

# NTC

Network Traffic Center  
La potenza senza controllo è nulla

Padova

09 maggio 2019



Arsenio Raimo  
[a.raimo@italferr.it](mailto:a.raimo@italferr.it)

# INDICE

<b>01</b>	Italferr	3
<b>02</b>	Nagios	5
<b>03</b>	Ntop	7
<b>04</b>	L'integrazione	13
<b>05</b>	Sviluppi futuri	27
<b>06</b>	Considerazioni finali	30



# Italferr S.p.a.



F5 F6 F7 F8

2046

# Italferr

## La missione

### Chi è

Italferr, società del Gruppo Ferrovie dello Stato Italiane, incarna il successo della grande ingegneria italiana, consolidatasi in oltre 30 anni di esperienze nei **grandi progetti infrastrutturali** per il **settore ferroviario** convenzionale e per quello ad **Alta Velocità**, nel **trasporto metropolitano e stradale**, nella progettazione di **porti e stazioni**, in Italia e all'estero.

### Cosa fa

Dalla **progettazione** fino agli appalti, alla **direzione e supervisione** dei lavori, al **collaudo e alla messa in servizio** di linee, stazioni, centri intermodali e interporti, al **project management**, alle **consulenze organizzative**, al **training** e al trasferimento di know-how specialistico ed innovativo.

Un'offerta di ingegneria che si declina nel settore delle infrastrutture ferroviarie in senso classico e metropolitane, e si differenzia trasversalmente in quello delle infrastrutture stradali, intermodali e portuali in Italia e all'estero a conferma di una visione globale orientata ad un business che interpreta l'ingegneria dei sistemi di trasporto in modo complessivo nelle sue più ampie e variegate forme possibili.

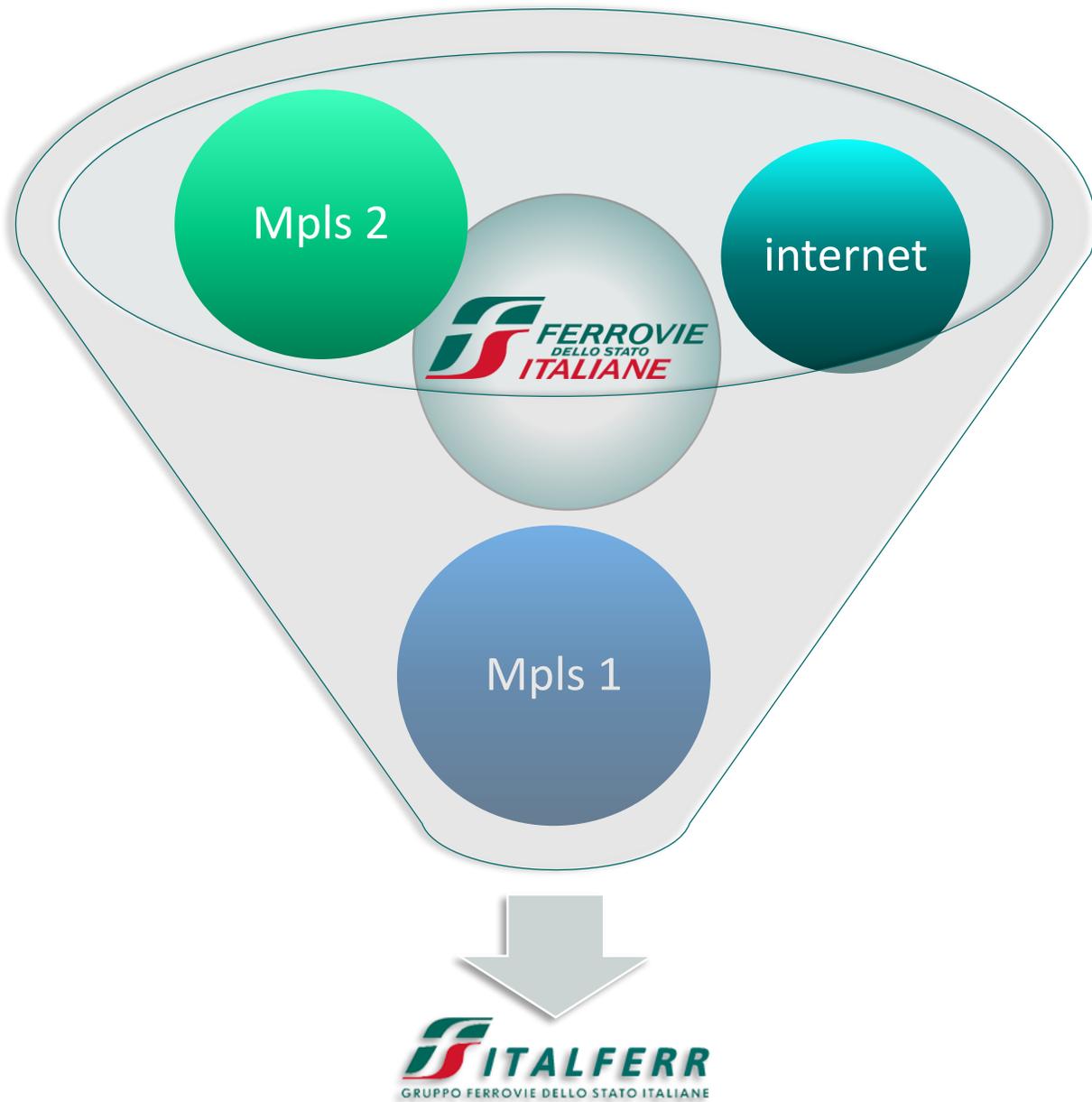
# Italferr

## Situazione geografica in Italia



# Italferr

## L'infrastruttura





# Nagios

## Monitorare e quantificare



# Quantificare e monitorare

**Nagios**<sup>®</sup>

## Che cos'è

Fornisce il monitoraggio di tutti i componenti dell'infrastruttura incluse applicazioni, servizi, sistemi operativi, protocolli di rete, metriche di sistema e infrastruttura di rete.

## Perchè

Non solo il monitoraggio dell'infrastruttura ma anche uno strumento di gestione contrattuale per la verifica degli SLA (disponibilità, quantità e qualità).

### Unhandled host problems | Hiding soft states

Hostname	Alias
PDM_INTERNET	PDM_INTERNET
LTE 10.168.1.1	LTE 10.168.1.1
LTE 10.166.1.1	LTE 10.166.1.1
LTE 10.165.1.1	LTE 10.165.1.1
LTE 10.164.1.1	LTE 10.164.1.1
LTE 10.163.1.1	LTE 10.163.1.1
LTE 10.161.1.1	LTE 10.161.1.1
Cantiere_Termini_Imerese	Cantiere_Termini_Imerese
Cantiere_Chivasso_OC	Cantiere_Chivasso_OC

