Leverage Innovation: ntopng

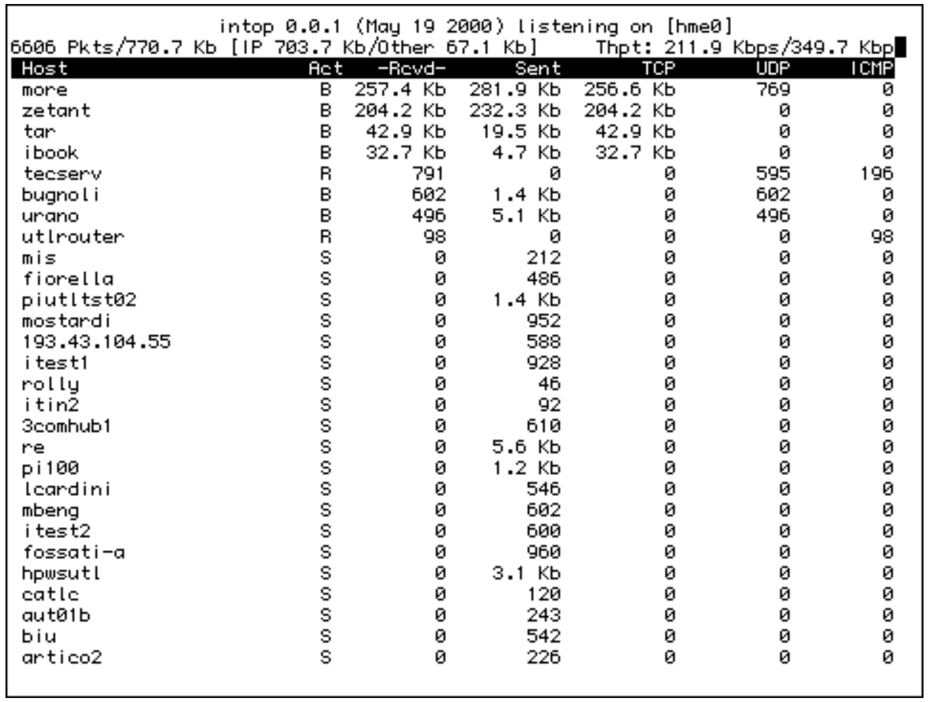
Luca Deri <deri@ntop.org>
@lucaderi

© 2017 - ntop.org

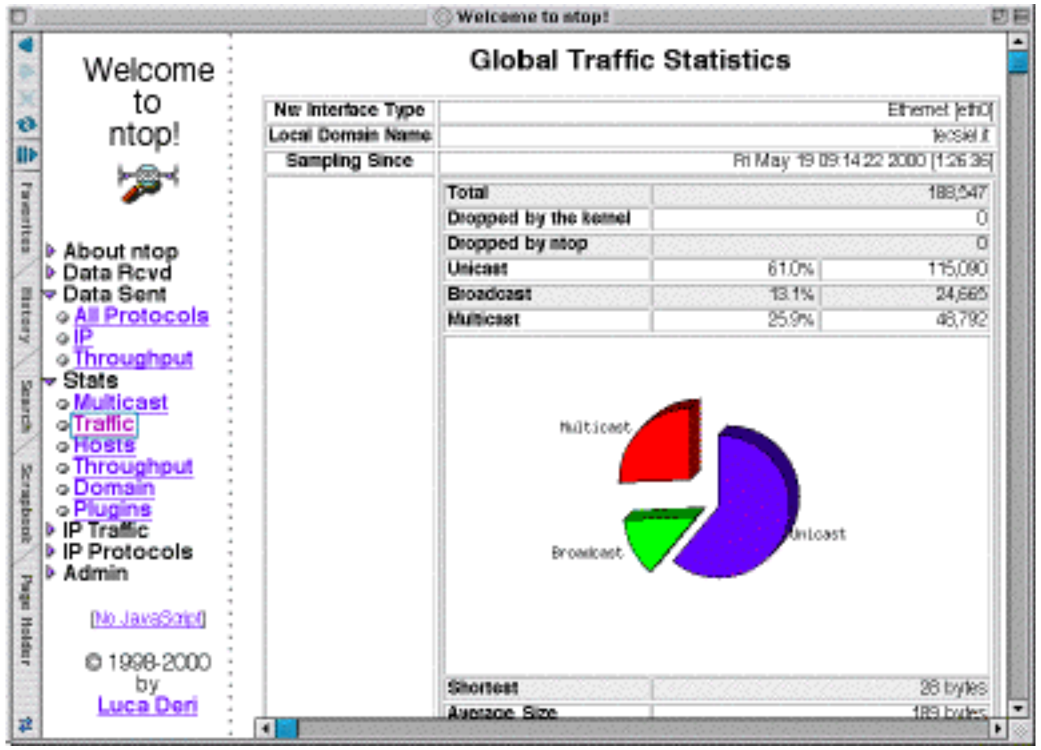
20 Years of ntop: 09/97-09/17

Welcome to ntop.org

As we enjoy great advantages from inventions of others, we should be glad of an opportunity to serve others by any invention of ours; and this we should do freely and generously.
Benjamin Franklin



```
                intop 0.0.1 (May 19 2000) listening on [hme0]
6606 Pkts/770.7 Kb [IP 703.7 Kb/Other 67.1 Kb]     Thpt: 211.9 Kbps/349.7 Kbp
 Host                     Act   -Rcvd-     Sent       TCP       UDP      ICMP
 more                      B  257.4 Kb  281.9 Kb  256.6 Kb       769        0
 zetant                    B  204.2 Kb  232.3 Kb  204.2 Kb         0        0
 tar                       B   42.9 Kb   19.5 Kb   42.9 Kb         0        0
 ibook                     B   32.7 Kb    4.7 Kb   32.7 Kb         0        0
 tecserv                   R       791         0         0       595      196
 bugnoli                   B       602    1.4 Kb         0       602        0
 urano                     B       496    5.1 Kb         0       496        0
 utlrouter                 R        98         0         0         0       98
 mis                       S         0       212         0         0        0
 fiorella                  S         0       486         0         0        0
 piutltst02                S         0    1.4 Kb         0         0        0
 mostardi                  S         0       952         0         0        0
 193.43.104.55             S         0       588         0         0        0
 itest1                    S         0       928         0         0        0
 rolly                     S         0        46         0         0        0
 itin2                     S         0        92         0         0        0
 3comhub1                  S         0       610         0         0        0
 re                        S         0    5.6 Kb         0         0        0
 pi100                     S         0    1.2 Kb         0         0        0
 lcardini                  S         0       546         0         0        0
 mbeng                     S         0       602         0         0        0
 itest2                    S         0       600         0         0        0
 fossati-a                 S         0       960         0         0        0
 hpwsutl                   S         0    3.1 Kb         0         0        0
 catlc                     S         0       120         0         0        0
 aut01b                    S         0       243         0         0        0
 biu                       S         0       542         0         0        0
 artico2                   S         0       226         0         0        0
```



