

# Strumenti di monitoring per la MAN universitaria pisana

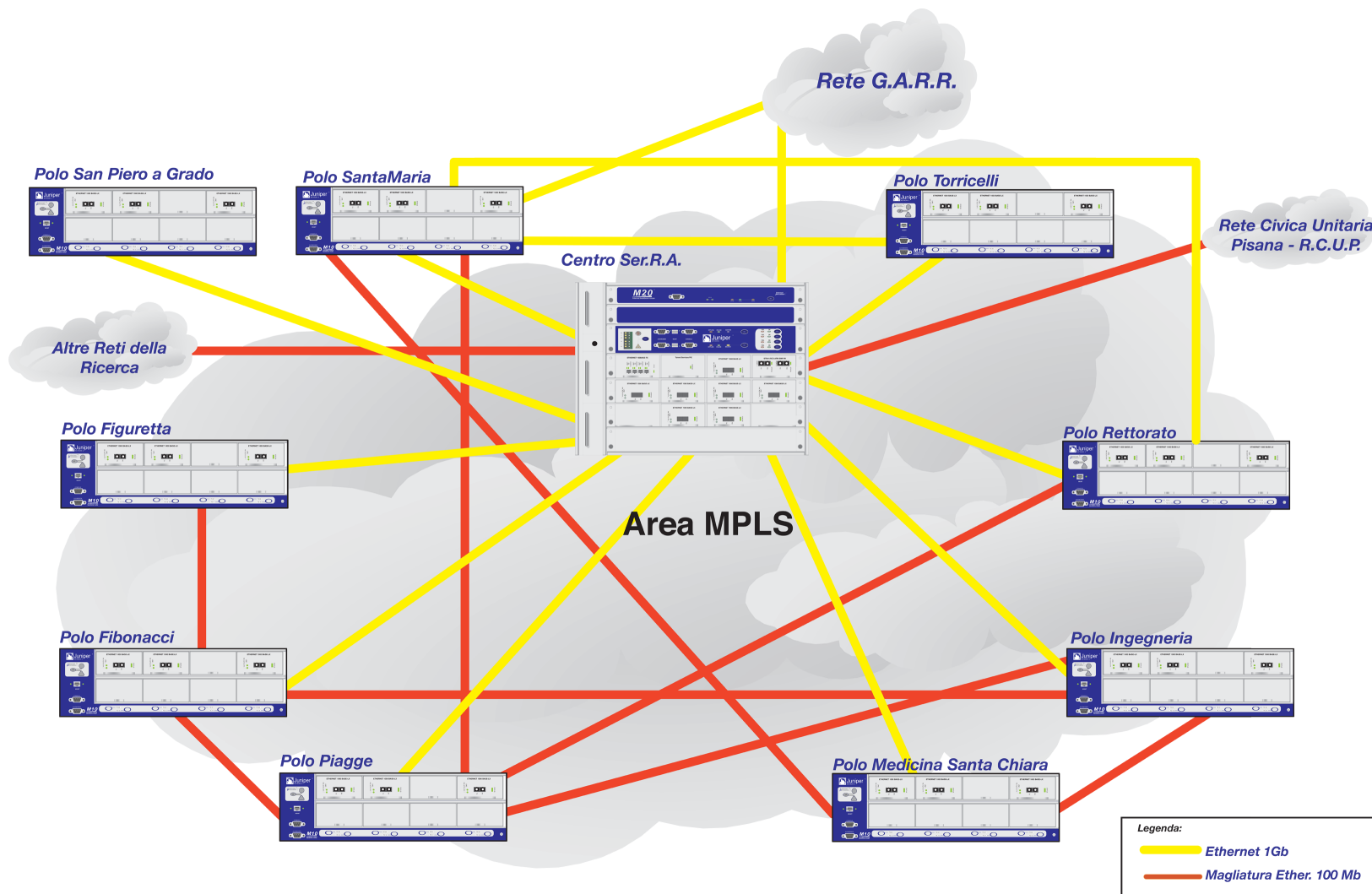


[simone.spinelli@unipi.it](mailto:simone.spinelli@unipi.it)

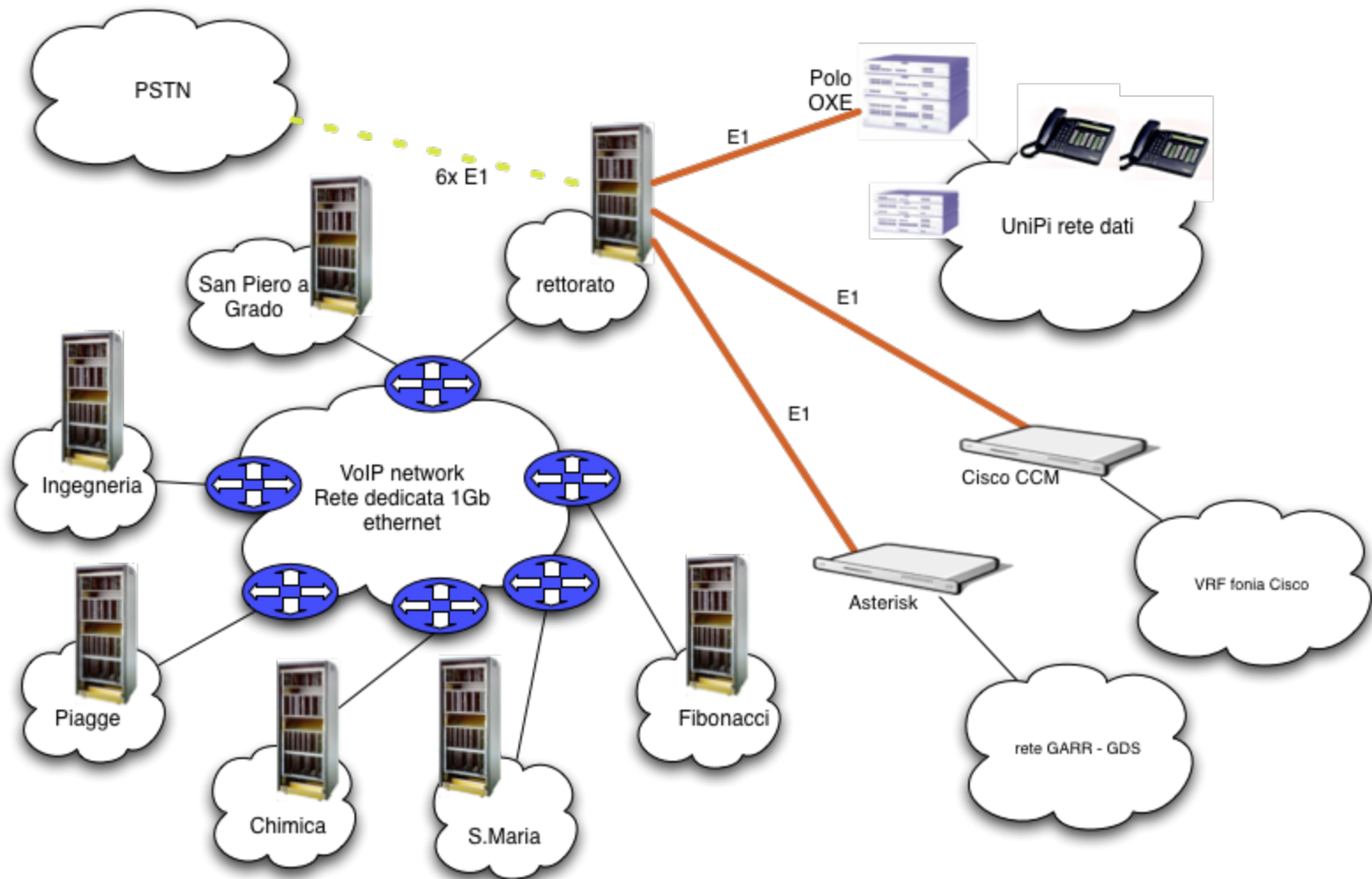
Garr-X il futuro della rete

- Una rete Campus/MAN di proprietà basata su una infrastruttura in F.O. con circa 50Km. di canalizzazioni
- Circa 200 siti diversi raggiunti ciascuno con 8 diverse fibre per i seguenti servizi:
  - Dati
  - Voce
  - Amministrazione
  - Usi diversi
- Circa 80 Km. di cavi in F.O. stesi sul territorio
- Copertura capillare del nord e del centro di Pisa
- Estensione da est - San Piero a Grado - ad ovest - Ospedaletto dell'area del comune di Pisa
- Interoperabilità con carrier diversi e enti diversi
- Reti cittadine parallele: R.C.U.P.