### Tactical overview

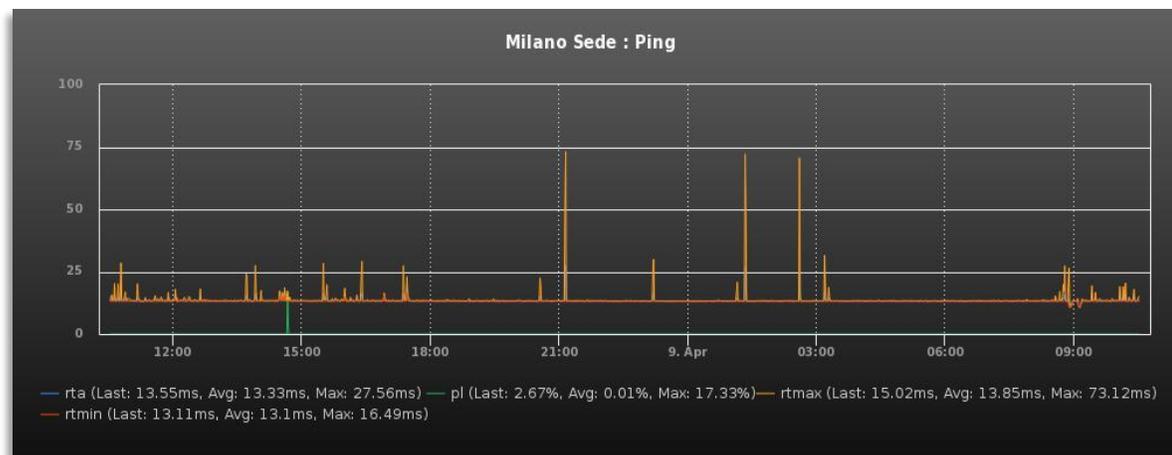
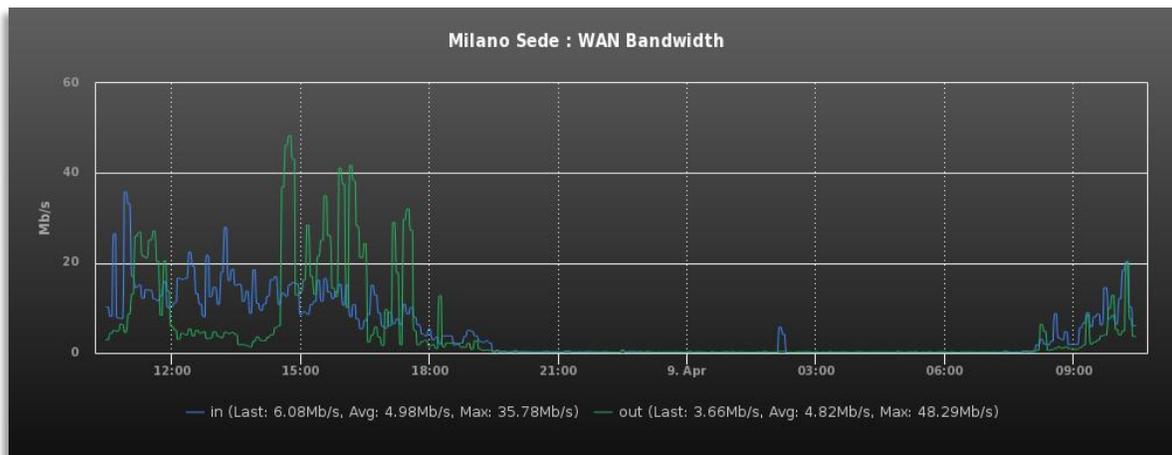
Type	Totals	Percentage %
Hosts up	85/94	90.43
Hosts down	9/94	9.57
Services up	602/626	96.17
Services down	24/626	3.83



### Unhandled service problems | Hiding soft states

Host	Service	State	Output	Last statechange	Last check
Cantiere_Ministero_pfSense	VPNLTE2 Status	1	WARNING: Interface ovpcn3 (index 19) is administratively down.	2019-04-09 05:30:03	2019-04-09 11:00:35
Cantiere_Postapiana_foggia	Ping WAN	2	PING CRITICAL - Packet loss = 0%, RTA = 648.17 ms	2019-03-07 12:44:37	2019-04-09 11:00:33
gis.italferr.it	HTTP	1	HTTP WARNING: HTTP/1.1 403 Forbidden - 1412 bytes in 0.224 second response time	2019-02-26 18:13:23	2019-04-09 10:55:08
ntc.italferr.it	Load	1	WARNING - load average: 4.27, 4.95, 5.38	2019-04-08 00:24:08	2019-04-09 11:00:27
ntopinternet.italferr.it	Database records count	1	76893	2019-04-09 10:54:50	2019-04-09 11:00:41
presidionormativo.italferr.it	HTTP	2	CHECK_NRPE STATE CRITICAL: Socket timeout after 10 seconds.	2019-04-09 09:13:54	2019-04-09 10:58:54
Torino-lingotto-pfsense	LAN Status	1	WARNING: SNMP error: No response from remote host "10.113.1.1"	2019-03-27 09:44:48	2019-04-09 11:00:34
Torino-lingotto-pfsense	VPNLTE Status	1	WARNING: SNMP error: No response from remote host "10.113.1.1"	2019-03-27 09:44:49	2019-04-09 11:00:25
Torino-lingotto-pfsense	VPNWAN Status	1	WARNING: SNMP error: No response from remote host "10.113.1.1"	2019-03-27 09:44:42	2019-04-09 11:00:17
Torino-lingotto-pfsense	WAN Status	1	WARNING: SNMP error: No response from remote host "10.113.1.1"	2019-03-27 09:45:46	2019-04-09 11:00:18
Torino_Sede	LAN Status	2	CRITICAL: Interface GigabitEthernet0/1 (index 3) is down.	2019-04-03 10:19:42	2019-04-09 11:00:39

# Nagios® dal 2006 in Italferr



State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	4d 3h 41m 49s	59.343%	59.343%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	<b>Total</b>	<b>4d 3h 41m 49s</b>	<b>59.343%</b>	<b>59.343%</b>
DOWN	Unscheduled	2d 20h 18m 11s	40.657%	40.657%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	<b>Total</b>	<b>2d 20h 18m 11s</b>	<b>40.657%</b>	<b>40.657%</b>
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	<b>Total</b>	<b>0d 0h 0m 0s</b>	<b>0.000%</b>	<b>0.000%</b>
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	<b>Total</b>	<b>0d 0h 0m 0s</b>	<b>0.000%</b>	
<b>All</b>	<b>Total</b>	<b>7d 0h 0m 0s</b>	<b>100.000%</b>	<b>100.000%</b>

## Report per Bologna\_sede dal 02-04-2019 al 02-04-2019

Dettagli	Data	Nome sede	RTT	Downtime	Packet loss	Traffico IN	Traffico OUT
📄	2019-04-02 07:00:00	Bologna_sede	12.264 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	651.226 kbps	191.153 kbps
📄	2019-04-02 08:00:00	Bologna_sede	12.304 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	3441.769 kbps	921.434 kbps
📄	2019-04-02 09:00:00	Bologna_sede	12.554 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	4079.477 kbps	1310.747 kbps
📄	2019-04-02 10:00:00	Bologna_sede	12.558 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	7975.835 kbps	1783.522 kbps
📄	2019-04-02 11:00:00	<b>Bologna_sede</b>	12.338 ms Ore non rispettate: 0	0h 0m	<b>0.333%</b> <b>Ore non rispettate: 1</b>	4729.201 kbps	1311.303 kbps
📄	2019-04-02 12:00:00	Bologna_sede	12.319 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	6719.903 kbps	2841.072 kbps
📄	2019-04-02 13:00:00	Bologna_sede	12.312 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	4269.673 kbps	563.818 kbps
📄	2019-04-02 14:00:00	Bologna_sede	12.370 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	5379.670 kbps	3947.781 kbps
📄	2019-04-02 15:00:00	<b>Bologna_sede</b>	12.301 ms Ore non rispettate: 0	0h 0m	<b>1.000%</b> <b>Ore non rispettate: 1</b>	5657.587 kbps	4076.148 kbps
📄	2019-04-02 16:00:00	Bologna_sede	12.377 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	5059.512 kbps	2163.998 kbps
📄	2019-04-02 17:00:00	Bologna_sede	14.178 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	1406.521 kbps	318.561 kbps
📄	2019-04-02 18:00:00	Bologna_sede	12.220 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	356.746 kbps	132.508 kbps
📄	2019-04-02 19:00:00	Bologna_sede	12.215 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	293.886 kbps	160.868 kbps
📄	2019-04-02 20:00:00	Bologna_sede	12.314 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	178.758 kbps	157.398 kbps
📄	2019-04-02 21:00:00	Bologna_sede	12.231 ms Ore non rispettate: 0	0h 0m	0.000% Ore non rispettate: 0	87.773 kbps	84.259 kbps
<b>Dettagli</b>	<b>Data</b>	<b>Nome sede</b>	<b>RTT</b>	<b>Downtime</b>	<b>Packet loss</b>	<b>Traffico IN</b>	<b>Traffico OUT</b>