© 1998-2000 by Luca Deri

Global Traffic Statistics

Nw Interface Type	Ethernet [eth0]
Local Domain Name	tecsiel.it
Sampling Since	Fri May 19 09:14:22 2000 [1:26:36]

Total		188,547
Dropped by the kernel		0
Dropped by ntop		0
Unicast	61.0%	115,090
Broadcast	13.1%	24,665
Multicast	25.9%	48,792
Shortest		28 bytes
Average Size		189 bytes

ntop: Our Tools

- Open Source (https://github.com/ntop)
  - ntopng: Web-based monitoring application
  - PF_RING: Accelerated RX/TX on Linux
  - nDPI: Deep Packet Inspection Toolkit
  - OZBC: Compressed Bitmap Index
- Proprietary
  - PF_RING ZC: 1/10/40/100 Gbit Line rate.
  - nProbe: 10G NetFlow/IPFIX Probe
  - nProbe Cento: flows+packets+security
  - n2disk/disk2n Network-to-disk and disk-to-network.
  - nScrub: Software DDoS Mitigation

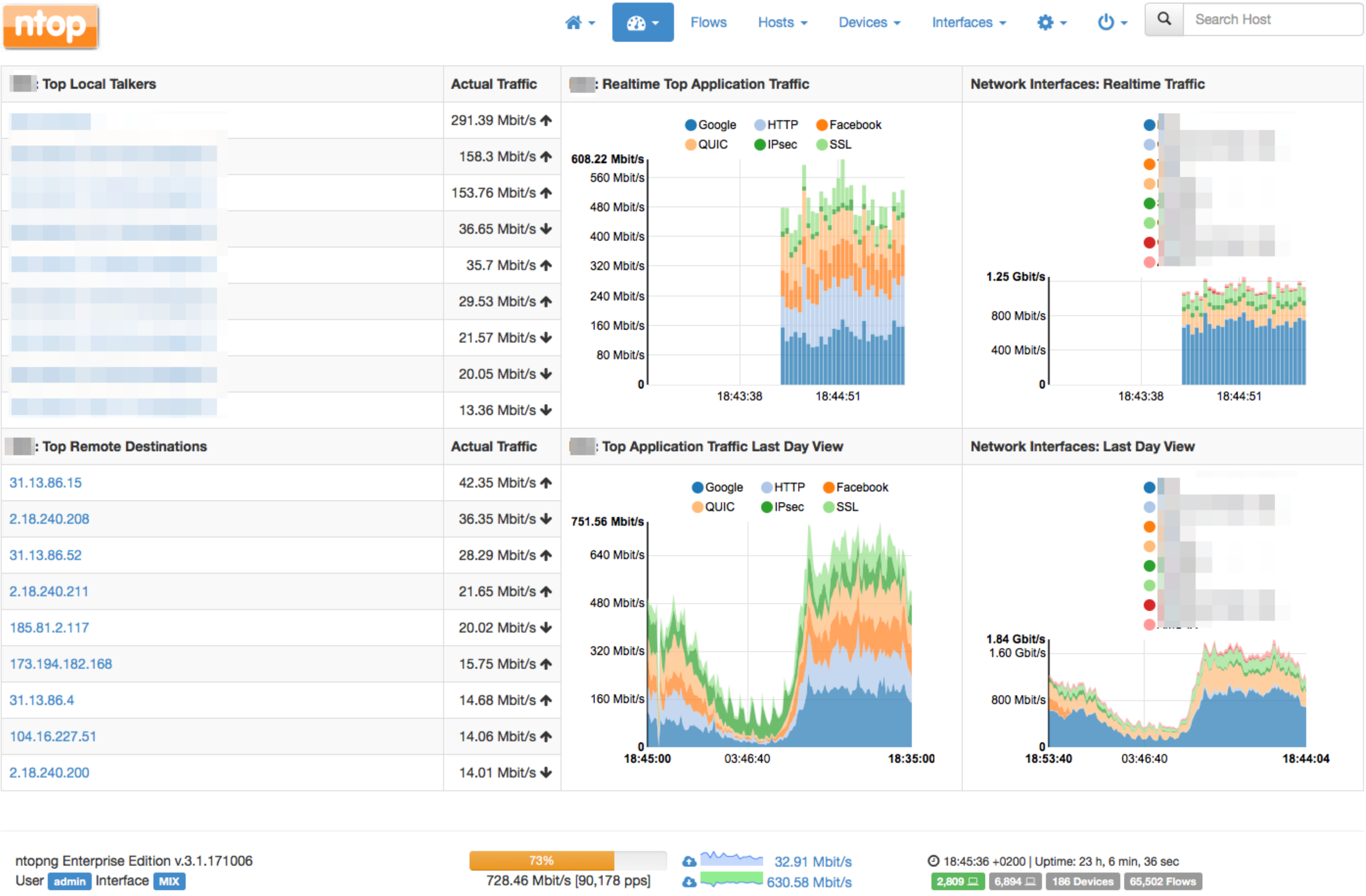
What Happens in Our Network?

- Do we have control over our network?
- It’s not possible to imagine a healthy network without a clear understanding of traffic flowing on our network.
- Knowledge is the first step towards evaluation of potential network security issues.
- Event correlation can provide us timely information about our network health.

Visibility

- What flows are "more relevant" than others?
- Can we use flows for more than just host/ protocol/application traffic accounting ?
- How can a network administrator look for a needle in a haystack when the monitoring platform is emitting tenth of thousand flows/ second?

Welcome to ntopng



: Top Local Talkers	Actual Traffic
[redacted]	291.39 Mbit/s ↑
[redacted]	158.3 Mbit/s ↑
[redacted]	153.76 Mbit/s ↑
[redacted]	36.65 Mbit/s ↓
[redacted]	35.7 Mbit/s ↑
[redacted]	29.53 Mbit/s ↑
[redacted]	21.57 Mbit/s ↓
[redacted]	20.05 Mbit/s ↓
[redacted]	13.36 Mbit/s ↓

: Top Remote Destinations	Actual Traffic
31.13.86.15	42.35 Mbit/s ↑
2.18.240.208	36.35 Mbit/s ↓
31.13.86.52	28.29 Mbit/s ↑
2.18.240.211	21.65 Mbit/s ↑
185.81.2.117	20.02 Mbit/s ↓
173.194.182.168	15.75 Mbit/s ↑
31.13.86.4	14.68 Mbit/s ↑
104.16.227.51	14.06 Mbit/s ↑
2.18.240.200	14.01 Mbit/s ↓

ntopng Enterprise Edition v.3.1.171006
User admin Interface MIX

73%
728.46 Mbit/s [90,178 pps]