# La rete UniPi: topologia

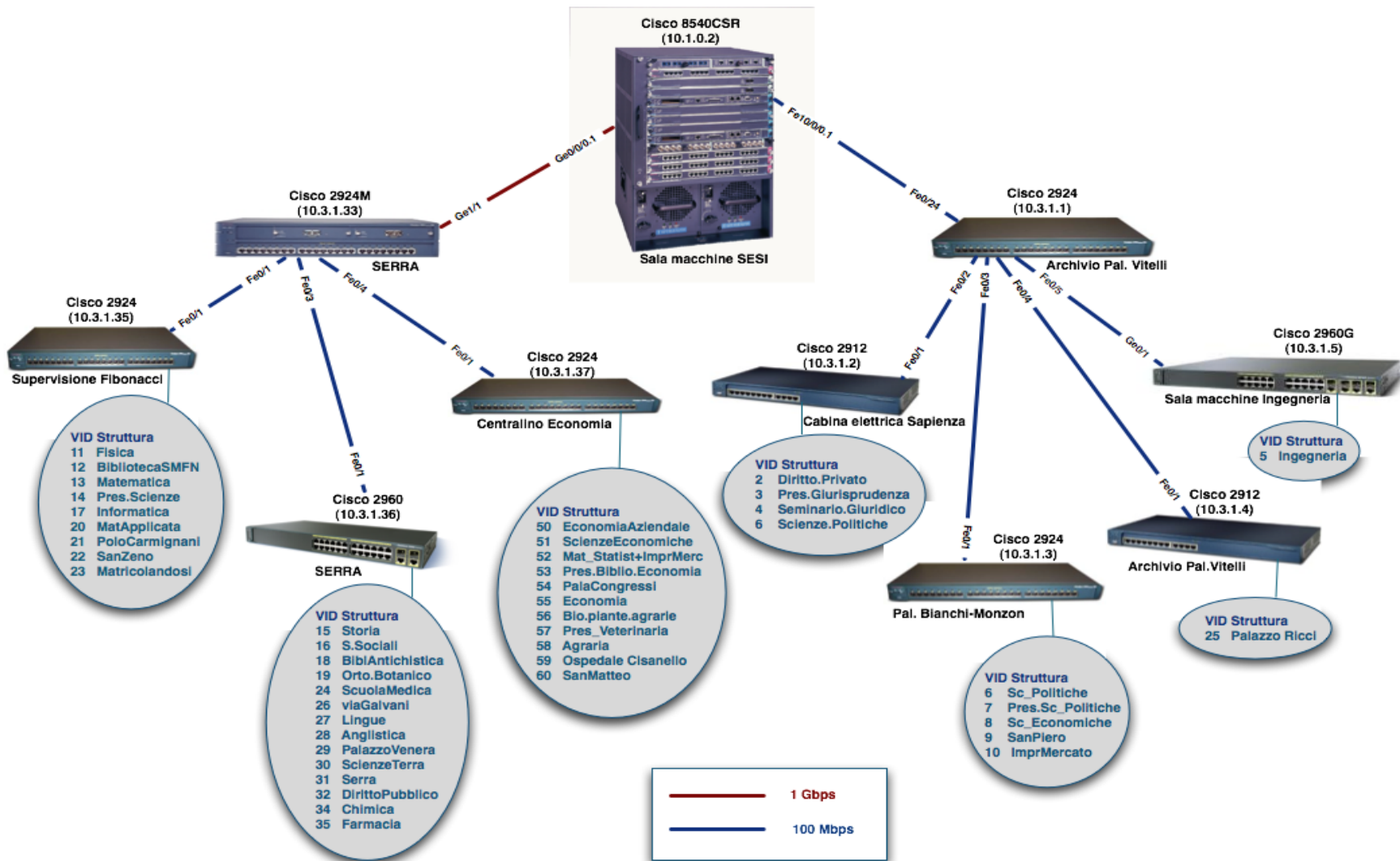


Garr-X il futuro della rete

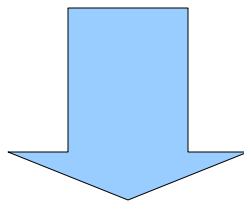


Garr-X il futuro della rete

# La rete amministrativa

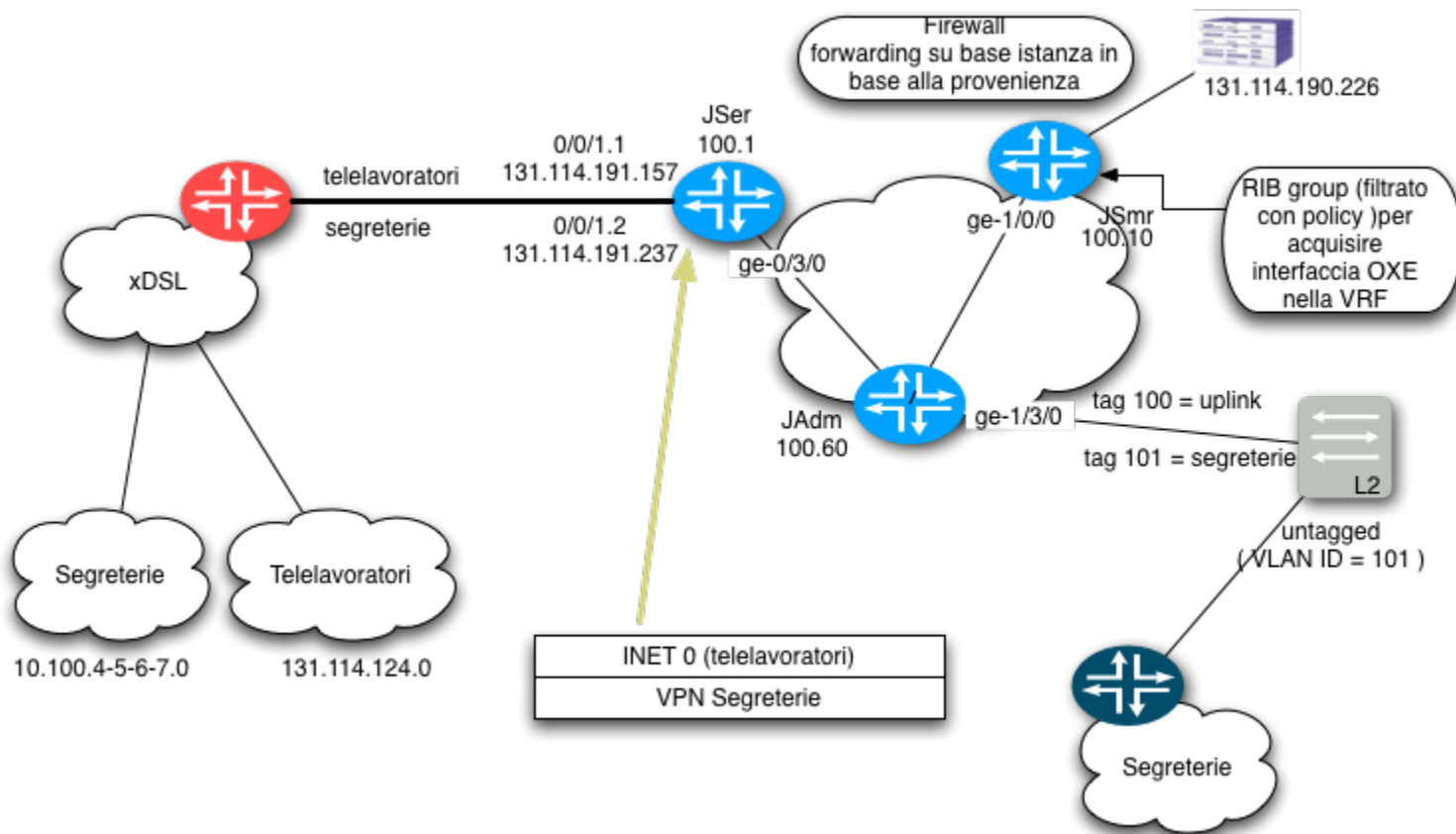


Oltre alle reti prima illustrate, che sono fisicamente segregate fra loro, abbiamo comunità che vengono trattate con tecnologie di virtualizzazione di rete sia di livello 2 che di livello 3, a volte (come nel caso di alcune segreterie studenti) anche passando attraverso altri provider.