**PROBLEM Host Alert: Palermo\_sede is DOWN**

DMNGS002RM01 <nagios@DMNGS002RM01.italferr.it>  
 Inviato: mercoledì 27/05/2015 03:23

A:

\*\*\*\*\* Nagios \*\*\*\*\*

Tipo di notifica: PROBLEM  
 Host: Palermo\_sede  
 Stato: DOWN  
 IP: 5.97.223.206  
 Indirizzo: Italferr Via Cimarosa, 10 Palermo  
 Info: (Host Check Timed Out)

Date/Time: Wed May 27 03:23:14 CEST 2015

[https://nagios.italferr.it/nagios/cgi-bin/status.cgi?host=Palermo\\_sede](https://nagios.italferr.it/nagios/cgi-bin/status.cgi?host=Palermo_sede)

DMNGS002RM01

- RECOVERY Host Alert: Palermo\_sede is UP 15 minuti fa
- \*\* Traffico eccessivo per l'host Cantiere\_Pisa con URL\*\* 17:10 26/05/2015
- \*\* Traffico eccessivo per l'host NAVIGAZIONE\_INTERNET con URL\*\* 17:00 26/05/2015
- \*\* Traffico eccessivo per l'host NAVIGAZIONE\_INTERNET con URL\*\* 16:00 26/05/2015
- \*\* Traffico eccessivo per l'host NAVIGAZIONE\_INTERNET con URL\*\* 16:40 25/05/2015
- \*\* Traffico eccessivo per l'host NAVIGAZIONE\_INTERNET con URL\*\* 15:40 25/05/2015
- \*\* Traffico eccessivo per l'host NAVIGAZIONE\_INTERNET con URL\*\* 14:40 25/05/2015
- \*\* Traffico eccessivo per l'host NAVIGAZIONE\_INTERNET con URL\*\* 11:00 25/05/2015
- RECOVERY Host Alert: Cantiere\_Orvieto is UP 23:52 24/05/2015
- PROBLEM Host Alert: Cantiere\_Orvieto is DOWN 23:10 24/05/2015
- RECOVERY Host Alert: Cantiere\_Bari\_Parconord is UP 05:29 23/05/2015
- PROBLEM Host Alert: Cantiere\_Bari\_Parconord is DOWN 05:27 23/05/2015
- \*\* Traffico eccessivo per l'host NAVIGAZIONE\_INTERNET con URL\*\* 17:00 22/05/2015

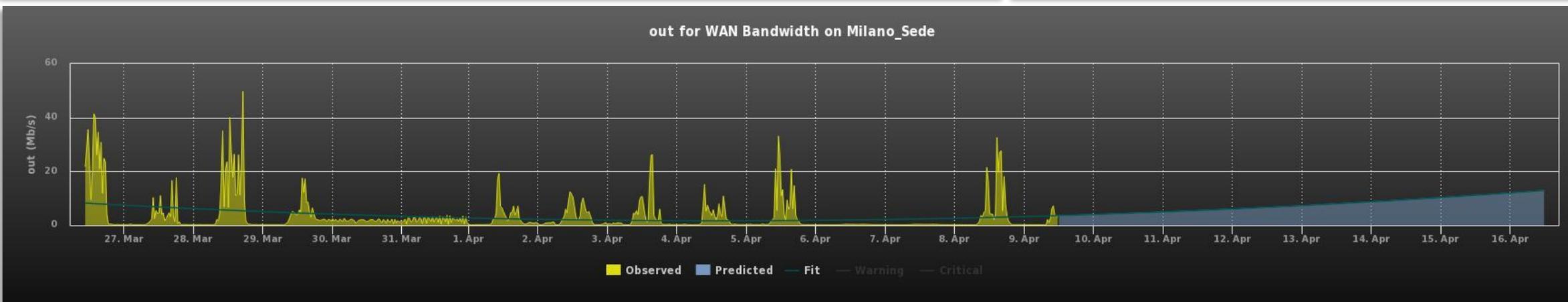
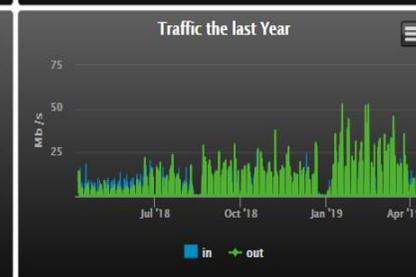
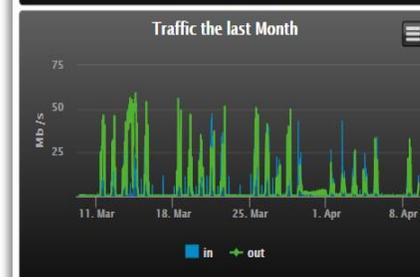
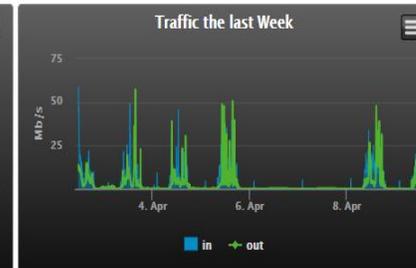
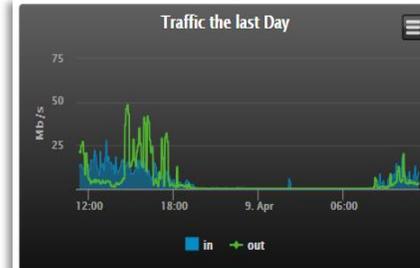
# Nagios® dal 2006 in Italferr

## Year: 2019

	Jan (1)	Feb (2)	Mar (3)	Quarter 1	Apr (4)	May (5)	Jun (6)	Quarter 2	Jul (7)	Aug (8)	Sep (9)	Quarter 3	Oct (10)	Nov (11)	Dec (12)	Quarter 4	Year
<b>In</b>	1.14 TB	1.04 TB	1.18 TB	3.36 TB	280.79 GB	0 B	0 B	280.79 GB	0 B	0 B	0 B	0 B	0 B	0 B	0 B	0 B	3.63 TB
<b>Out</b>	2.07 TB	2.27 TB	2.07 TB	6.41 TB	209.12 GB	0 B	0 B	209.12 GB	0 B	0 B	0 B	0 B	0 B	0 B	0 B	0 B	6.61 TB
<b>Max</b>	2.07 TB	2.27 TB	2.07 TB	6.41 TB	280.79 GB	0 B	0 B	280.79 GB	0 B	0 B	0 B	0 B	0 B	0 B	0 B	0 B	6.61 TB
<b>Sum</b>	3.21 TB	3.31 TB	3.25 TB	9.76 TB	489.91 GB	0 B	0 B	489.91 GB	0 B	0 B	0 B	0 B	0 B	0 B	0 B	0 B	10.24 TB