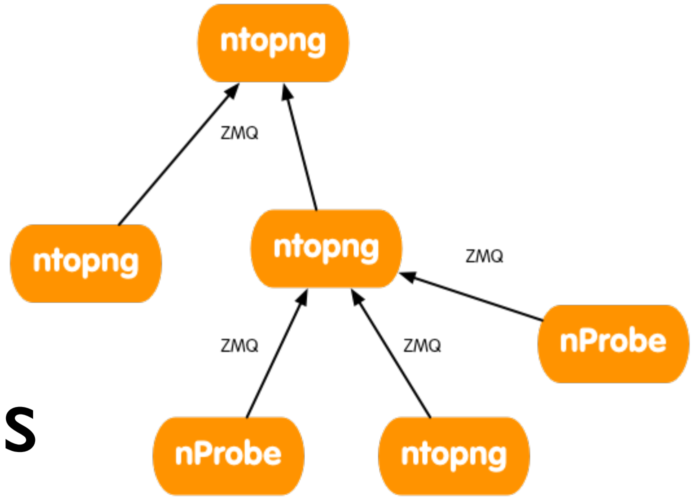
32.91 Mbit/s
630.58 Mbit/s

18:45:36 +0200 | Uptime: 23 h, 6 min, 36 sec
2,809 | 6,894 | 186 Devices | 65,502 Flows

© 2017 - ntop.org

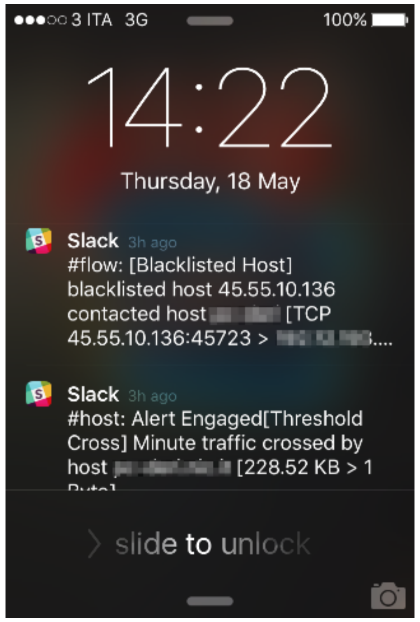
ntopng Design Principles

- Open
  - The ntopng engine is open-source, but even more important, monitored data is open and it can be exported to external apps: no proprietary stuff.
- Self-contained
  - No cloud or off-site data sharing for achieving our monitoring goal: not just for GDPR compliancy but because data is ours.
- Pervasive
  - You can monitor a distributed network as you can deploy it in complex topologies



© 2017 - ntop.org

Yes You Can


●●●○○ 3 ITA 3G 100%

14:22

Thursday, 18 May

Slack 3h ago
#flow: [Blacklisted Host] blacklisted host 45.55.10.136 contacted host [redacted] [TCP 45.55.10.136:45723 > [redacted]....

Slack 3h ago
#host: Alert Engaged[Threshold Cross] Minute traffic crossed by host [redacted] [228.52 KB > 1

slide to unlock

- Embedded alerting system pluggable with nagios and messaging systems.
- Use it as Grafana datasource

ntopng by ntop
DATA SOURCE
ntopng datasource

- Ready for openstack CLOUD SOFTWARE WIRESHARK VAGRANT docker elastic
- nDPI: passive mode = monitoring, inline = IPS
- Support for NetFlow/sFlow/SNMP.
- Passive/Active Network Device Discovery.
- Traffic Behaviour Analysis.

ntopng Editions: Matrix

Community

- Realtime traffic and L7 applications visibility
- Historical charts for hosts, networks, ASes, VLANs, host pools
- Historical top talkers (sources and destinations)
- Threshold- and anomaly-based alerts
- Geolocation
- Network discovery and devices inventory

Professional

everything in Community plus

- Extended realtime visibility with dashboards
- Advanced network activity reports generation
- Rich historical flows drill-down and export (requires MySQL)
- SNMP v1/v2c
- Custom BPF-based traffic profiles
- Traffic bridging and policing

Enterprise

everything in Professional plus

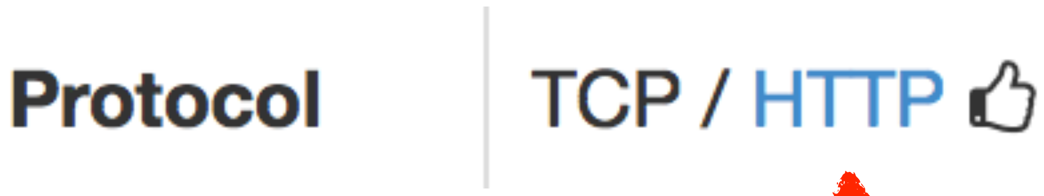
- Alerts dashboard
- SNMP v1/v2c with historical charts
- Netflow/sFlow devices ports monitoring (via nProbe)
- Captive portal, safe search and parental control
- Algorithms for faster (5x+) historical flows export and exploration

What Can ntopng Do For Me?

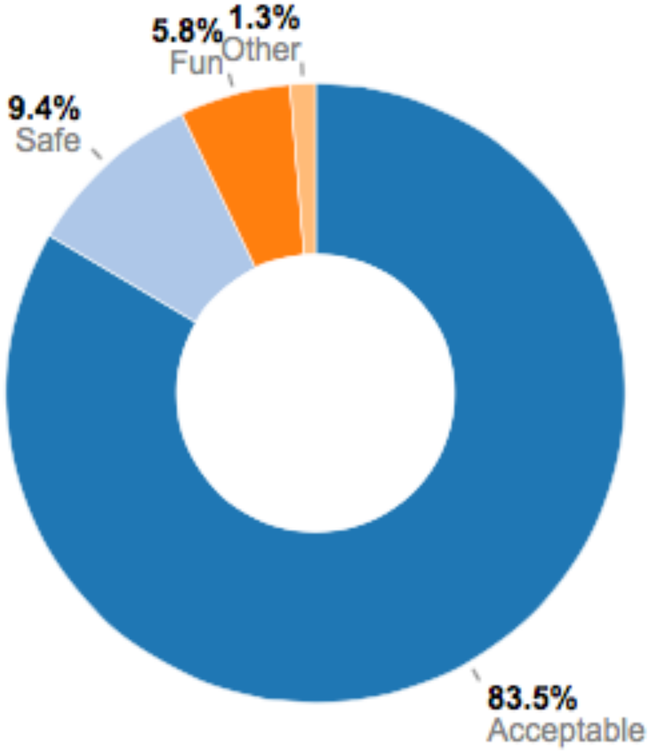
Collect and Interpret Flows

Layer 4 Protocol

Good or Bad?

