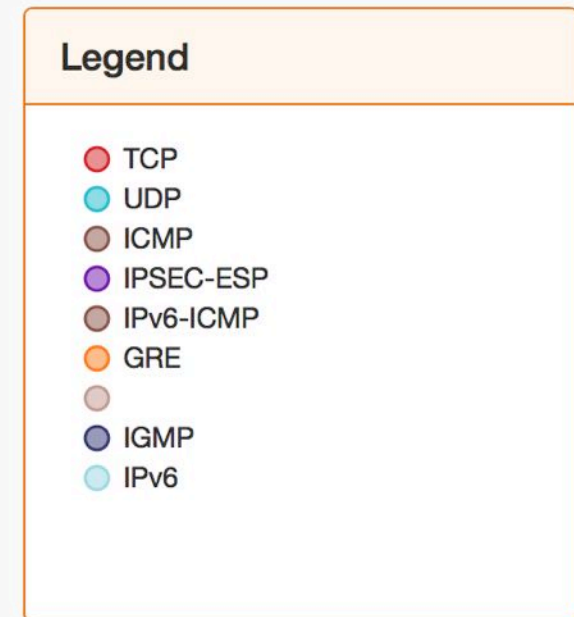
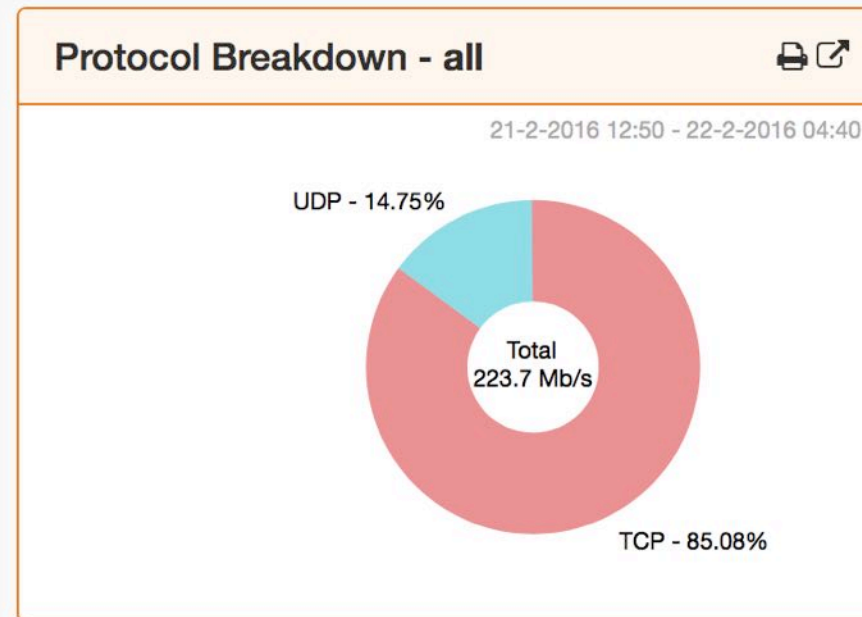
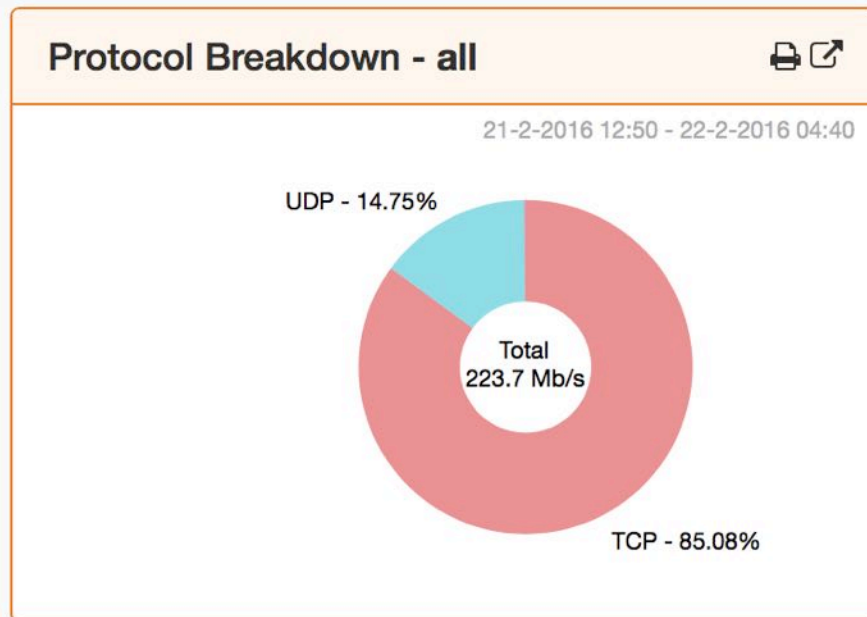
- Aimini
- ANtsP2P
- AppleJuice
- Ares
- Bitcoin Mining
- BitTorrent
- DirectConnect
- eDonkey
- eDonkey
- Freenet
- Gnutella
- Gnutella
- iMesh
- Kazaa/Fasttrack
- KaZaa/Fasttrack
- Manolito
- Mute
- OFF
- OpenFT
- Pando
- Soulseek
- Soulseek
- StealthNet
- Thunder/Webthunder
- UUSEE
- WinMX
- WINNY