C'e' uno strato ulteriore al quale il sistema di monitoring deve elevarsi per poter svolgere la sua funzione.

# Le Segreterie remote



Quello che ci si aspetta da un sistema di monitoring e' che ci venga fornito lo stato e i cambiamenti di stato di:

- rete
- apparati di rete
- server
- servizi

Questo per tutte le reti delle quali abbiamo parlato prima.

Occorrerà quindi che le macchine che si occupano del monitoring abbiano accesso a tali reti .



Altre caratteristiche che il sistema deve avere sono:

- supporto multivendor: uso di protocolli standard
- poco invasivo, viste le diverse soluzioni di connettività
- facilmente adattabile alle nostre esigenze
- stabilità
- scalabilità
- basso costo (umano e finanziario)

Abbiamo diviso il problema in tre fronti

## **Allarmistica :**

Ci informa se qualcosa smette di funzionare o supera certi limiti prefissati.

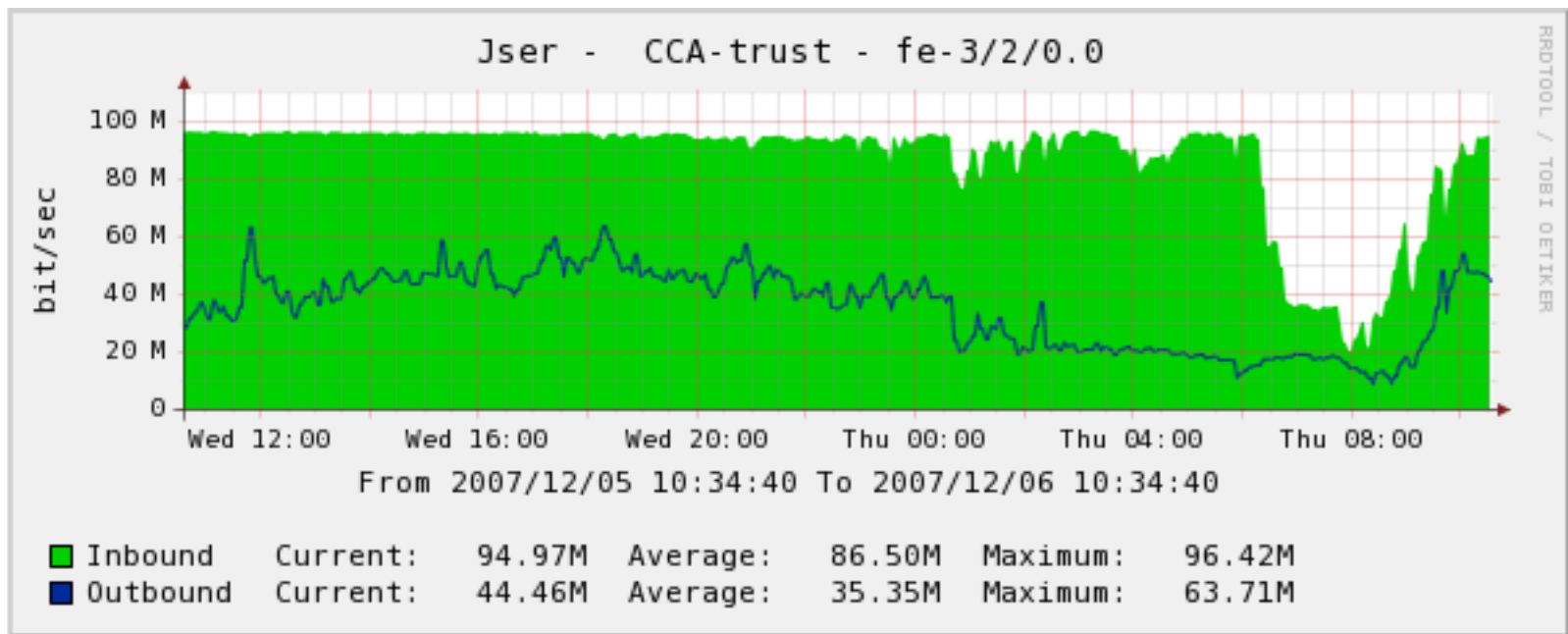
## **Analisi del traffico:**

Permette di capire che traffico attraversa la nostra rete, se alcune categorie di traffico sono penalizzate rispetto ad altre, aiuta nella individuazione delle politiche di filtering e QoS . (ancora in fase di sviluppo)

## **Raccolta statistiche:**

Ci serve per sapere l'andamento medio, nel tempo, di una certa variabile, da qui avremo una indicazione dell'utilizzo della risorsa

Una tipica situazione da evitare....



# Gli strumenti scelti:

## **La soluzione scelta per la produzione di grafici e' Cacti:**

“The complete rrdtool-based graphing solution”

Cacti ci consente di graficare una grande quantita' di variabili di interesse, quali traffico sulle interfacce, temperature, carico macchina e quant'altro.

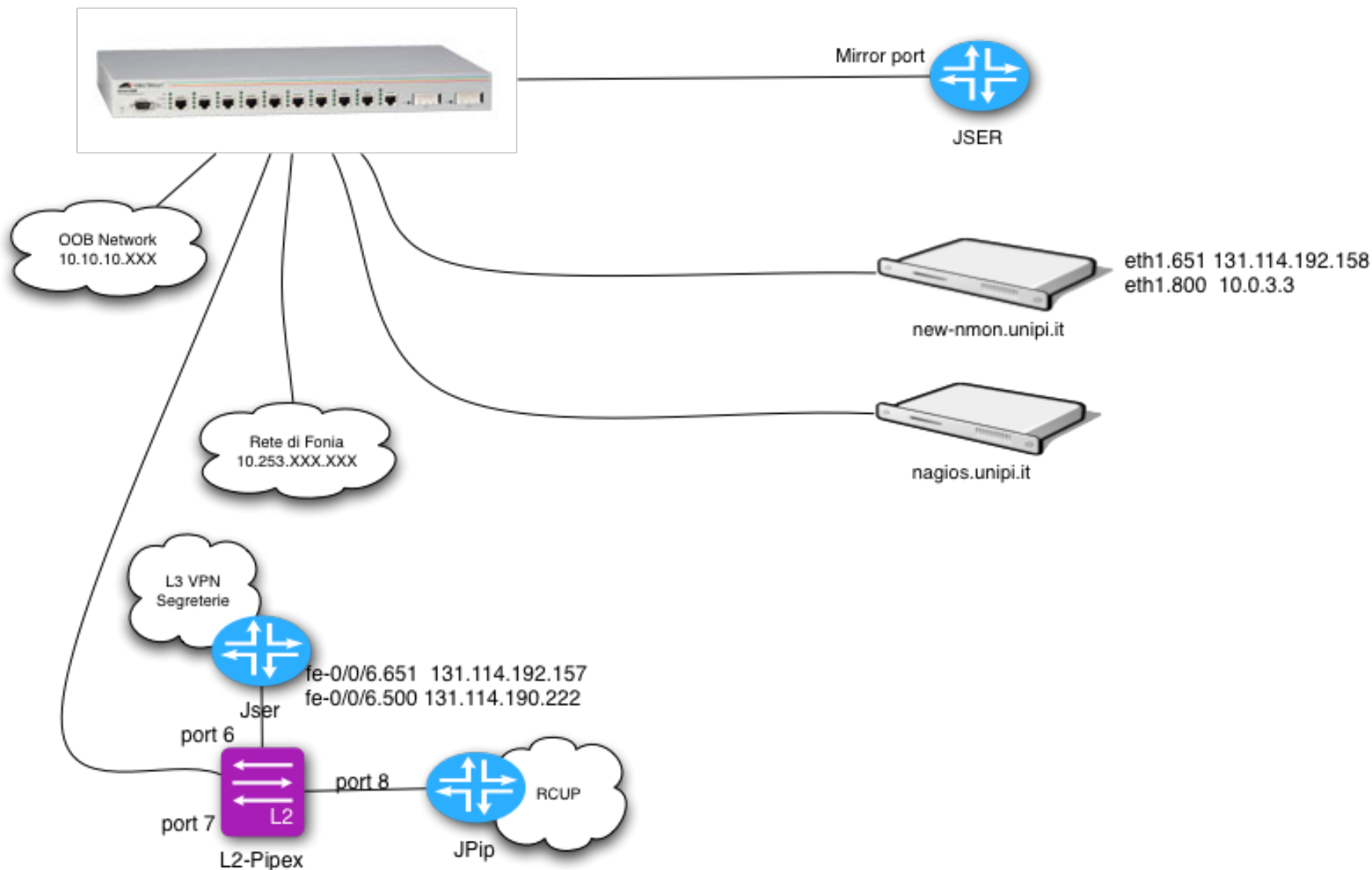
## **Per la parte di allarmistica la scelta e' ricaduta su Nagios :**