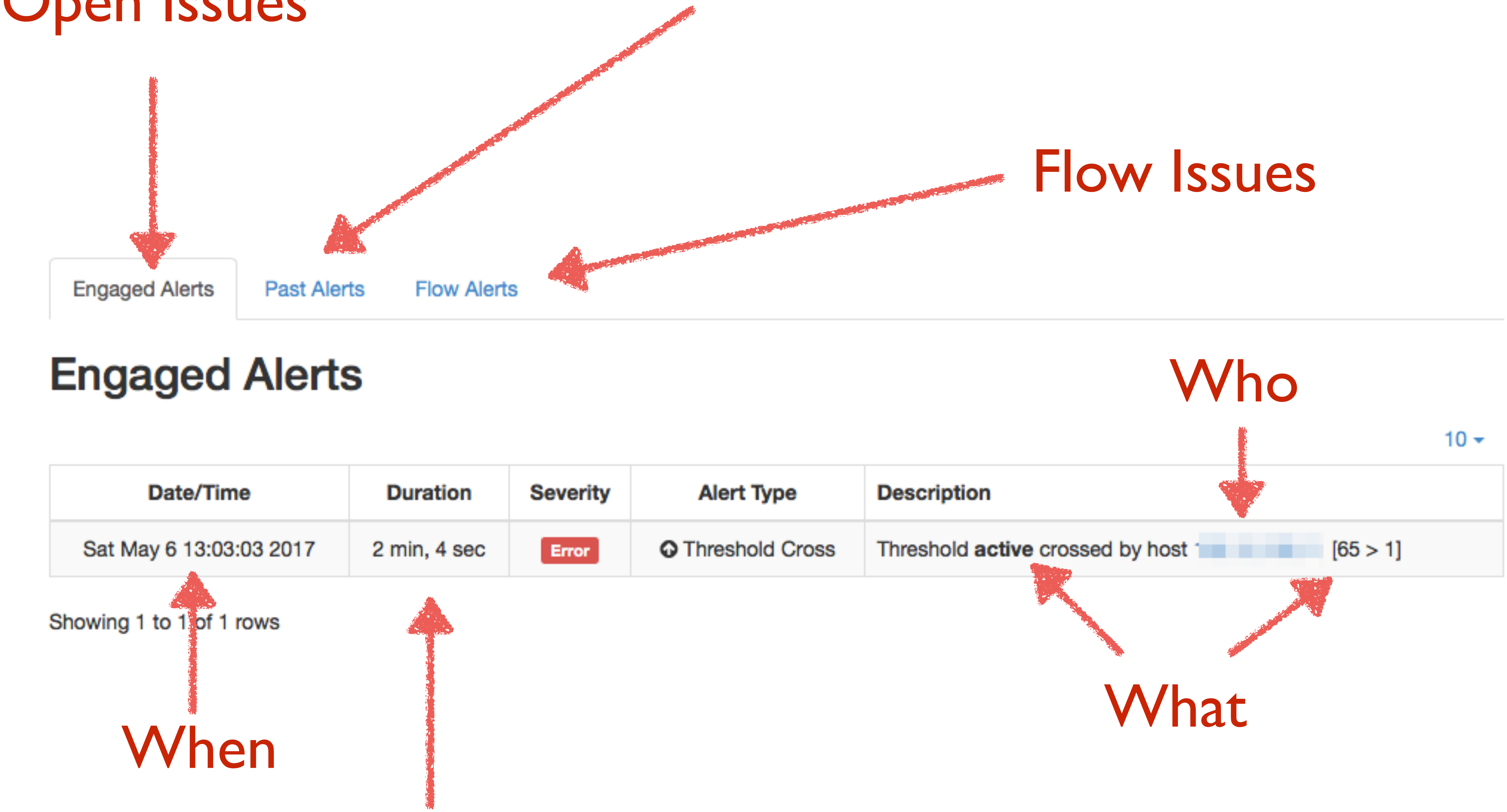


Protocol | TCP / HTTP 👍



Layer 7 Protocol

Know What's Wrong [2/2]



Open Issues

Past Issues

Flow Issues

Engaged Alerts | Past Alerts | Flow Alerts

Engaged Alerts

Who

10 ▾

Date/Time	Duration	Severity	Alert Type	Description
Sat May 6 13:03:03 2017	2 min, 4 sec	Error	⬆ Threshold Cross	Threshold **active** crossed by host [redacted] [65 > 1]

Showing 1 to 1 of 1 rows

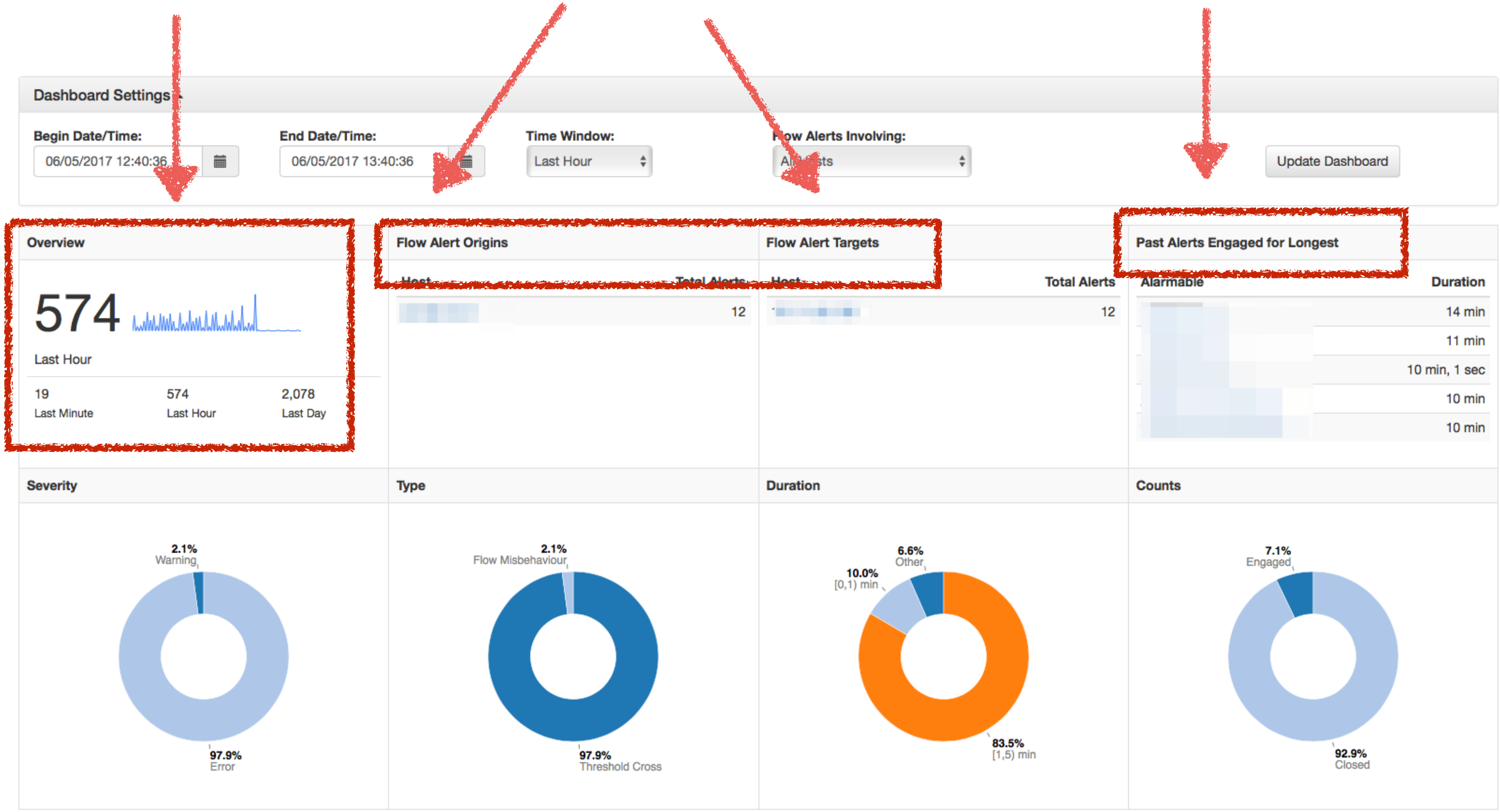
What

When

How Long

Know What's Wrong [2/2]