- Cisco Skinny
- Cisco VPN
- GRE
- GTP
- HamachiVPN
- HTTP Connect
- HTTP Proxy
- IP in IP
- IPSEC
- IPSEC/UDP
- ISAKMP
- L2TP
- NetMotion
- OpenVPN
- PPP
- PPTP
- Socks
- SoftEthernet
- SSH
- SSL
- SSL (no cert)
- SSTP
- Teredo
- TOR
- UltraSurf
- UPnP
- VPN-X
- VTUN
- YourFreedom Tunnel

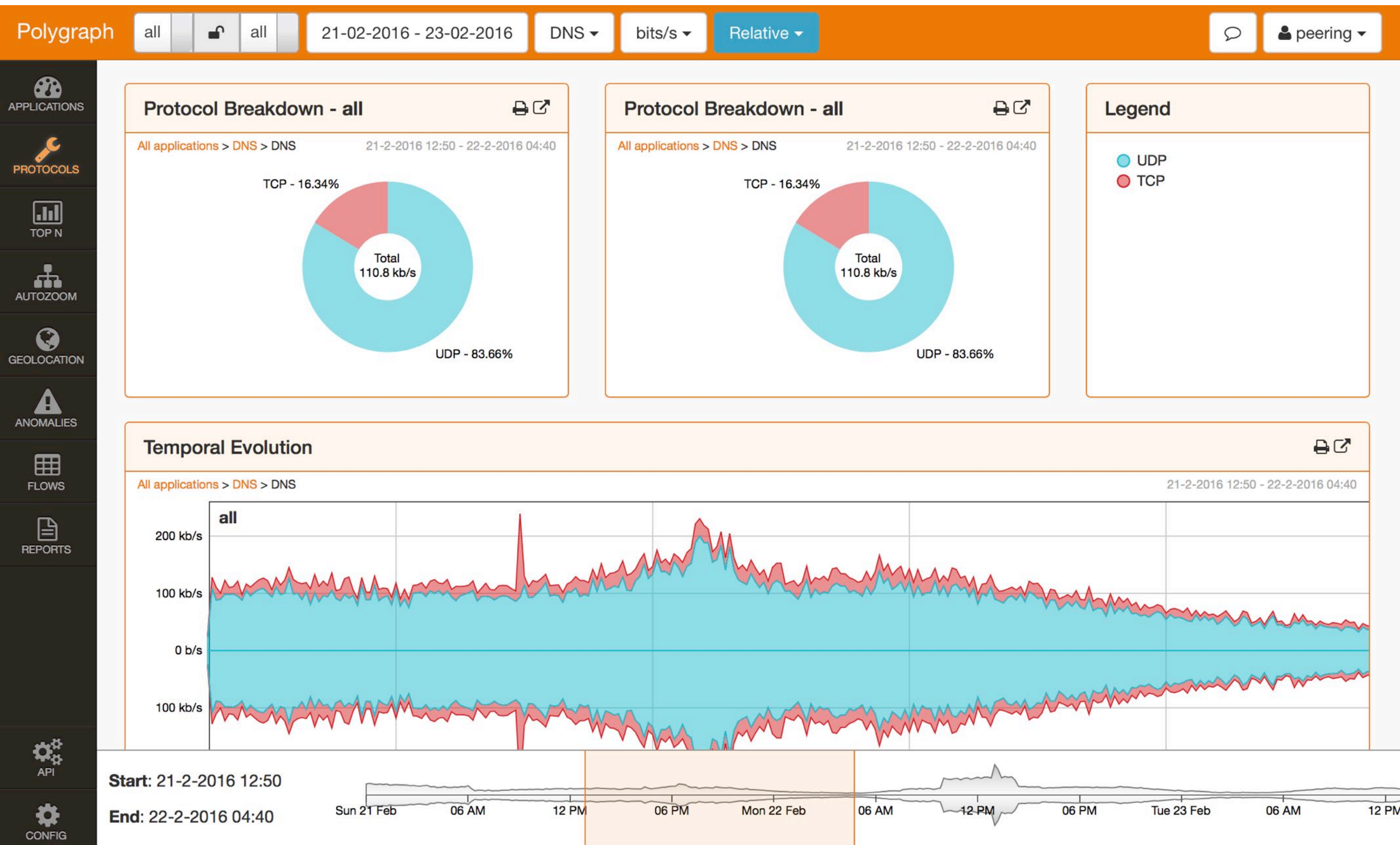
- Apple iCloud
- Dropbox
- FTP
- TFTP
- DirectDownloadLink
- Filetopia
- Skyfile postpaid
- Skyfile prepaid
- Skyfile rudics
- Wuala
- DNS
- LLMNR
- MulticastDNS