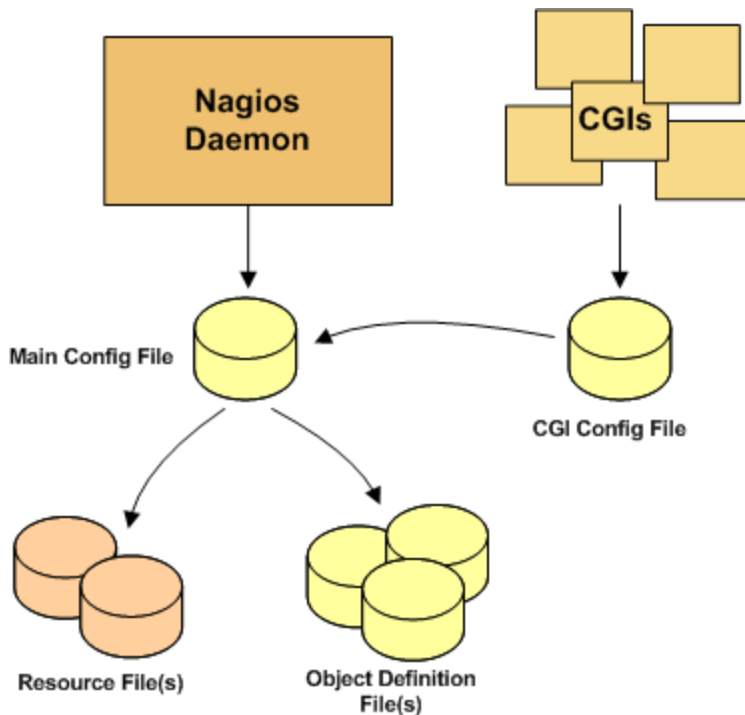
“Nagios Ain't Gonna Insist On Sainthood”

Si tratta di un sistema di monitoring completo che permette di controllare apparati di rete, server, e servizi

## **Per l'analisi del traffico di rete ci siamo orientati verso Ntop:**

Una soluzione pensata appositamente per questo tipo di applicazioni che permette elevate performances anche su reti ad elevato carico.



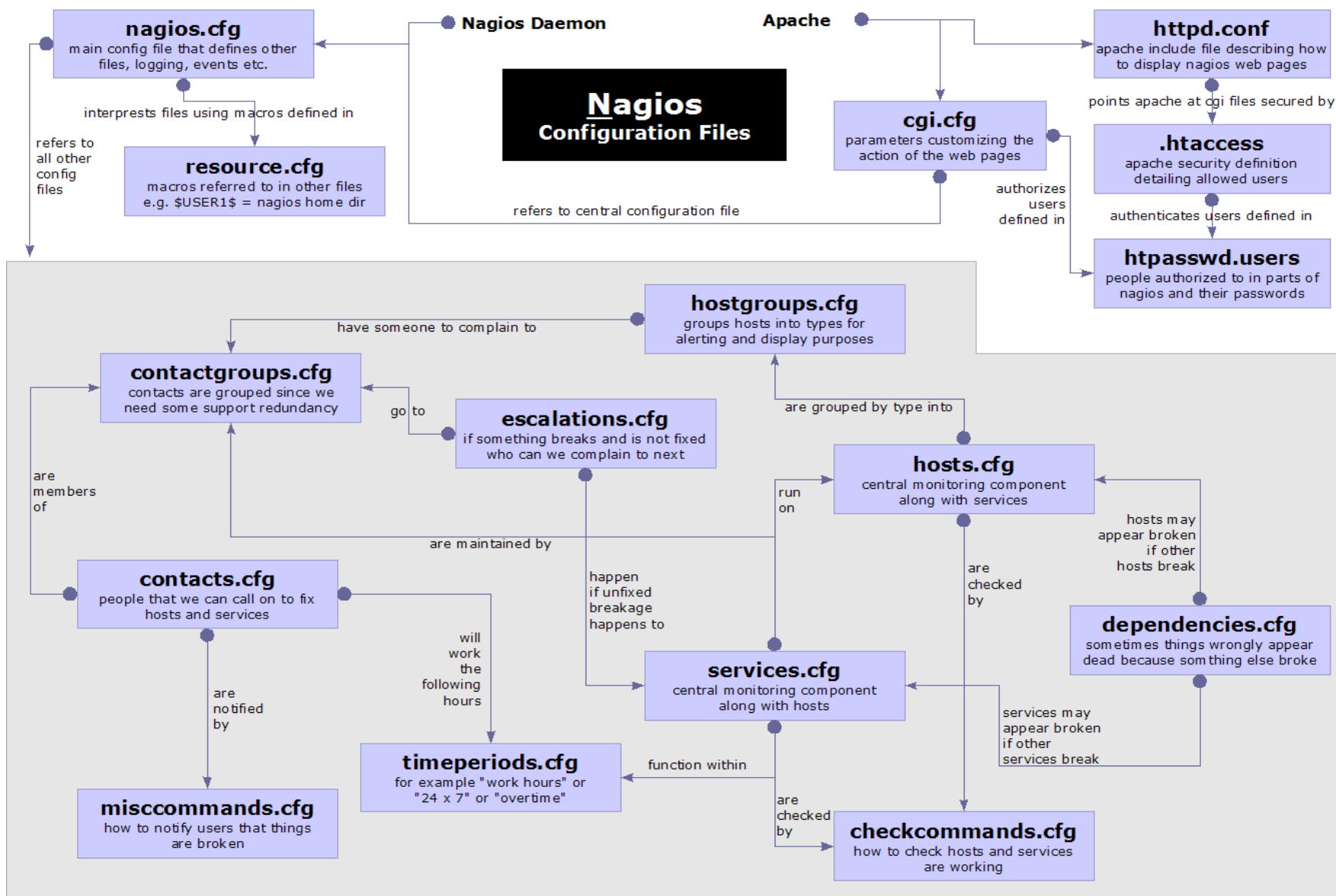


- Si tratta di un demone che gestisce tutte le operazioni.
- Negli Object Definition Files si specificano hosts, services, hostgroups, contacts, contactgroups, commands, etc.
- Nei Resource Files le configurazioni sensibili (tipo password) per non renderle disponibili ai cgi.
- CGI Config Files: configurazioni dei CGI (responsabili dell'interfaccia web)

## Dove reperire il codice:

- [www.nagios.org](http://www.nagios.org) : nagios daemon, nrpe, plugin standard
- [www.nagiosexchange.org](http://www.nagiosexchange.org) : plugin di ogni genere e tipo
- **Un po' ovunque si trova qualcuno che ha scritto qualcosa**
- Si trovano i pacchetti per molte distribuzioni
- Per compilare il sorgente un semplice `./configure && make && make install` è sufficiente nella maggior parte dei casi
- Si tratta di una architettura a plugin. Oltre al demone si puo' installare altro software, il piu' importante è nrpe (Nagios Remote Plugin Executor) ma ci sono una infinità di plugin scritti da una vasta e attiva comunità di sviluppatori.