Overview　　Top Origins / Targets　　Longest Issues to Fix



Dashboard Settings

Begin Date/Time: 06/05/2017 12:40:36

End Date/Time: 06/05/2017 13:40:36

Time Window: Last Hour

Flow Alerts Involving: All Hosts

Overview

574 Last Hour

19	574	2,078
Last Minute	Last Hour	Last Day

Flow Alert Origins

Host	Total Alerts
[redacted]	12

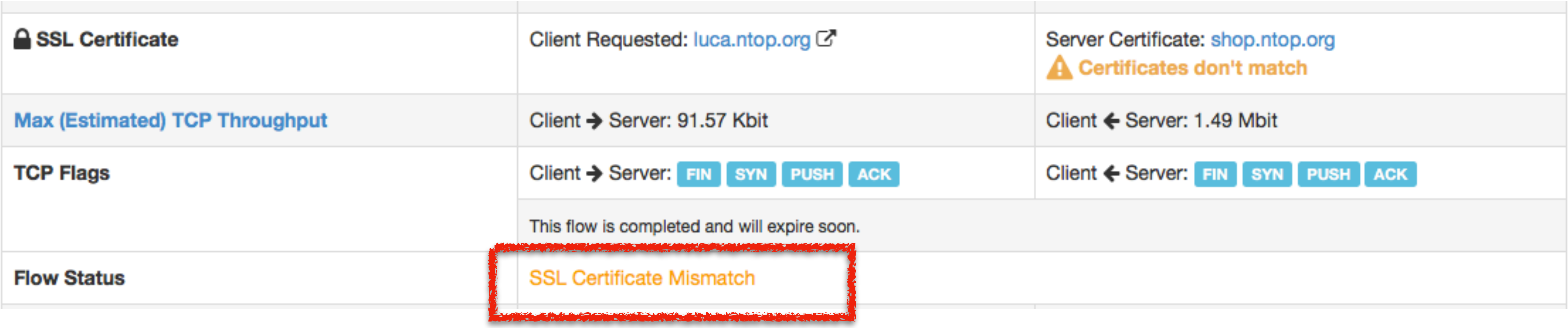
Flow Alert Targets

Host	Total Alerts
[redacted]	12

Past Alerts Engaged for Longest

Alarmable	Duration
[redacted]	14 min
[redacted]	11 min
[redacted]	10 min, 1 sec
[redacted]	10 min
[redacted]	10 min

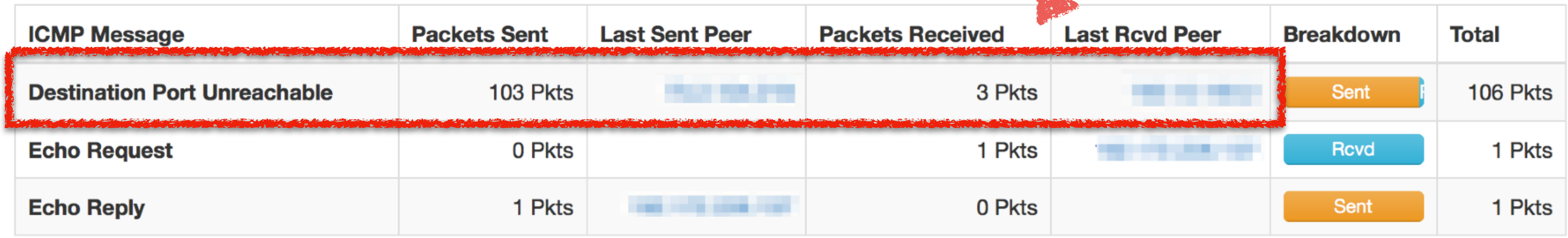
…Even When Things Look Normal



SSL Certificate	Client Requested: luca.ntop.org	Server Certificate: shop.ntop.org ⚠ Certificates don't match
Max (Estimated) TCP Throughput	Client → Server: 91.57 Kbit	Client ← Server: 1.49 Mbit
TCP Flags	Client → Server: FIN SYN PUSH ACK	Client ← Server: FIN SYN PUSH ACK
	This flow is completed and will expire soon.	
Flow Status	SSL Certificate Mismatch	