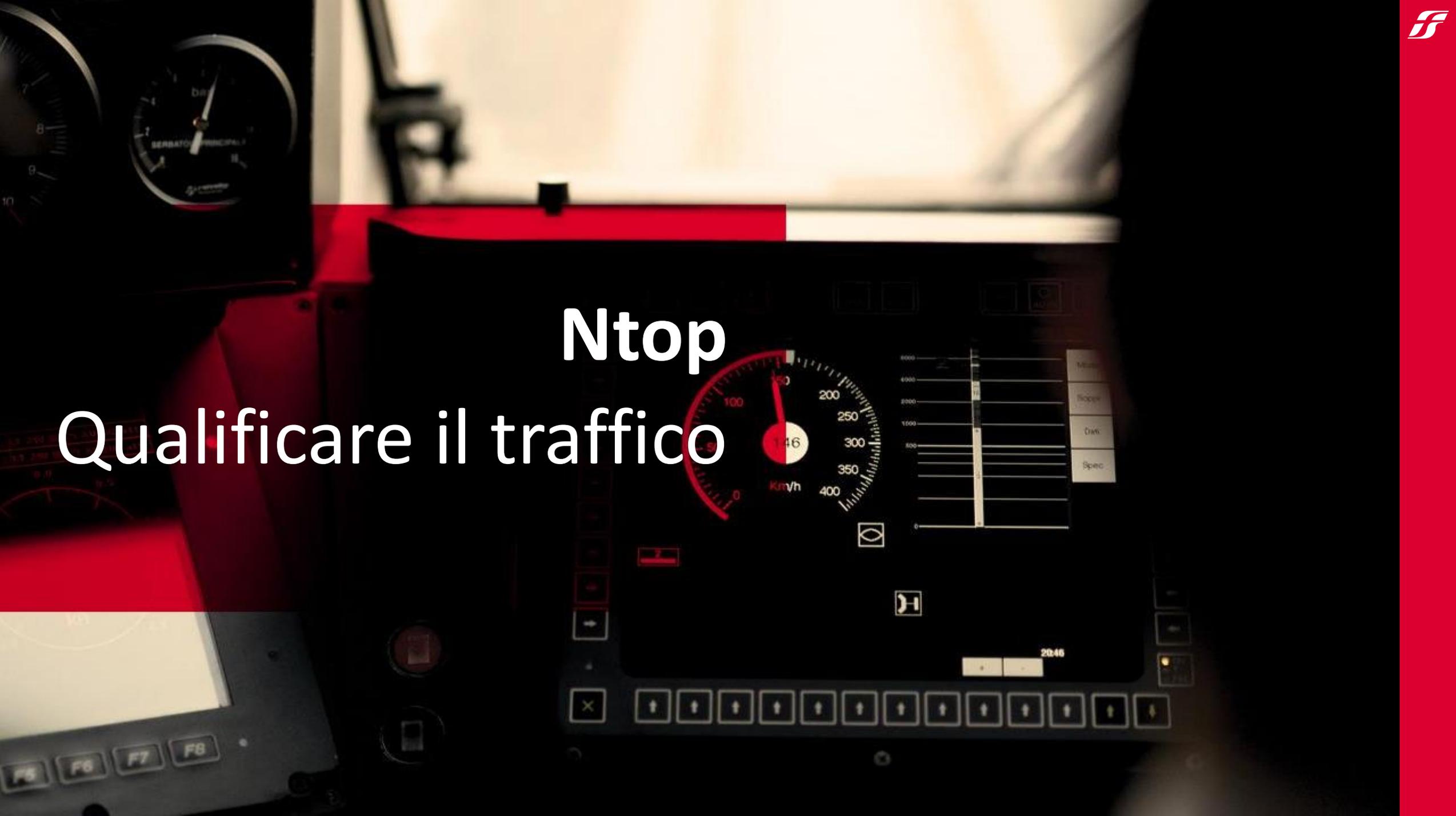
## Year: 2018

	Jan (1)	Feb (2)	Mar (3)	Quarter 1	Apr (4)	May (5)	Jun (6)	Quarter 2	Jul (7)	Aug (8)	Sep (9)	Quarter 3	Oct (10)	Nov (11)	Dec (12)	Quarter 4	Year
<b>In</b>	877.75 GB	762.37 GB	967.79 GB	2.55 TB	913.98 GB	881.67 GB	1.01 TB	2.76 TB	1.07 TB	707.47 GB	1.09 TB	2.85 TB	1.2 TB	1.06 TB	776.73 GB	3.02 TB	11.18 TB
<b>Out</b>	428.25 GB	476.72 GB	477.37 GB	1.35 TB	476.74 GB	470.06 GB	759.61 GB	1.67 TB	1.07 TB	1005.39 GB	1.29 TB	3.34 TB	1.43 TB	1.43 TB	935.74 GB	3.77 TB	10.13 TB
<b>Max</b>	877.75 GB	762.37 GB	967.79 GB	2.55 TB	913.98 GB	881.67 GB	1.01 TB	2.76 TB	1.07 TB	1005.39 GB	1.29 TB	3.34 TB	1.43 TB	1.43 TB	935.74 GB	3.77 TB	11.18 TB
<b>Sum</b>	1.28 TB	1.21 TB	1.41 TB	3.9 TB	1.36 TB	1.32 TB	1.75 TB	4.43 TB	2.14 TB	1.67 TB	2.38 TB	6.2 TB	2.64 TB	2.49 TB	1.67 TB	6.8 TB	21.32 TB



# Ntop

## Qualificare il traffico



F5 F6 F7 F8

## Ma non basta.....

Monitorando gli hosts abbiamo quantificato i flussi di traffico, la loro qualità e disponibilità ma non sappiamo quale siano le componenti che concorrono all'occupazione della banda in tempo reale o nel passato.



**ntop**

- Mostra il **traffico di rete** in tempo reale e gli host attivi
- Produce **report a lungo termine** per diverse **metriche di rete**, inclusi throughput e protocolli applicativi
- **Monitora e segnala** throughput in tempo reale, latenze di rete e applicazioni, Round Trip Time (RTT), statistiche TCP (ritrasmissioni, pacchetti scaduti, perdita di pacchetti) e byte e pacchetti trasmessi
- **Archivia su disco** statistiche sul traffico persistenti per consentire ricerche e analisi per periodi passati
- **Scope i protocolli applicativi** (Facebook, YouTube, BitTorrent, ecc.) Sfruttando la tecnologia nDPI , ntop Deep Packet Inspection (DPI)
- Supporto per **l'esportazione di dati** monitorati da MySQL , ElasticSearch e LogStash
- **Esplorazione storica** interattiva dei dati monitorati esportati su MySQL