# Nagios: configurazione





Tanti files di configurazione che possono confondere il sistemista

- Fortunatamente si tratta di una configurazione intuitiva: tutto va dove ci si aspetta che vada
- Nagios fornisce l'utile strumento di verifica (`nagios -v nagios.cfg`) che va sempre usato

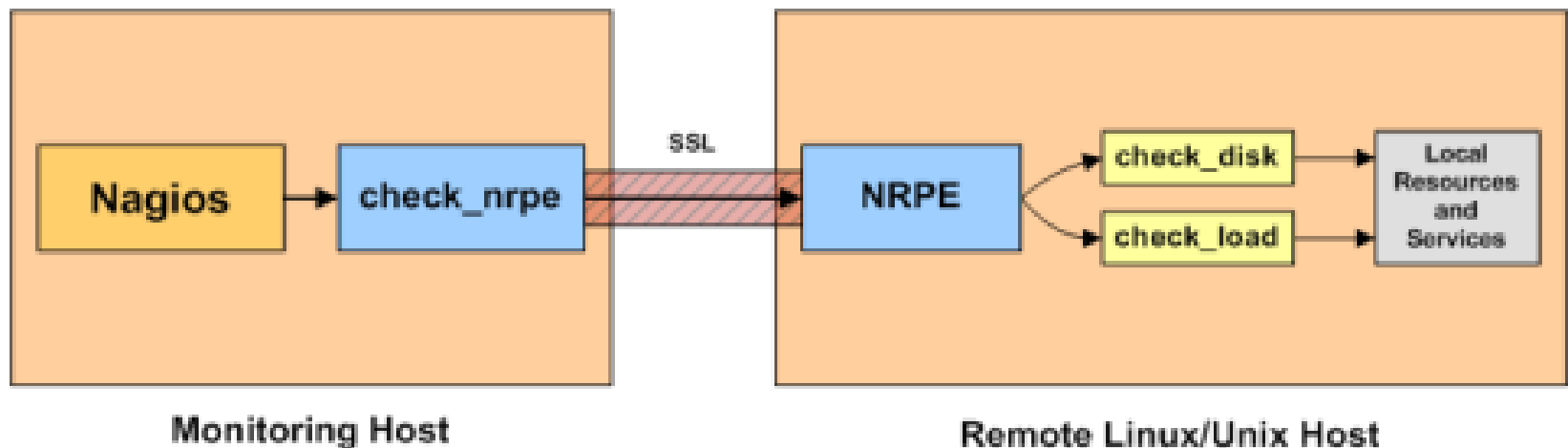
# Configurazione host:

```
# Generic host definition template
define host{
    name                generic-host
    notifications_enabled 1
    event_handler_enabled 1
    flap_detection_enabled 1
    process_perf_data    1
    retain_status_information 1
    retain_nonstatus_information 1
    register              0
    contact_groups        serra-group
}
```

```
define host{
    use                generic-host
    host_name          router_Rettorato
    alias              router_Rettorato
    address            10.253.1.200
    check_command      check-host-alive
    hostgroups         retefonia_Router
    max_check_attempts 10
    notification_interval 120
    notification_period 24x7
    notification_options d,u,r
}
```

Si tratta di un agent che si installa sull'host (Linux/unix) monitorato:

- comunica con il server tramite ssl
- esegue I plugin in locale
- valida alternativa ad SNMP



# Configurazione servizio:

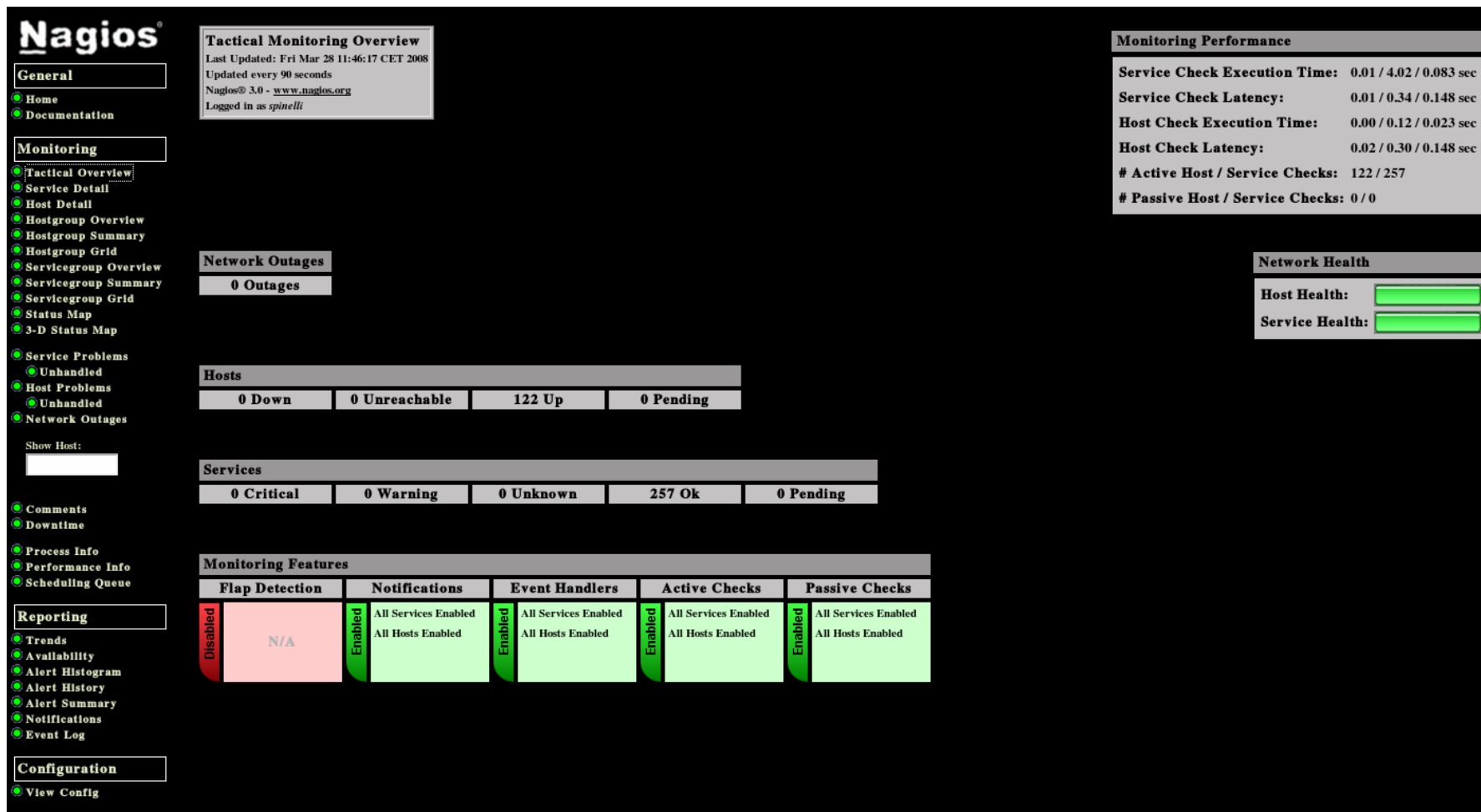
```
define service{
    use                network-service
    host_name          router_Rettorato
    service_description check_ospf_with_Piagge
    check_command      check_ospf!192.168.1.14:Piagge
}
```

```
define service{
    use                local-service
    host_name          mailserver,mixer
    service_description remote_check_amavisd
    check_command      check_nrpe_t60!check_amavisd
}
define service{
    use                local-service
    host_name          asterisk,new-nmon,marvin
    service_description remote_check_linux_raid
    check_command      check_nrpe!check_linux_raid
}
```

A nagios abbiamo affidato tutta l'allarmistica:

- si tratta di un software che scala piuttosto bene, al momento abbiamo 160 host monitorati con 297 servizi e un load average sulla macchina pressoché nullo
- ha una interfaccia web “bruttina” ma ben leggibile e completa
- come abbiamo già detto può contare su una comunità di sviluppatori grande e attiva
- fornisce report di disponibilità in maniera rapida, integrata e che sono facilmente comprensibili da tutti

- host alive service: con ping controlla che tutti gli host (router, servers, centrali telefoniche ecc...) siano effettivamente raggiungibili
- allarmistica sul routing: verifica lo stato dei collegamenti BGP,IS-IS,OSPF e presto anche lo stato degli LSP
- allarmistica sui server: occupazione dei filesystem, carico CPU, stato dei raid software ecc...
- allarmistica sui servizi: verifica che i servizi funzionino correttamente ( radius, webserver, antispam, ecc..)