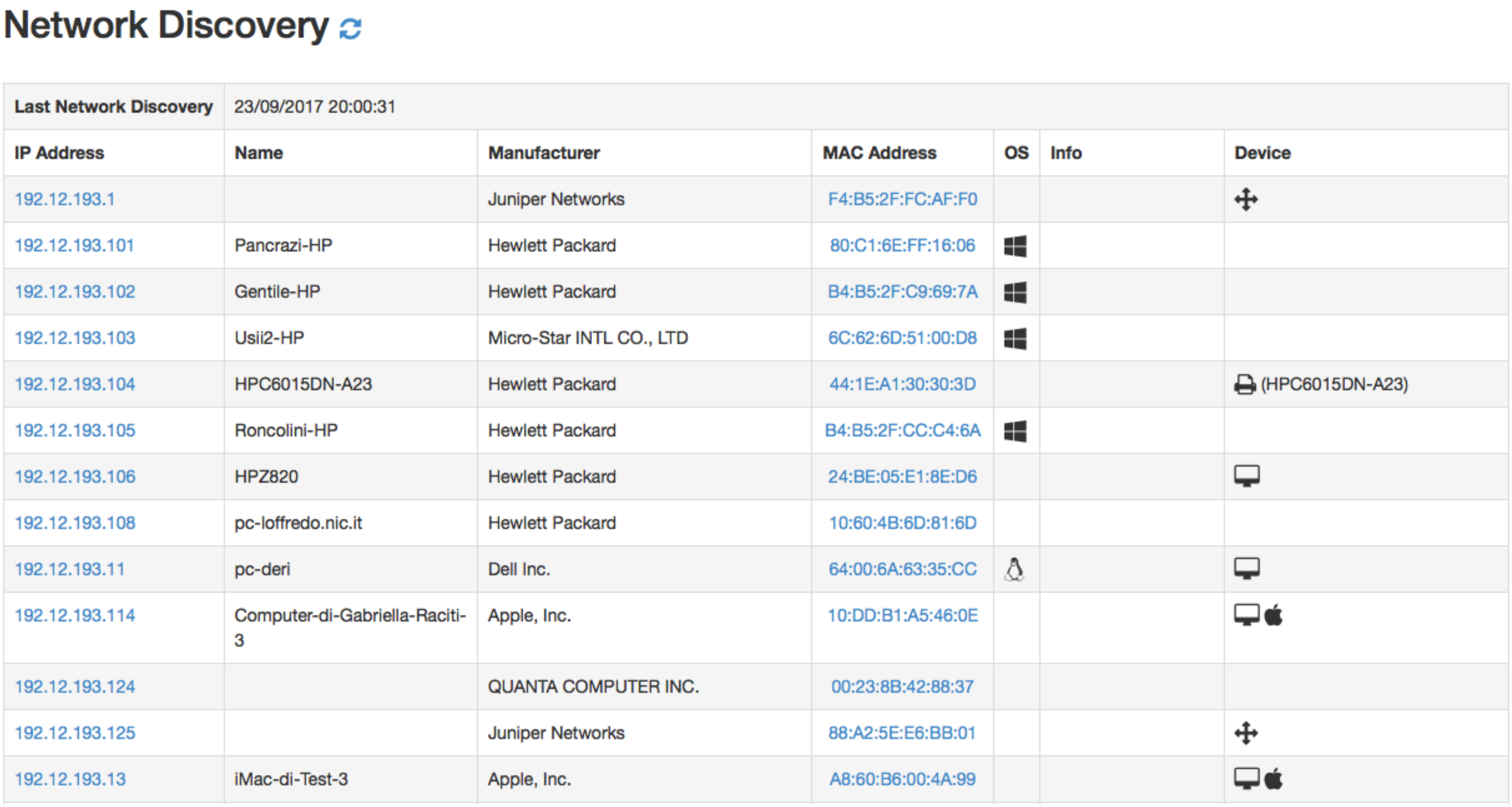
Invalid Configuration or Threat ?

Service Down or Scan?



ICMP Message	Packets Sent	Last Sent Peer	Packets Received	Last Rcvd Peer	Breakdown	Total
Destination Port Unreachable	103 Pkts	[redacted]	3 Pkts	[redacted]	Sent	106 Pkts
Echo Request	0 Pkts		1 Pkts	[redacted]	Rcvd	1 Pkts
Echo Reply	1 Pkts	[redacted]	0 Pkts		Sent	1 Pkts