## Ntop in Italferr dal 2013, qualificare il traffico in tempo reale.

ntop

🏠
🌐
⚠️
Flows
Hosts
Interfaces
Devices
⚙️
🔌

enp0s25: Top Local Talkers	Actual Traffic
pdl09244.italferr.corp.local [ITALFERR]	9.24 Mbit/s ↑
pdl09438.italferr.corp.local [ITALFERR]	4.81 Mbit/s ↑
pdl09087.italferr.corp.local [ITALFERR]	3.49 Mbit/s ↓
pdlp02156.italferr.corp.local [ITALFERR]	1.79 Mbit/s ↑
pdlp01760.italferr.corp.local [ITALFERR]	1.3 Mbit/s ↓
pdl08541.italferr.corp.local [ITALFERR]	736.79 kbit/s ↑
pdl08828.italferr.corp.local [PDL08828]	648.06 kbit/s ↑
pdlp02365.italferr.corp.local	593.12 kbit/s ↑
10.87.128.80	173.67 kbit/s ↑

enp0s25: Realtime Top Application Traffic

Network Interfaces: Realtime Traffic

enp0s25: Top Remote Destinations	Actual Traffic
10.69.1.4	11.17 Mbit/s ↑
lyncdiscoverinternal.italferr.it	8.02 Mbit/s ↑
10.246.132.29	3.42 Mbit/s ↓
mbox.cert.legalmail.it	2.36 Mbit/s ↑
10.246.131.35	1.4 Mbit/s ↓
10.19.60.175	1.26 Mbit/s ↑
10.2.7.42	1.0 Mbit/s ↑
10.2.7.100	722.66 kbit/s ↑
ifdmc005rm01.italferr.corp.local [@]	392.27 kbit/s ↑

enp0s25: Top Application Traffic Last Day View

Network Interfaces: Last Day View

ntopng Enterprise Edition v.3.9.190405  
 User 6001240 Interface enp0s25

27%  
26.83 Mbit/s [4,500 pps]

🕒 12:42:56 +0200 | Uptime: 4 days, 01:40:47  
282 🖨️
1,007 🖨️
13 Devices
2,682 Flows

	Application▼	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
<a href="#">Info</a>	G+ HTTP.GoogleServices <a href="#">🔗</a>	TCP	pdld08017.italferr.corp.....:63656	mtalk.google.com:http-alt	< 1 sec	Client Server	0 bit/s ➡	8.03 KB	mtalk.google.com
<a href="#">Info</a>	G+ HTTP.GoogleServices <a href="#">🔗</a>	TCP	pdld01760.italferr.corp.....:59824	www.googletagservices.co...:http-alt	00:45	Client Server	0 bit/s ➡	3.32 KB	www.googletagservices.co...
<a href="#">Info</a>	DNS.Office365 <a href="#">🔗</a>	UDP	pdld08681.italferr.corp.....:54495	ifdmc008rm01.italferr.co...:domain	< 1 sec	Client Server	0 bit/s ➡	223 Bytes	crl.microsoft.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld09087.italferr.corp.....:58550	nexusrules.officeapps.li...:http-alt	00:02	Server	0 bit/s ➡	47.63 KB	nexusrules.officeapps.li...
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld07565.italferr.corp.....:63291	nexusrules.officeapps.li...:http-alt	00:01	Server	0 bit/s ➡	43.42 KB	nexusrules.officeapps.li...
<a href="#">Info</a>	DNS.Office365 <a href="#">🔗</a>	UDP	pdld08935.italferr.corp.....:55111	ifdmc008rm01.italferr.co...:domain	< 1 sec	Client Server	0 bit/s ➡	223 Bytes	crl.microsoft.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld09574.italferr.corp.....:58402	outlook.office365.com:http-alt	00:02	Client Server	0 bit/s ➡	8.55 KB	outlook.office365.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld09574.italferr.corp.....:58396	odc.officeapps.live.com:http-alt	00:02	Client Server	0 bit/s ➡	10.32 KB	odc.officeapps.live.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld09574.italferr.corp.....:58395	nexusrules.officeapps.li...:http-alt	00:01	Client Server	0 bit/s ➡	8.53 KB	nexusrules.officeapps.li...
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld09217.italferr.corp.....:61459	nexusrules.officeapps.li...:http-alt	00:01	Client Server	0 bit/s ➡	11.48 KB	nexusrules.officeapps.li...
<a href="#">Info</a>	DNS.Office365 <a href="#">🔗</a>	UDP	pdld08681.italferr.corp.....:62771	ifdmc008rm01.italferr.co...:domain	< 1 sec	Client Server	0 bit/s ➡	223 Bytes	crl.microsoft.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld09244.italferr.corp.....:62093	outlook.office365.com:http-alt	00:02	Client Server	0 bit/s ➡	8.51 KB	outlook.office365.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld09244.italferr.corp.....:62091	odc.officeapps.live.com:http-alt	00:01	Client Server	0 bit/s ➡	10.33 KB	odc.officeapps.live.com
<a href="#">Info</a>	DNS.Office365 <a href="#">🔗</a>	UDP	pdld09217.italferr.corp.....:63018	ifdmc008rm01.italferr.co...:domain	< 1 sec	Client Server	0 bit/s ➡	223 Bytes	crl.microsoft.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld08613.italferr.corp.....:55693	outlook.office365.com:http-alt	00:02	Client Server	0 bit/s ➡	6.68 KB	outlook.office365.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld09244.italferr.corp.....:62090	nexusrules.officeapps.li...:http-alt	00:02	Client Server	0 bit/s ➡	8.53 KB	nexusrules.officeapps.li...
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld08613.italferr.corp.....:55686	odc.officeapps.live.com:http-alt	00:02	Client Server	0 bit/s ➡	10.23 KB	odc.officeapps.live.com
<a href="#">Info</a>	HTTP.Office365 <a href="#">🔗</a>	TCP	pdld08613.italferr.corp.....:55685	nexusrules.officeapps.li...:http-alt	00:02	Client Server	0 bit/s ➡	9.81 KB	nexusrules.officeapps.li...

ntop

Home Alerts Flows Hosts Interfaces Devices Settings Power

Host: 10.87.37.170
Traffic
Packets
Ports
Peers
Applications
DNS
HTTP
Flows
Sites
SNMP
Talkers

<b>(Router/AccessPoint) MAC Address</b>	Cisco_FB:FB:C8 ( 30:E4:DB:FB:FB:C8 )	+ Router/Switch ⚙
<b>IP Address</b>	10.87.37.170 [ 10.87.0.0/16 ]	Host Pool: Not Assigned ⚙
<b>Name</b>	pdld09350.italferr.corp.local [ Local Private ]	
<b>First / Last Seen</b>	29/03/2019 09:33:06 [11 days, 04:05:43 ago]	09/04/2019 14:38:35 [00:14 ago]
<b>Sent vs Received Traffic Breakdown</b>	<div style="display: flex; justify-content: space-around; width: 100%;"> <div style="width: 45%; background-color: #f96; text-align: center;">Sent</div> <div style="width: 45%; background-color: #00a0c0; text-align: center;">Rcvd</div> </div>	
<b>Traffic Sent / Received</b>	4,560,137 Pkts / 410.51 MB —	10,624,268 Pkts / 13.52 GB —
<b>Flows: Active / Total / Low Goodput / Anomalous / Port Unreach</b>	<b>As Client</b>	<b>As Server</b>
	12 ↓ / 74,886 ↑ / 0 — / 3,253 — / 3 —	0 — / 68 — / 0 — / 51 — / 0 —
<b>TCP Packets Sent Analysis</b>	<b>Retransmissions</b>	20 Pkts —
	<b>Out of Order</b>	0 Pkts —
	<b>Lost</b>	2 Pkts —
	<b>KeepAlive</b>	0 Pkts —
<b>Reset Host Stats</b>	<input type="button" value="Reset Host Stats"/>	
<b>Additional Host Names</b>	<b>Source</b>	<b>Name</b>
	DNS Resolution	pdld09350.italferr.corp.local
<b>Download</b> ⬇	JSON	<div style="display: flex; gap: 10px;"> <span>1 min ▾</span> <input type="text" value="Filter (BPF)"/> <input type="button" value="pcap download"/> </div>

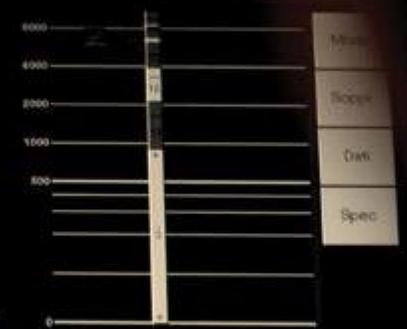
# L'integrazione



THE ENGINE TO BE USED FOR  
THE ENGINE TO BE USED FOR

km/h

F5 F6 F7 F8



A control panel for the digital instrument cluster. It features a central display area with a gear shift indicator, a 'P' button, and a 'D' button. Below the display is a row of buttons: a 'X' button, followed by ten directional buttons (up, down, left, right), and a 'D' button. At the bottom right, there are two buttons labeled '2046'.