**Nagios**  
 Tactical Monitoring Overview  
 Last Updated: Fri Mar 28 11:46:17 CET 2008  
 Updated every 90 seconds  
 Nagios® 3.0 - [www.nagios.org](http://www.nagios.org)  
 Logged in as *spinelli*

**Monitoring Performance**

Service Check Execution Time:	0.01 / 4.02 / 0.083 sec
Service Check Latency:	0.01 / 0.34 / 0.148 sec
Host Check Execution Time:	0.00 / 0.12 / 0.023 sec
Host Check Latency:	0.02 / 0.30 / 0.148 sec
# Active Host / Service Checks:	122 / 257
# Passive Host / Service Checks:	0 / 0

**Network Health**

Host Health: ██████████  
 Service Health: ██████████

**Network Outages**

0 Outages

**Hosts**

0 Down	0 Unreachable	122 Up	0 Pending
--------	---------------	--------	-----------

**Services**

0 Critical	0 Warning	0 Unknown	257 Ok	0 Pending
------------	-----------	-----------	--------	-----------

**Monitoring Features**

	Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Disabled	N/A	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled

**Reporting**

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

**Configuration**

- View Config

### Current Network Status

Last Updated: Fri Mar 28 11:46:50 CET 2008  
 Updated every 90 seconds  
 Nagios® 3.0 - [www.nagios.org](http://www.nagios.org)  
 Logged in as *spinelli*

- [View Service Status Detail For All Host Groups](#)
- [View Host Status Detail For All Host Groups](#)
- [View Status Overview For All Host Groups](#)
- [View Status Grid For All Host Groups](#)

### Host Status Totals

Up	Down	Unreachable	Pending
122	0	0	0

All Problems	All Types
0	122

### Service Status Totals

Ok	Warning	Unknown	Critical	Pending
257	0	0	0	0

All Problems	All Types
0	257

### Status Summary For All Host Groups

Host Group	Host Status Summary	Service Status Summary
<a href="#">Amministrazione Net (Amministrazione Net)</a>	10 UP	30 OK
<a href="#">Cisco CCM (Cisco CCM)</a>	3 UP	3 OK
<a href="#">P1P Fonia (P1P Fonia)</a>	5 UP	5 OK
<a href="#">Rete OOB (Rete OOB)</a>	9 UP	9 OK
<a href="#">Routers (Routers)</a>	12 UP	33 OK
<a href="#">Servers (Servers)</a>	25 UP	69 OK
<a href="#">Switches (Switches)</a>	17 UP	17 OK
<a href="#">Virtual Boxes (Virtual Boxes)</a>	8 UP	8 OK
<a href="#">rete OXE (rete OXE)</a>	7 UP	7 OK
<a href="#">rete autenticata (rete autenticata)</a>	5 UP	5 OK
<a href="#">retefonia CPU (retefonia CPU)</a>	12 UP	12 OK
<a href="#">retefonia Router (retefonia Router)</a>	9 UP	19 OK



# Qualche screenshot... (3)

## Current Network Status

Last Updated: Fri Mar 28 11:47:35 CET 2008  
 Updated every 90 seconds  
 Nagios® 3.0 - [www.nagios.org](http://www.nagios.org)  
 Logged in as *spinelli*

[View History For This Host](#)

[View Notifications For This Host](#)

[View Service Status Detail For All Hosts](#)

## Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

[All Problems](#) [All Types](#)

0	1
---	---


## Service Status Totals

Ok	Warning	Unknown	Critical	Pending
26	0	0	0	0

[All Problems](#) [All Types](#)

0	26
---	----

## Service Status Details For Host 'Jser'

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
Jser	 <a href="#">check CPU usage</a>	OK	03-28-2008 11:42:44	21d 18h 27m 39s	1/4	5 Minute Avg CPU Usage is 4%
	<a href="#">check bgp with CNR</a>	OK	03-28-2008 11:45:21	21d 22h 36m 48s	1/4	BGP to CNR is Up
	<a href="#">check bgp with Garr</a>	OK	03-28-2008 11:46:33	21d 22h 35m 16s	1/4	BGP to Garr is Up
	<a href="#">check bgp with Jadm</a>	OK	03-28-2008 11:42:45	21d 22h 36m 47s	1/4	BGP to Jadm is Up
	<a href="#">check bgp with Jfig</a>	OK	03-28-2008 11:45:22	21d 22h 35m 15s	1/4	BGP to Jfig is Up
	<a href="#">check bgp with Jjing</a>	OK	03-28-2008 11:46:34	0d 23h 40m 23s	1/4	BGP to Jjing is Up
	<a href="#">check bgp with Jmed</a>	OK	03-28-2008 11:42:45	21d 22h 35m 14s	1/4	BGP to Jmed is Up
	<a href="#">check bgp with Jpet</a>	OK	03-28-2008 11:45:23	21d 22h 36m 45s	1/4	BGP to Jpet is Up
	<a href="#">check bgp with Jpge</a>	OK	03-28-2008 11:46:34	21d 22h 35m 13s	1/4	BGP to Jpge is Up
	<a href="#">check bgp with Jpip</a>	OK	03-28-2008 11:42:46	21d 22h 36m 44s	1/4	BGP to Jpip is Up
	<a href="#">check bgp with Jsmr</a>	OK	03-28-2008 11:45:24	21d 22h 35m 12s	1/4	BGP to Jsmr is Up
	<a href="#">check bgp with Jspr</a>	OK	03-28-2008 11:46:35	21d 22h 36m 43s	1/4	BGP to Jspr is Up
	<a href="#">check bgp with Nodalis</a>	OK	03-28-2008 11:42:47	21d 22h 35m 11s	1/4	BGP to Nodalis is Up
	<a href="#">check bgp with RCU</a>	OK	03-28-2008 11:45:24	21d 22h 36m 42s	1/4	BGP to RCU is Up
	<a href="#">check bgp with Jfib</a>	OK	03-28-2008 11:46:36	21d 22h 35m 10s	1/4	BGP to Jfib is Up
	<a href="#">check isis with GARR</a>	OK	03-28-2008 11:42:48	17d 21h 54m 50s	1/4	Link to GARR is Up
	<a href="#">check isis with Jadm</a>	OK	03-28-2008 11:45:25	17d 21h 57m 13s	1/4	Link to Jadm is Up
	<a href="#">check isis with Jfib</a>	OK	03-28-2008 11:46:37	20d 18h 48m 30s	1/4	Link to Jfib is Up
	<a href="#">check isis with Jjing</a>	OK	03-28-2008 11:42:49	0d 23h 39m 6s	1/4	Link to Jjing is Up
	<a href="#">check isis with Jmed</a>	OK	03-28-2008 11:45:26	17d 21h 57m 12s	1/4	Link to Jmed is Up
	<a href="#">check isis with Jpet</a>	OK	03-28-2008 11:46:38	17d 20h 42m 44s	1/4	Link to Jpet is Up
	<a href="#">check isis with Jpge</a>	OK	03-28-2008 11:42:50	17d 21h 54m 48s	1/4	Link to Jpge is Up
	<a href="#">check isis with Jsmr</a>	OK	03-28-2008 11:45:27	17d 21h 57m 11s	1/4	Link to Jsmr is Up
	<a href="#">check isis with Jspr</a>	OK	03-28-2008 11:46:39	17d 21h 55m 59s	1/4	Link to Jspr is Up
	<a href="#">check ospf with rete20</a>	OK	03-28-2008 11:42:50	21d 0h 0m 56s	1/4	Link to rete20 is Up
	<a href="#">ping</a>	OK	03-28-2008 11:47:28	164d 19h 12m 5s	1/5	PING OK - Packet loss = 0%, RTA = 0.58 ms