Active Network Discovery



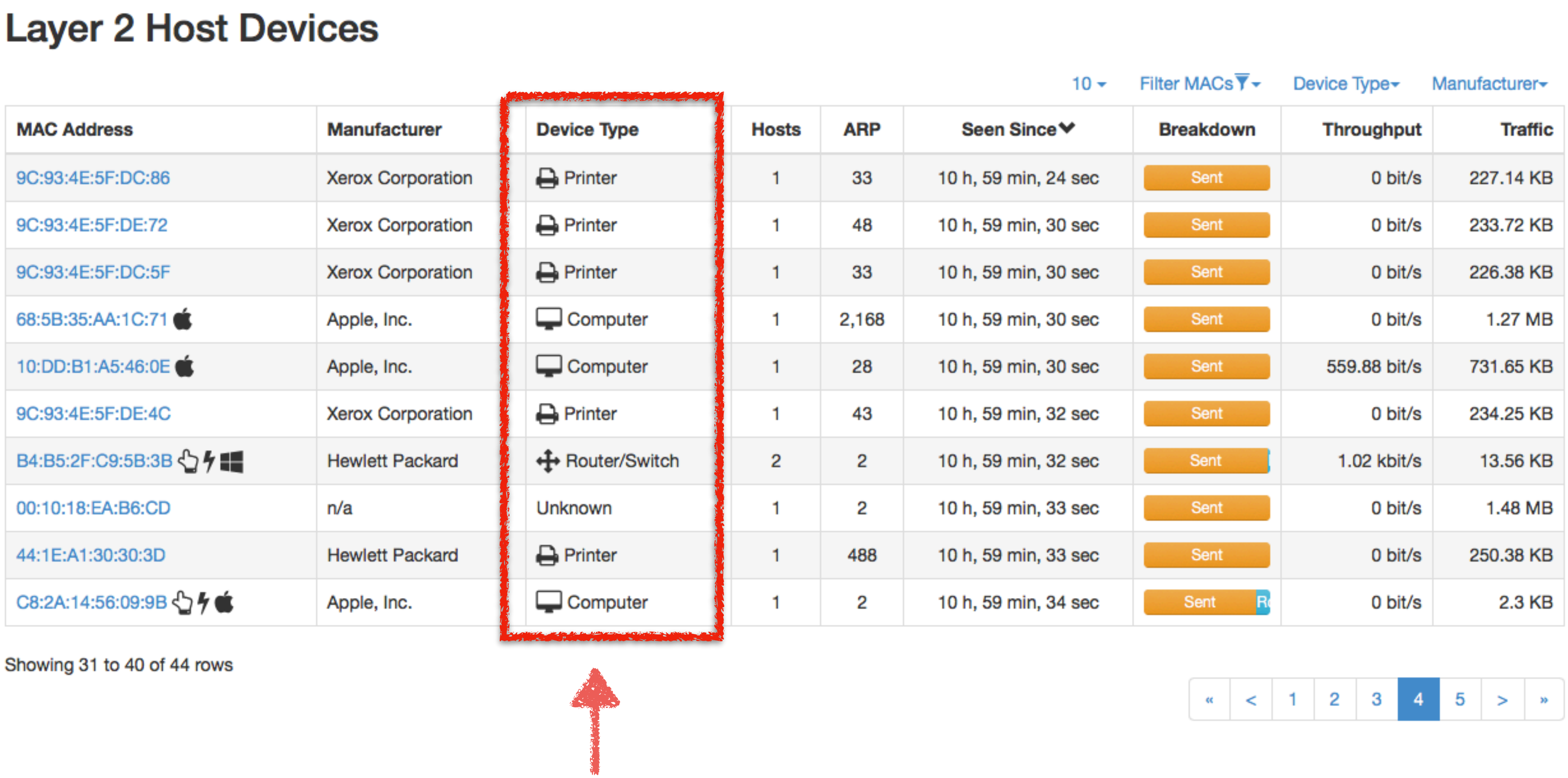
Network Discovery ↻

Last Network Discovery	23/09/2017 20:00:31

IP Address	Name	Manufacturer	MAC Address	OS	Info	Device
192.12.193.1		Juniper Networks	F4:B5:2F:FC:AF:F0			✥
192.12.193.101	Pancrazi-HP	Hewlett Packard	80:C1:6E:FF:16:06	⊞		
192.12.193.102	Gentile-HP	Hewlett Packard	B4:B5:2F:C9:69:7A	⊞		
192.12.193.103	Usii2-HP	Micro-Star INTL CO., LTD	6C:62:6D:51:00:D8	⊞		
192.12.193.104	HPC6015DN-A23	Hewlett Packard	44:1E:A1:30:30:3D			🖨 (HPC6015DN-A23)
192.12.193.105	Roncolini-HP	Hewlett Packard	B4:B5:2F:CC:C4:6A	⊞		
192.12.193.106	HPZ820	Hewlett Packard	24:BE:05:E1:8E:D6			🖥
192.12.193.108	pc-loffredo.nic.it	Hewlett Packard	10:60:4B:6D:81:6D			
192.12.193.11	pc-deri	Dell Inc.	64:00:6A:63:35:CC	🐧		🖥
192.12.193.114	Computer-di-Gabriella-Raciti-3	Apple, Inc.	10:DD:B1:A5:46:0E			🖥
192.12.193.124		QUANTA COMPUTER INC.	00:23:8B:42:88:37			
192.12.193.125		Juniper Networks	88:A2:5E:E6:BB:01			✥
192.12.193.13	iMac-di-Test-3	Apple, Inc.	A8:60:B6:00:4A:99			🖥

© 2017 - ntop.org

Passive Network Discovery



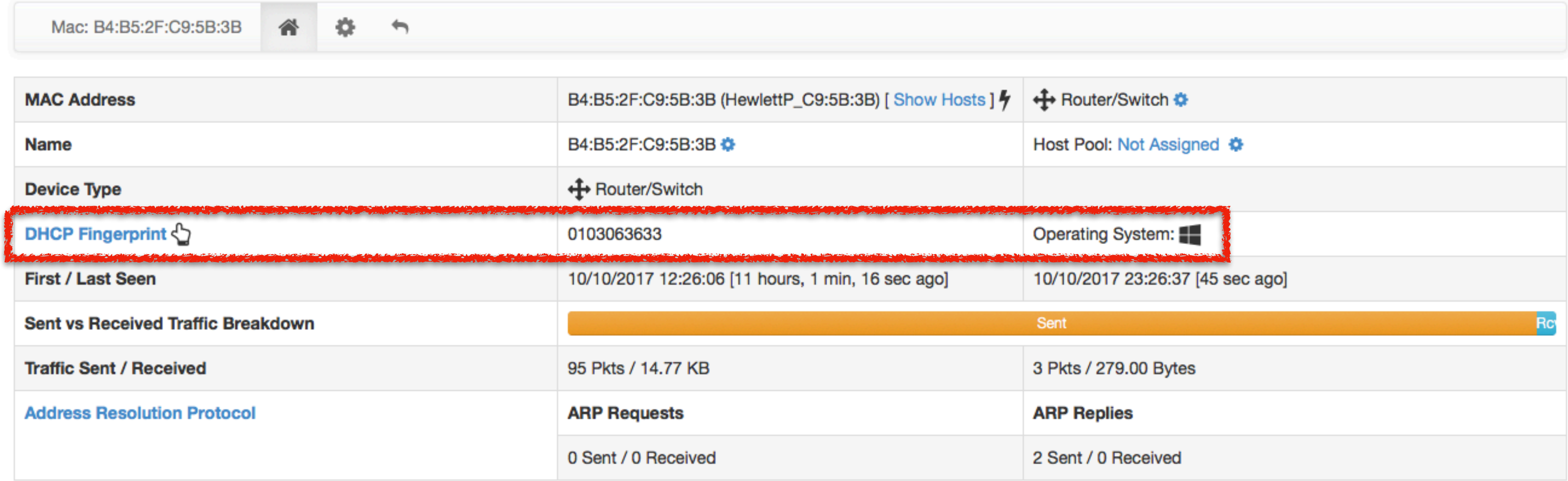
Layer 2 Host Devices

MAC Address	Manufacturer	Device Type	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
9C:93:4E:5F:DC:86	Xerox Corporation	Printer	1	33	10 h, 59 min, 24 sec	Sent	0 bit/s	227.14 KB
9C:93:4E:5F:DE:72	Xerox Corporation	Printer	1	48	10 h, 59 min, 30 sec	Sent	0 bit/s	233.72 KB
9C:93:4E:5F:DC:5F	Xerox Corporation	Printer	1	33	10 h, 59 min, 30 sec	Sent	0 bit/s	226.38 KB
68:5B:35:AA:1C:71	Apple, Inc.	Computer	1	2,168	10 h, 59 min, 30 sec	Sent	0 bit/s	1.27 MB
10:DD:B1:A5:46:0E	Apple, Inc.	Computer	1	28	10 h, 59 min, 30 sec	Sent	559.88 bit/s	731.65 KB
9C:93:4E:5F:DE:4C	Xerox Corporation	Printer	1	43	10 h, 59 min, 32 sec	Sent	0 bit/s	234.25 KB
B4:B5:2F:C9:5B:3B 👆⚡⊞	Hewlett Packard	Router/Switch	2	2	10 h, 59 min, 32 sec	Sent	1.02 kbit/s	13.56 KB
00:10:18:EA:B6:CD	n/a	Unknown	1	2	10 h, 59 min, 33 sec	Sent	0 bit/s	1.48 MB
44:1E:A1:30:30:3D	Hewlett Packard	Printer	1	488	10 h, 59 min, 33 sec	Sent	0 bit/s	250.38 KB
C8:2A:14:56:09:9B 👆⚡	Apple, Inc.	Computer	1	2	10 h, 59 min, 34 sec	Sent R	0 bit/s	2.3 KB

Showing 31 to 40 of 44 rows

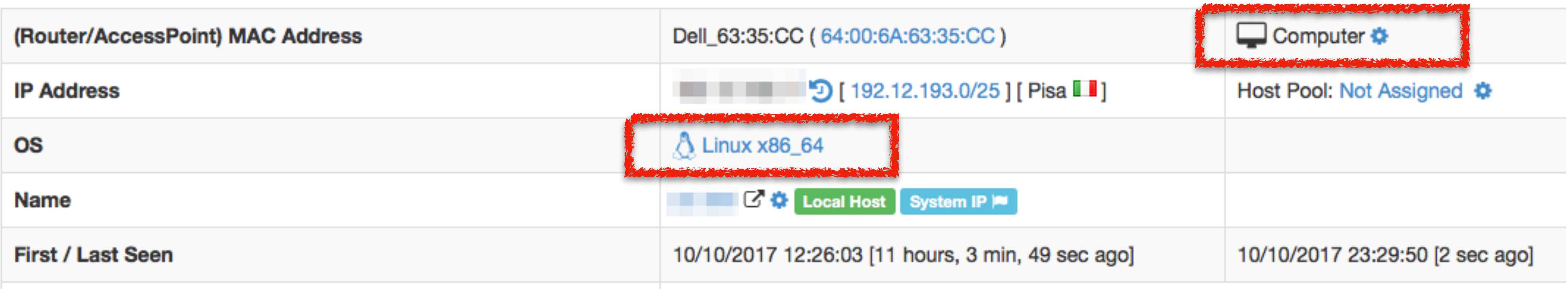
SSDP / MDNS / ARP

Passive OS/Device Fingerprinting



Mac: B4:B5:2F:C9:5B:3B

MAC Address	B4:B5:2F:C9:5B:3B (HewlettP_C9:5B:3B) [Show Hosts]	Router/Switch
Name	B4:B5:2F:C9:5B:3B	Host Pool: Not Assigned
Device Type	Router/Switch	
DHCP Fingerprint	0103063633	Operating System: ⊞
First / Last Seen	10/10/2017 12:26:06 [11 hours, 1 min, 16 sec ago]	10/10/2017 23:26:37 [45 sec ago]
Sent vs Received Traffic Breakdown	Sent	Rc
Traffic Sent / Received	95 Pkts / 14.77 KB	3 Pkts / 279.00 Bytes
Address Resolution Protocol	**ARP Requests**	**ARP Replies**
	0 Sent / 0 Received	2 Sent / 0 Received