# ntop + Nagios®

Integrazione ntop Nagios in Italferr

La flessibilità dei due strumenti open source ha permesso la loro integrazione

ntop



Nagios®

# ntop + Nagios®

L'integrazione



SNMP lettura delle mib

ntop



Router  
sede/cantiere

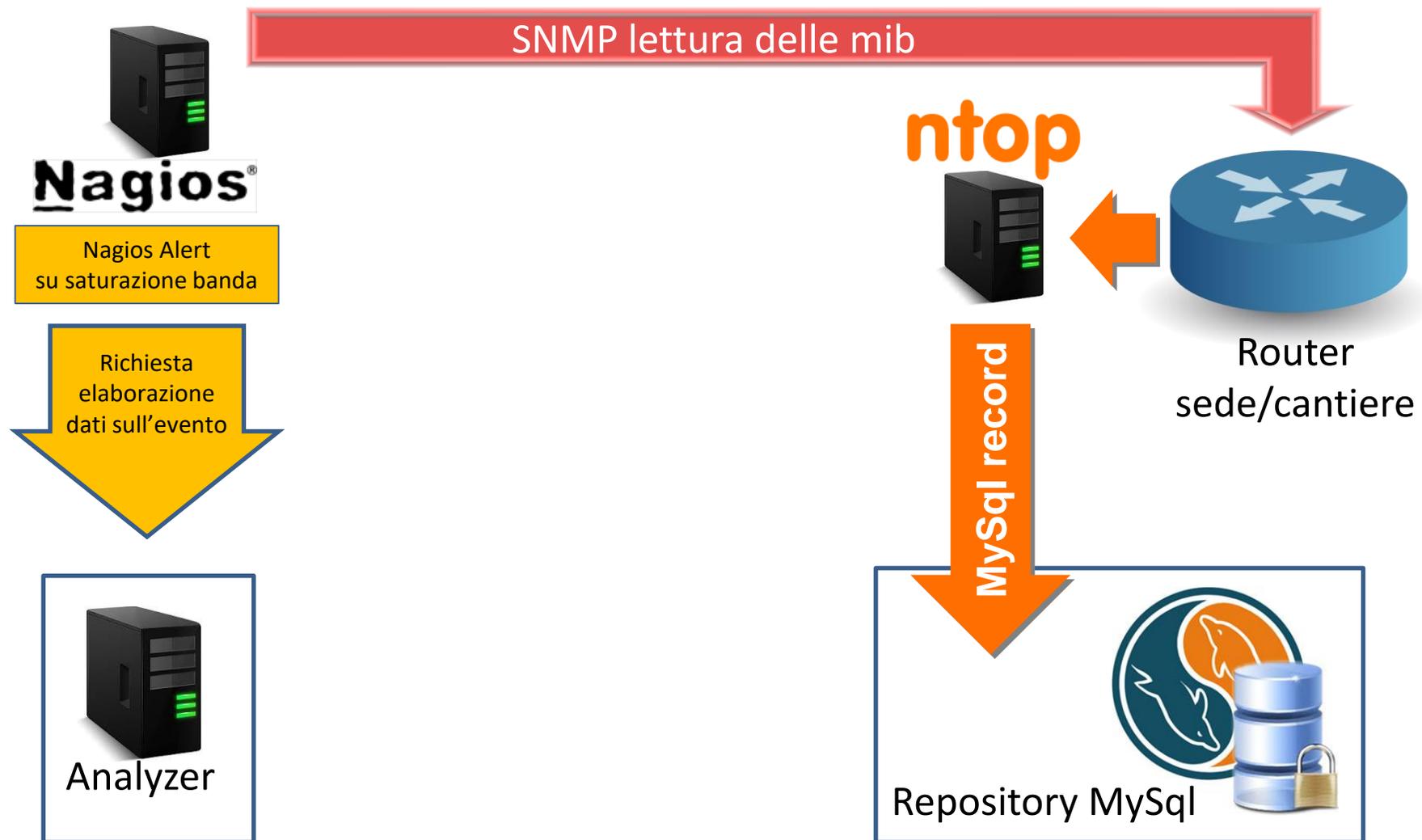
MySQL record



Repository MySQL

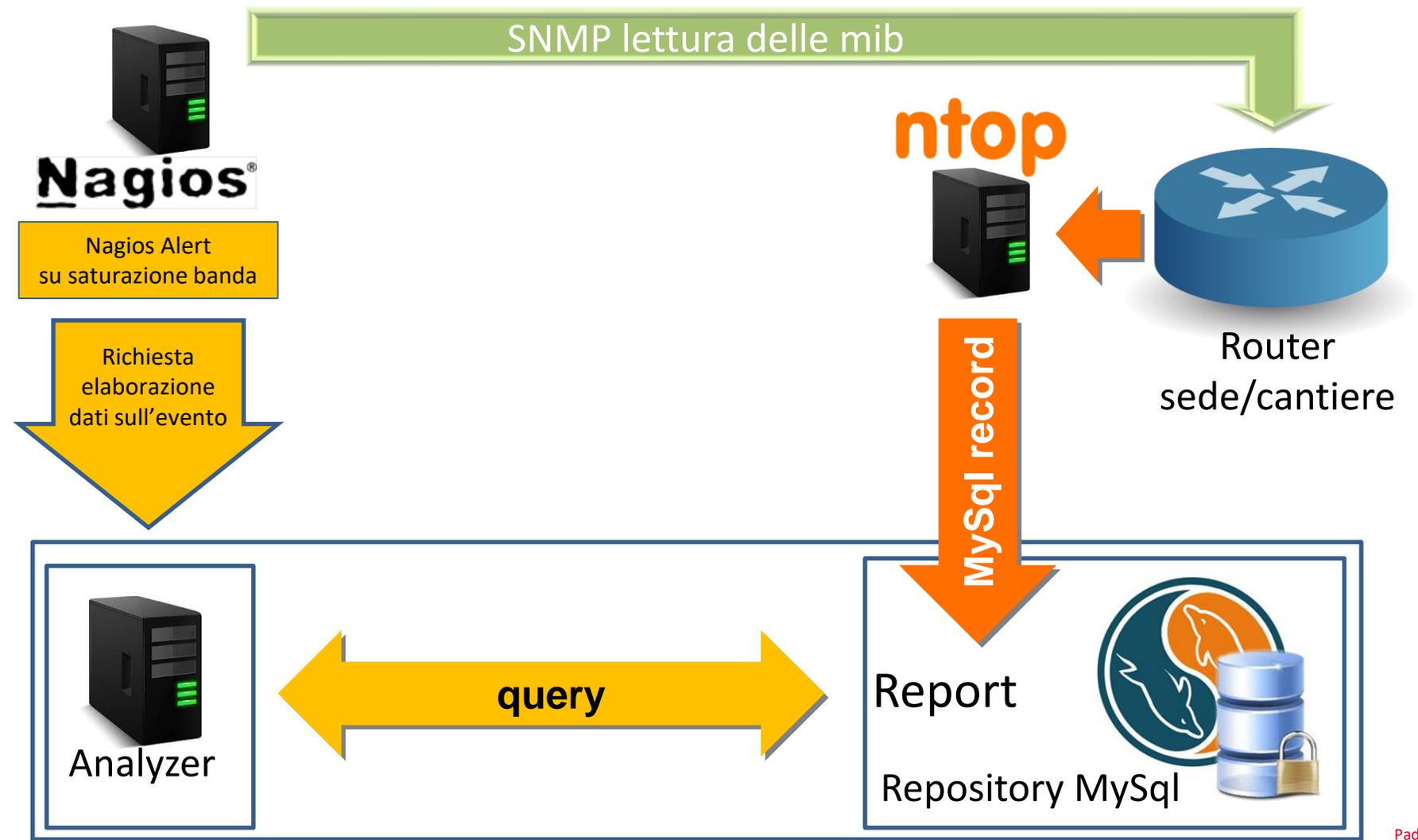
# ntop + Nagios®

L'integrazione



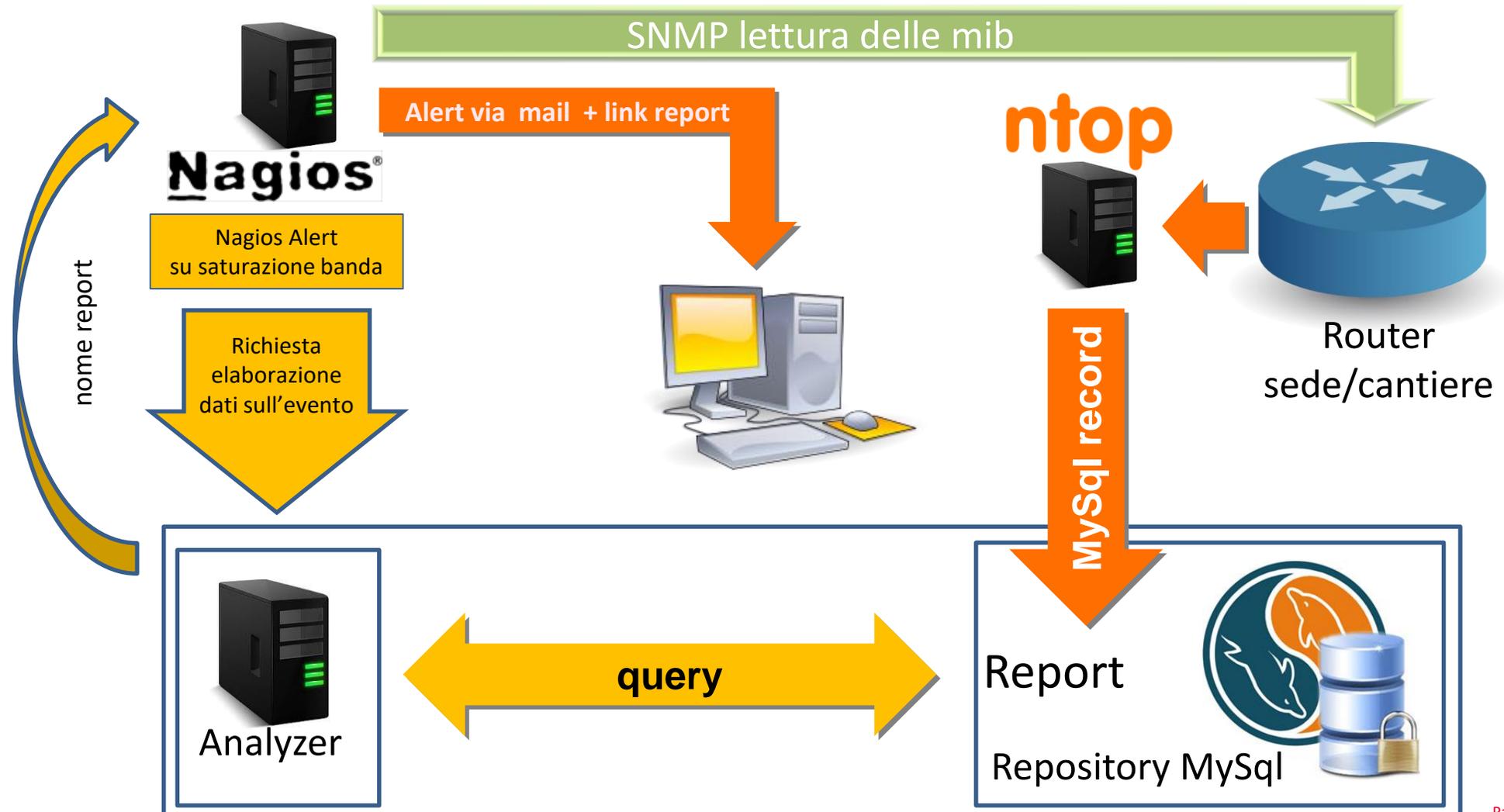
# ntop + Nagios®

L'integrazione



# ntop + Nagios®

L'integrazione



# ntop + Nagios®

L'integrazione



venerdì 05/04/2019 16:06  
 NagiosXI <nagiosxi@italferr.it>  
 \*\* Traffico eccessivo per l'host Milano\_Sede con URL\*\*  
 A stefano.bizzarro@technoinside.it; a.raimo.italferr.it@italferr.it



L'host Milano\_Sede ha superato la soglia di traffico di guardia per 1 ora.  
 L'analisi e' disponibile qui:

[alyzer/generated/Milano\\_Sede\\_2019-04-05\\_16:0611\\_2019-04-05\\_15:06:11-agi.html](#)  
 disponibile qui:  
[ferr.it/ua/pro/report.lua?num\\_minutes=60&period\\_begin\\_str=05%2F04%2F2019%2015%3A06%3A11&period\\_end\\_str=05%2F04%2F2019%2016%3A06%3A11](#)

Tabella RENT001GE01 Record analisi 30865

Stato    Traffico per host    Traffico per protocollo

Cerca:		
Protocollo	Traffico	Traffico %
Totale	17.62 GB	100.00 %
DPM	16.53 GB	93.83 %
HTTP_Proxy	226.16 MB	1.25 %
SMB	224.40 MB	1.24 %

Host	Traffico trasmesso
10.76.32.193	35.21 MB
10.19.149.41	25.97 MB
10.19.61.60	9.71 MB
10.76.32.95	6.16 MB
10.76.33.99	3.98 MB
10.76.30.240	3.29 MB

Total Traffic: 8.96 GB

Top Networks [Average Traffic/sec]