Garr-X il futuro della rete

**Current Network Status**  
 Last Updated: Fri Mar 28 11:48:22 CET 2008  
 Updated every 90 seconds  
 Nagios® 3.0 - [www.nagios.org](http://www.nagios.org)  
 Logged in as *spinelli*

[View History For This Host](#)  
[View Notifications For This Host](#)  
[View Service Status Detail For All Hosts](#)

### Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	All Types
0	1

### Service Status Totals

Ok	Warning	Unknown	Critical	Pending
6	0	0	0	0

All Problems	All Types
0	6

### Service Status Details For Host 'nagios'

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
nagios	Current Load	OK	03-28-2008 11:45:52	105d 11h 35m 27s	1/4	OK - load average: 0.29, 0.23, 0.28
	Current Users	OK	03-28-2008 11:47:04	401d 6h 41m 27s	1/4	USERS OK - 3 users currently logged in
	PING	OK	03-28-2008 11:43:15	401d 6h 40m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.02 ms
	RAID status	OK	03-28-2008 11:45:53	133d 20h 43m 46s	1/4	LINUX_RAID OK - md0 : active raid1 sdb1[1] sda1[0] 11727296 blocks [2/2] [UU] :: md1 : active raid1 sdb2[1] sda2[0] 1959808 blocks [2/2] [UU] :: md2 : active raid1 sdb3[1] sda3[0] 29302464 blocks [2/2] [UU] :: md3 : active raid1 sdb4[1] sda4[0] 29615744 blocks [2/2] [UU]
	Root Partition	OK	03-28-2008 11:47:04	401d 6h 41m 27s	1/4	DISK OK - free space: / 9072 MB (79% inode=-):
	Total Processes	OK	03-28-2008 11:43:16	401d 6h 40m 9s	1/4	PROCS OK: 26 processes with STATE = RSZDT

6 Matching Service Entries Displayed

### Hostgroup Availability Report

Last Updated: Sat Mar 29 12:08:09 CET 2008  
 Nagios® 3.0 - [www.nagios.org](http://www.nagios.org)  
 Logged in as *spinelli*

### Hostgroup 'Routers'

01-01-2008 00:00:00 to 03-29-2008 12:08:09

Duration: 88d 12h 8m 9s

[ Availability report completed in 0 min 0 sec ]

First assumed host state: First assumed service state

Unspecified Unspecified

Report period: Backtracked archives:

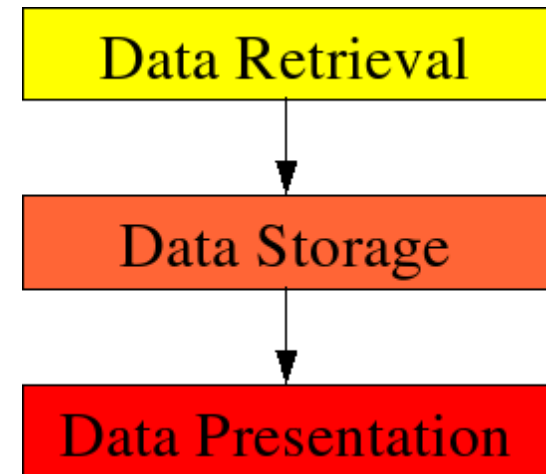
This Year 4

Update

### Hostgroup 'Routers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
<a href="#">Jadm</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Jfib</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Jfig</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Jing</a>	99.497% (99.497%)	0.503% (0.503%)	0.000% (0.000%)	0.000%
<a href="#">Jmed</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Jpet</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Jpge</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Jser</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Jsmr</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">Jspr</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">sdh-gw</a>	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
<a href="#">sumbra</a>	98.176% (98.176%)	1.824% (1.824%)	0.000% (0.000%)	0.000%
Average	99.806% (99.806%)	0.194% (0.194%)	0.000% (0.000%)	0.000%

- Usa SNMP o script per la collezione dei dati e rrdtool per lo storage e la presentazione
- Architettura modulare con templates, plugin ecc...
- Comunità vasta e attiva di sviluppatori
- Grafica ogni tipo di variabili



## **Dove reperire il codice :**

- **www.cacti.net : cacti, spine, alcuni template e scripts e documentazione**
- **http://forums.cacti.net : plugin, templates, supporto ecc...**

Si trovano i pacchetti per molte distribuzioni (debian ecc... )

Funziona anche su Windows

Ci sono un po' di operazioni da fare ma l'installazione è rapida e indolore:

- Si estrae l'archivio nella document-root del web server
- Set-up di my-sql (viene usato come backend)
- Set up del crontab per lanciare il poller

- Il traffico e gli errori per le interfacce degli apparati di rete
- Contatori di varia natura
- Temperature (dischi, CPU, ecc...)
- LoadAverage e spazio disco
- Occupazione RAM
- Tensioni, velocità ventole
- Qualsiasi variabile venga passata...

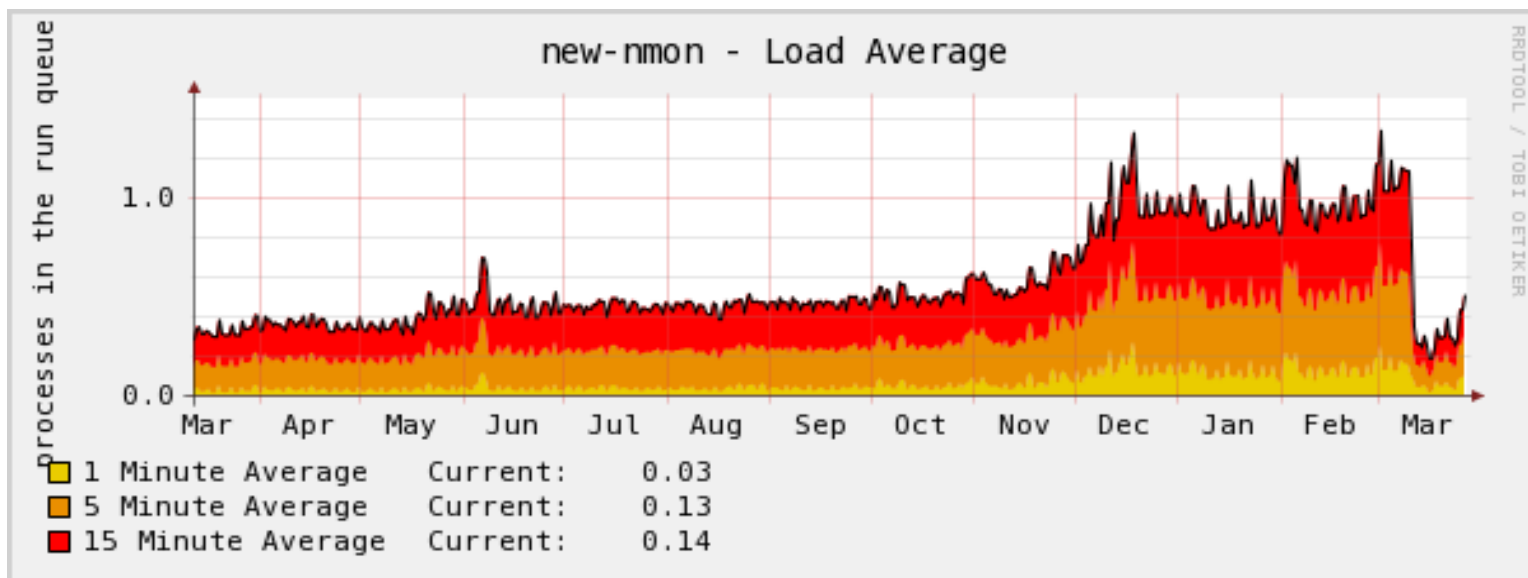


# Spine (Cactid)

Cacti viene fornito con un poller scritto in php che si occupa di lanciare gli scripts/query di raccolta dati.