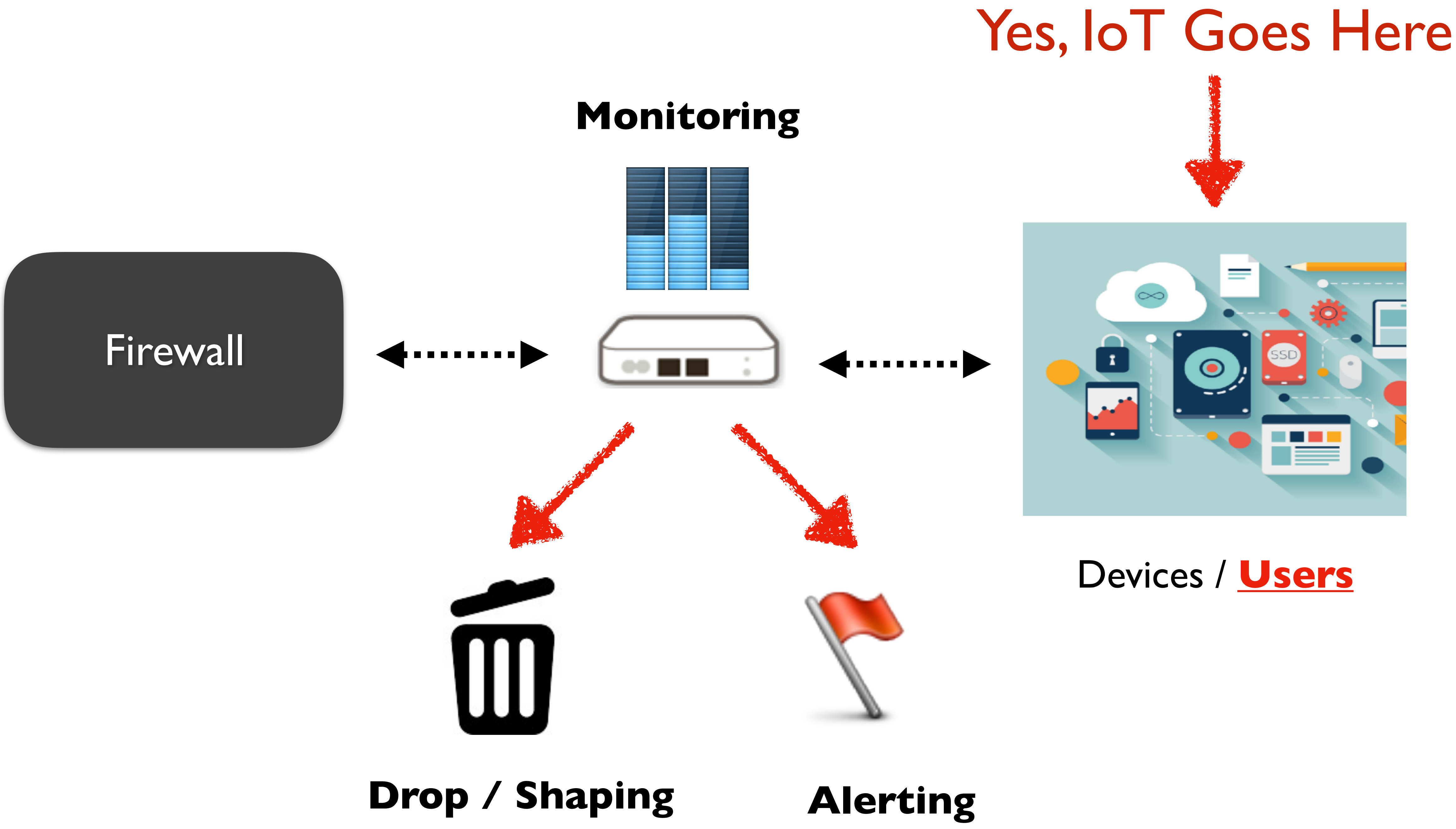


(Router/AccessPoint) MAC Address	Dell_63:35:CC (64:00:6A:63:35:CC)	Computer
IP Address	[redacted] [192.12.193.0/25] [Pisa 🇮🇹]	Host Pool: Not Assigned
OS	Linux x86_64	
Name	[redacted] Local Host System IP	
First / Last Seen	10/10/2017 12:26:03 [11 hours, 3 min, 49 sec ago]	10/10/2017 23:29:50 [2 sec ago]

Security in Three Phases

- Learning
  - Identify network elements (discovery), assign them a role (e.g. a printer).
- Profiling
  - Bind a device to a profile (e.g. a printer cannot Skype or share files using BitTorrent) and enforce it via alarms or traffic policy enforcement.
- Continuous Monitoring
  - Physical constraints (e.g. MAC/IP binding and switch port location), traffic constraints (e.g. a new protocol serviced by a device or throughput above/under its historical baseline can be an indication of a problem).

ntopng: Edge Traffic Policer



Yes, IoT Goes Here

Monitoring

Firewall

Devices / **Users**

Drop / Shaping

Alerting

Some Facts: What is About

- Designed to complement (not replace) firewalls and security devices by:
  - Enforcing per user/device traffic policies and assigning devices to users.
  - Layer 7 traffic policy (drop + shaping) based on device type, user, and time of the day.
  - Periodic asset discovery to detect new devices connected to the LAN and enforcing their traffic.
  - Multicast/broadcast monitoring to fingerprint devices and discover network overlays created by users.
  - Prevent access to malware, inappropriate (for minors) and unsafe Internet contents.

Final Remarks

- Modern devices create new monitoring challenges and require an *integrated monitoring* approach: element + periodic active scans + permanent passive traffic monitoring.
- Monitoring hundred/thousand devices require *scalability* and *intelligence* in the monitoring platform (analytics and big data is not enough, platform must be reactive, distributed, multi-tenant).
- Bytes+Packet-based monitoring must be *complemented* with specialised metrics, DPI, realtime monitoring, flexible (on-the-go) alerting.