“Live” demo

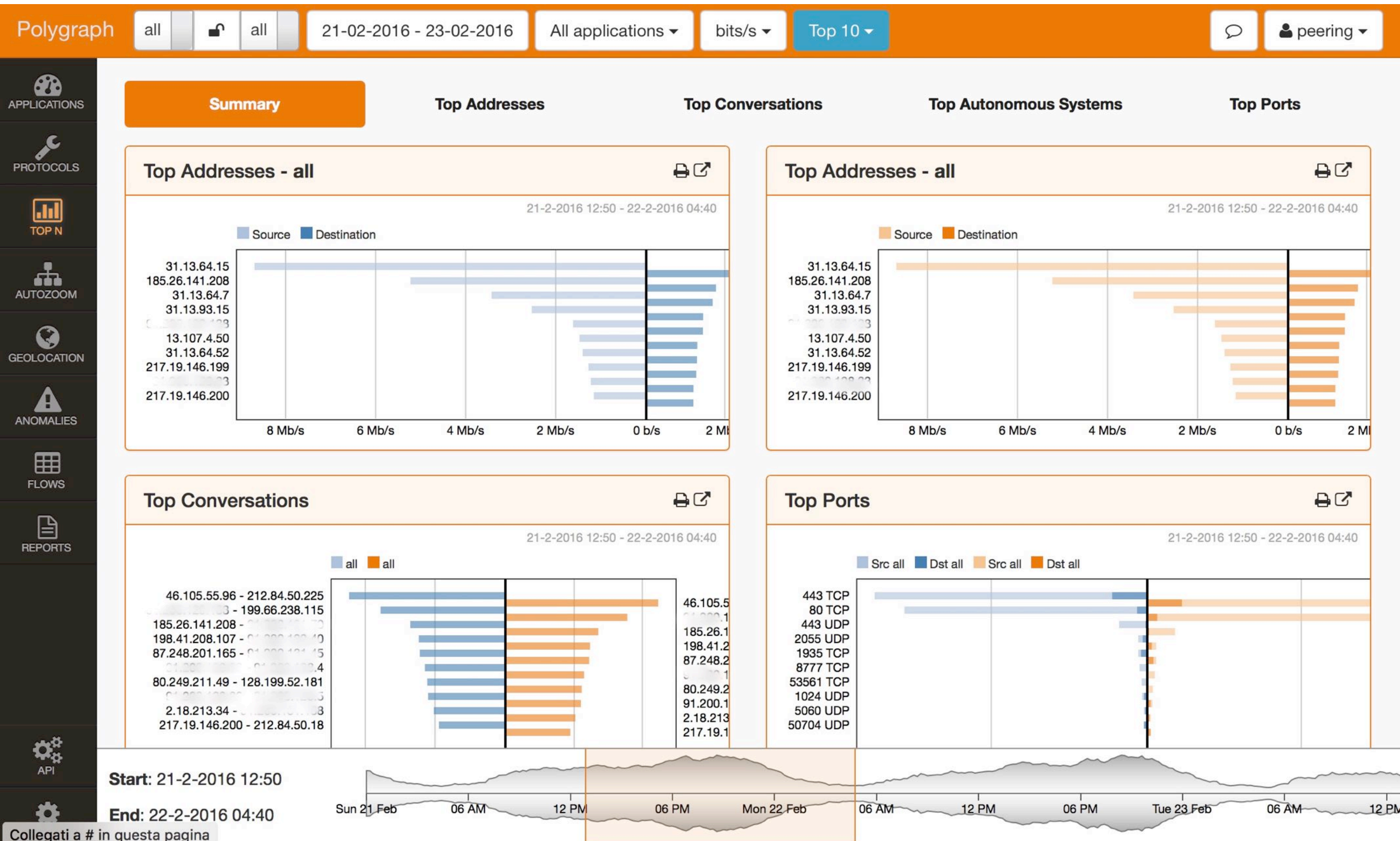
- APPLICATIONS
- PROTOCOLS
- TOP N
- AUTOZOOM
- GEOLOCATION
- ANOMALIES
- FLows
- REPORTS
- API
- CONFIG