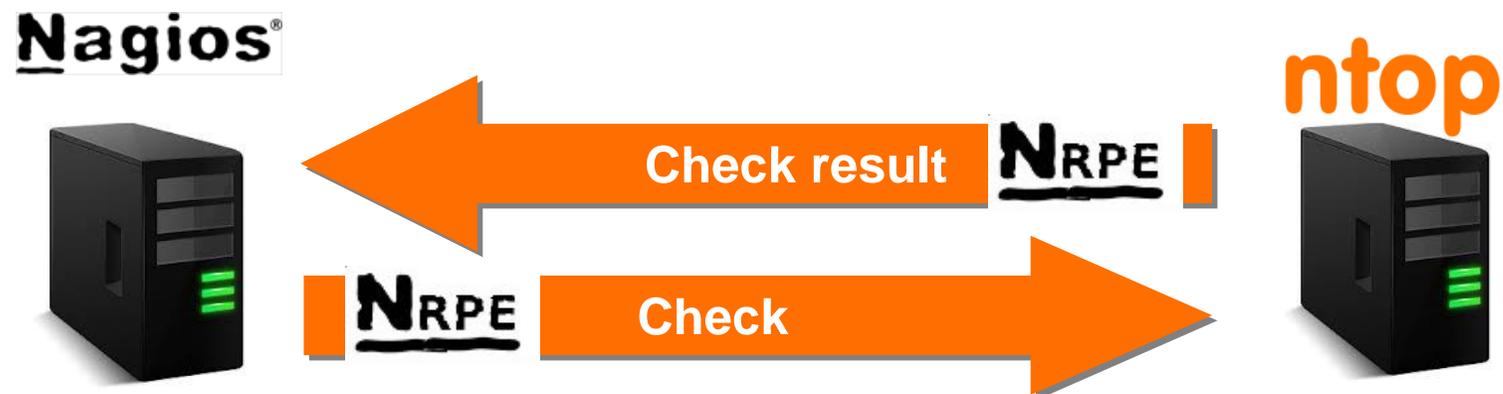
Senders		Receivers	
10.87.0.0/16	5.10 GB (12.17 Mbit/s)	10.87.0.0/16	1.92 GB (4.57 Mbit/s)
10.19.87.0/24	426.23 MB (993.19 Kbit/s)	172.16.87.0/24	34.10 MB (79.45 Kbit/s)
172.16.87.0/24	50.95 MB (118.73 Kbit/s)	10.19.87.0/24	22.67 MB (52.83 Kbit/s)

Applications

Application Breakdown

# ntop + Nagios®

## Integrazione ntop Nagios in Italferr



Host	Service	Status	Duration	Attempt	Last Check	Status Information
ntopmilano.italferr.it	Data Transfer	Ok	4d 4h 35m 50s	1/10	2019-04-09 15:41:56	0
	Database records count	Ok	11m 4s	1/10	2019-04-09 15:41:44	3146
	Load	Ok	4d 4h 35m 8s	1/10	2019-04-09 15:42:05	OK - load average: 0.44, 0.60, 0.86
	Maintenance status	Ok	4d 4h 35m 35s	1/10	2019-04-09 15:42:01	Maintenance: Until Sat Dec 21 08:10:02 2019 [255 days left]
	Ntop database records count	Ok	4d 4h 35m 50s	1/10	2019-04-09 15:41:31	6921920
	Ntopng Process	Ok	1d 15h 40m 20s	1/10	2019-04-09 15:41:51	1
	Ntopng Secondary Process	Ok	4d 4h 35m 40s	1/10	2019-04-09 15:41:11	1
	Ping	Ok	6d 5h 23m 53s	1/10	2019-04-09 15:41:58	OK - 10.19.87.38: rta 13.071ms, lost 0%

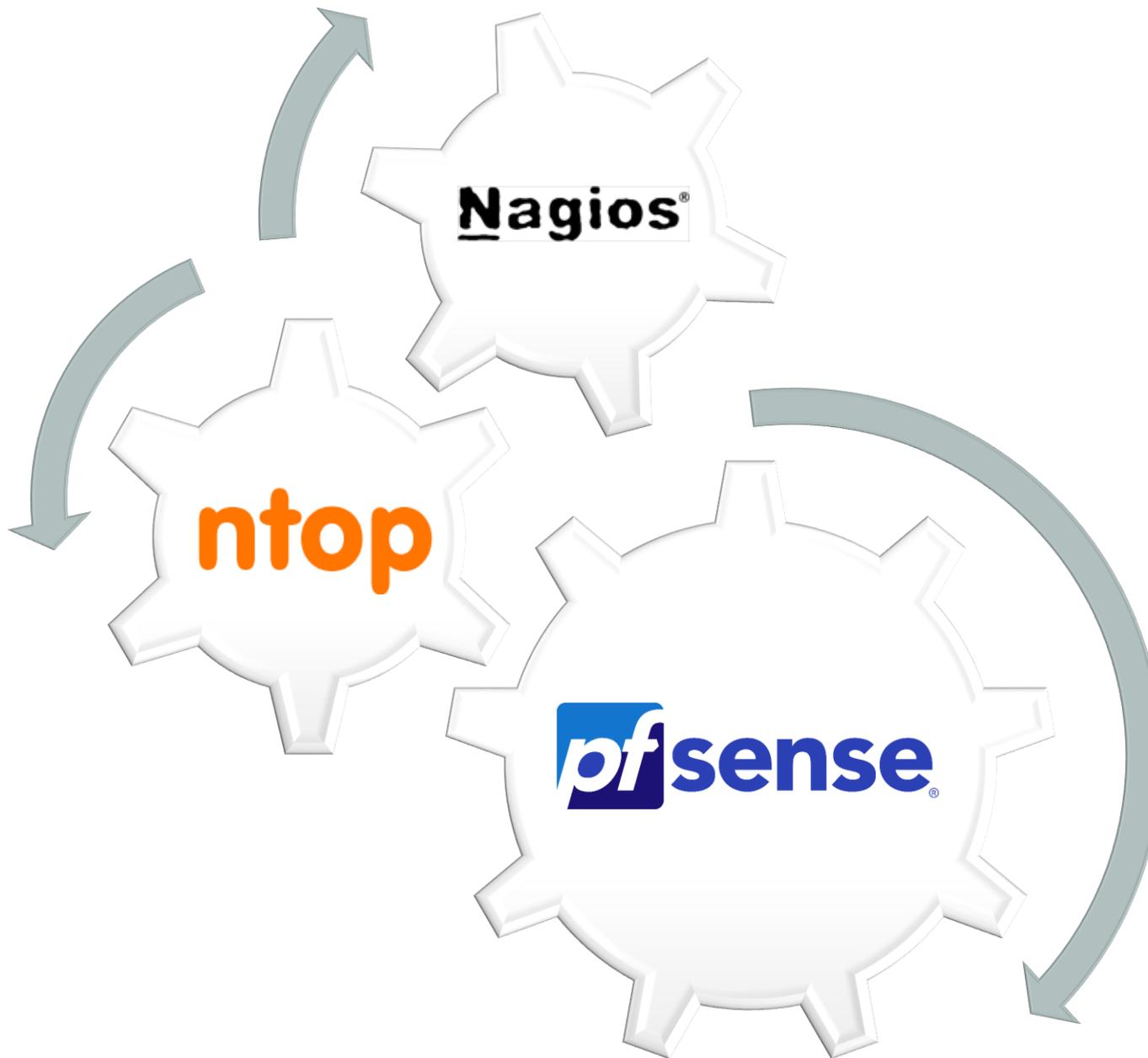
# Sviluppi futuri

Il limite è la fantasia non la tecnologia



## Sviluppi futuri

Stiamo sviluppando una soluzione per erogare connettività svincolata dalla tecnologia trasmissiva e dagli operatori che vede nell'integrazione tra **pfsense** e **ntop** la soluzione.



# Considerazioni finali



## Costi

L'open source è free ma non è gratis:  
sposta gli investimenti dai cespiti alle persone



## Stabilità

13 anni di utilizzo



## Flessibilità

Integrazione in processi interni SI

**Grazie**

**Domande e risposte (forse)**