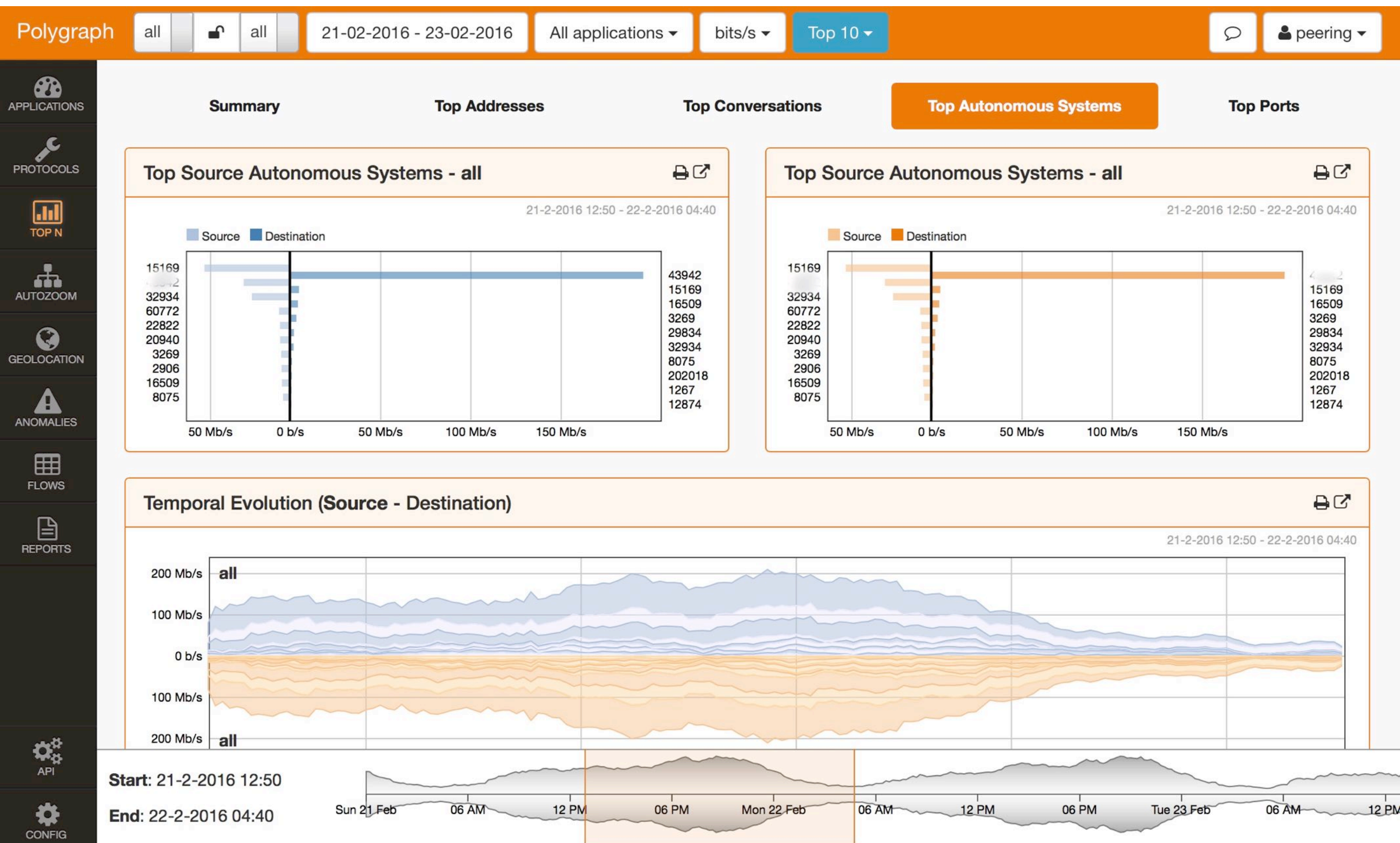
“Live” demo



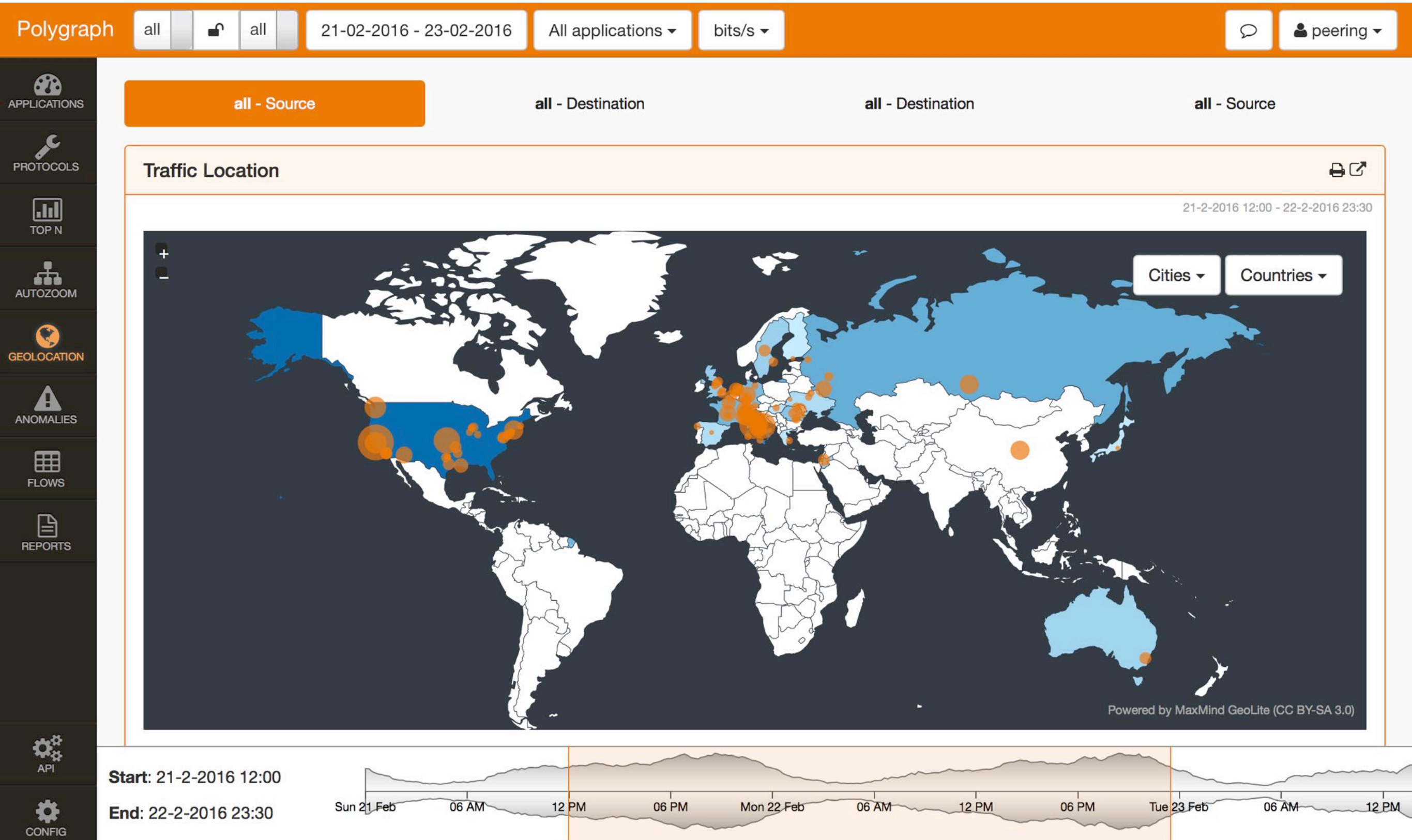
“Live” demo



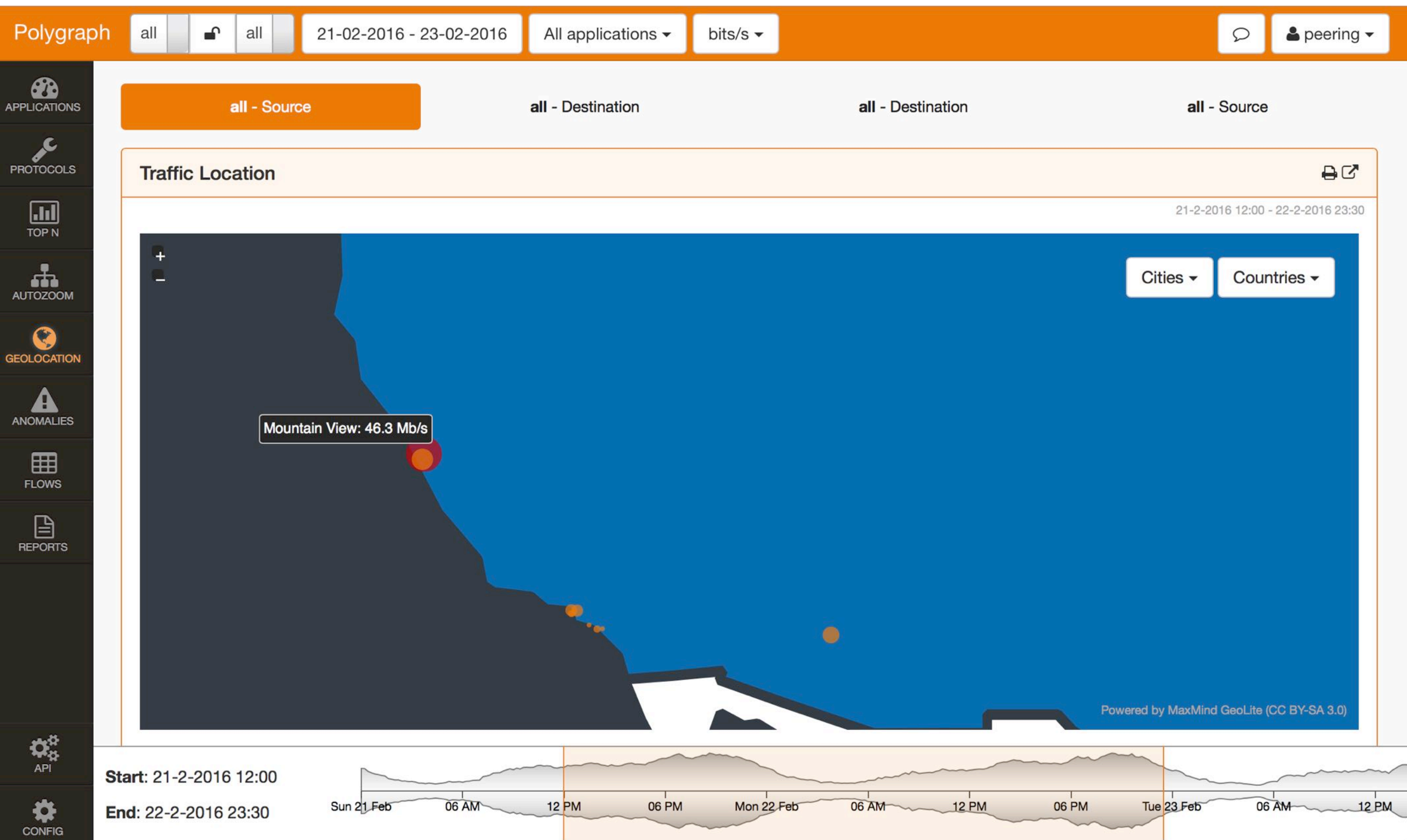
“Live” demo



“Live” demo



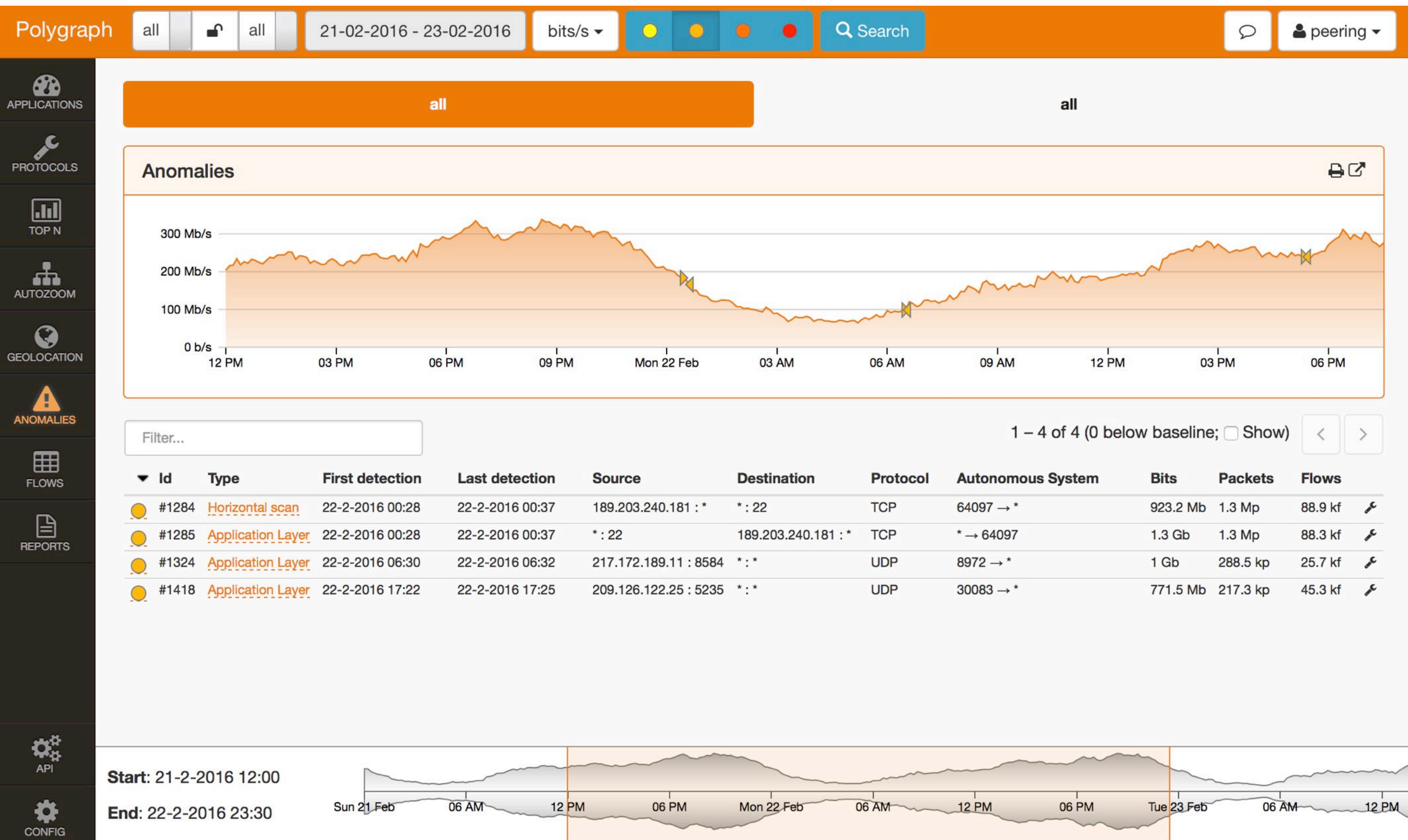
“Live” demo



“Live” demo

You can also make reports,
watch and export the store
flows, and

“Live” demo



Security

The security is another application of the Traffic Flow.

My contents will stop here, hope you'll enjoy a dedicated presentation this evening.

Wrap up

- ✓ With the Traffic Flow and a NetFlow Analyzer you can know what happen in your network and the kind of traffic exchanged by your customers
- ✓ From this privileged point of view you can manage, plan and prevent the “things” of your network.

Wrap up

✓ I hope you'll deploy soon your privileged “point of observation” 😊

Thank you!

Q & A

<http://training.grifonline.it>
training@grifonline.it