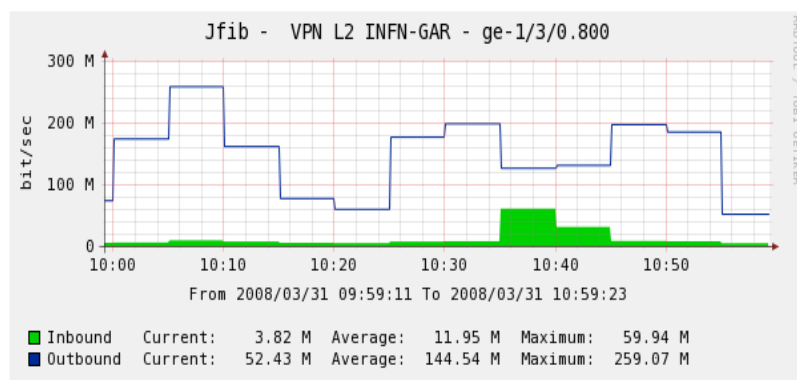
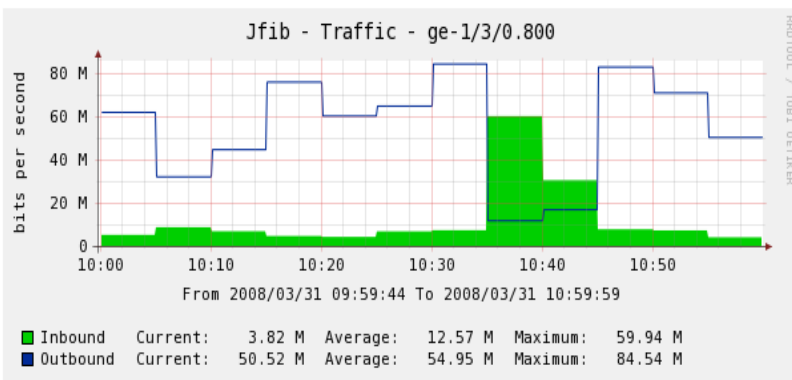
Non si tratta di una soluzione scalabile, e va sostituita con Spine appena inizia a crescere il numero di grafici.

Al momento monitoriamo 93 hosts con 844 grafici, ma il sistema puo' ancora crescere...



Per interfacce al gigabit occorre sempre usare counters a 64bit !


Un esempio di cio' che succede quando si usano counters sottodimensionati è visibile qui sotto:






- Con appositi templates e' possibile graficare moltissime variabili quali tensioni, temperature, velocità delle ventole, firewall counters, ecc...
- In particolare gli host template aiutano l'amministratore perchè caratterizzano l'host che si vuole monitorare
- In genere sono composti di script per la collezione dei dati da graph template per la presentazione
- Ce ne sono moltissimi e sono facili da modificare e adattare a specifiche esigenze

console
graphs
nagios
weathermap



Console -> Devices -> (Edit) Logged in as admin (Logout)

- Create
- New Graphs
- Management
- Graph Management
- Graph Trees
- Data Sources
- Devices**
- SuperLinks Pages
- Weathermaps
- Collection Methods
- Data Queries
- Data Input Methods
- Templates
- Graph Templates
- Host Templates
- Data Templates
- Import/Export
- Import Templates
- Export Templates
- Configuration
- Settings
- Utilities
- System Utilities
- User Management
- Logout User



Devices [new]

**Description**  
Give this host a meaningful description.

**Hostname**  
Fully qualified hostname or IP address for this device.

**Host Template**  
Choose what type of host, host template this is. The host template will govern what kinds of data should be gathered from this type of host.

**Notes**  
Enter notes to this host.

**Disable Host**  
Check this box to disable all checks for this host.

 Disable Host

Availability/Reachability Options

**Downed Device Detection**  
The method Cacti will use to determine if a host is available for polling.  
*NOTE: It is recommended that, at a minimum, SNMP always be selected.*

**Ping Method**  
The type of ping packet to sent.  
*NOTE: ICMP on Linux/UNIX requires root privileges.*

**Ping Port**  
TCP or UDP port to attempt connection.

**Ping Timeout Value**  
The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings.

**Ping Retry Count**  
The number of times Cacti will attempt to ping a host before failing.

SNMP Options

**SNMP Version**  
Choose the SNMP version for this device.

console
graphs
nagios
weathermap

Logged in as admin (Logout)

Console -> Create New Graphs

Create

**New Graphs**

Management

Graph Management

Graph Trees

Data Sources

Devices

SuperLinks Pages

Weathermaps

Collection Methods

Data Queries

Data Input Methods

Templates

Graph Templates

Host Templates

Data Templates

Import/Export

Import Templates

Export Templates

Configuration


Settings

Utilities

System Utilities

User Management

Logout User



## 2960\_Ingegneria (10.3.1.5)

Cisco Router

[\\*Edit this Host](#)

[\\*Create New Host](#)

Host:  Graph Types:

**Graph Templates**

Graph Template Name

Create: Cisco - CPU Usage

Create:

**Data Query [SNMP - Interface Statistics]**

<< Previous Showing Rows 1 to 20 of 26 [1,2] Next >>

Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	Hardware Address	IP Address	
1	Up	Vlan1	Vl1		propVirtual	1000000000	00:19:06:09:F0:40	10.3.1.5	☐
10101	Up	GigabitEthernet0/1	Gi0/1	Trunk con Aggregazione1 Rettorato	ethernetCsmacd	1000000000	00:19:06:09:F0:01		☐
10102	Up	GigabitEthernet0/2	Gi0/2	Presidenza	ethernetCsmacd	1000000000	00:19:06:09:F0:02		☐
10103	Up	GigabitEthernet0/3	Gi0/3	Ing. Aereospaziale	ethernetCsmacd	1000000000	00:19:06:09:F0:03		☐
10104	Up	GigabitEthernet0/4	Gi0/4	Ing. Telecomunicazioni	ethernetCsmacd	1000000000	00:19:06:09:F0:04		☐
10105	Up	GigabitEthernet0/5	Gi0/5	Ing. Idraulica	ethernetCsmacd	1000000000	00:19:06:09:F0:05		☐
10106	Up	GigabitEthernet0/6	Gi0/6	Centro di Calcolo Biennio	ethernetCsmacd	1000000000	00:19:06:09:F0:06		☐
10107	Up	GigabitEthernet0/7	Gi0/7	Centro Piaggio	ethernetCsmacd	1000000000	00:19:06:09:F0:07		☐
10108	Up	GigabitEthernet0/8	Gi0/8	Sistemi Elettrici	ethernetCsmacd	1000000000	00:19:06:09:F0:08		☐
10109	Up	GigabitEthernet0/9	Gi0/9	Ing. Meccanica Nucleare	ethernetCsmacd	1000000000	00:19:06:09:F0:09		☐
10110	Down	GigabitEthernet0/10	Gi0/10	Biblioteca di Ingegneria	ethernetCsmacd	1000000000	00:19:06:09:F0:0A		☐
10111	Up	GigabitEthernet0/11	Gi0/11	Ing. Chimica	ethernetCsmacd	1000000000	00:19:06:09:F0:0B		☐
10112	Up	GigabitEthernet0/12	Gi0/12	Energetica	ethernetCsmacd	1000000000	00:19:06:09:F0:0C		☐
10113	Up	GigabitEthernet0/13	Gi0/13	Ing. Strutturale	ethernetCsmacd	1000000000	00:19:06:09:F0:0D		☐
10114	Down	GigabitEthernet0/14	Gi0/14		ethernetCsmacd	1000000000	00:19:06:09:F0:0E		☐
10115	Down	GigabitEthernet0/15	Gi0/15		ethernetCsmacd	1000000000	00:19:06:09:F0:0F		☐

Ci siamo posti il problema di come graficare il traffico delle reti virtualizzate...

Abbiamo seguito 3 approcci differenti a seconda dei casi:

- se l'apparato è raggiungibile in altri modi (OOB) si sfrutta quel collegamento e si fanno le query direttamente all'apparato
- se l'apparato è raggiungibile solo attraverso la VPN e supporta snmp si fanno le query attraverso la VPN stessa

- se l'apparato è raggiungibile solo attraverso la VPN e non supporta snmp si usano dei contatori per il traffico di interesse sull'interfaccia di raccolta .

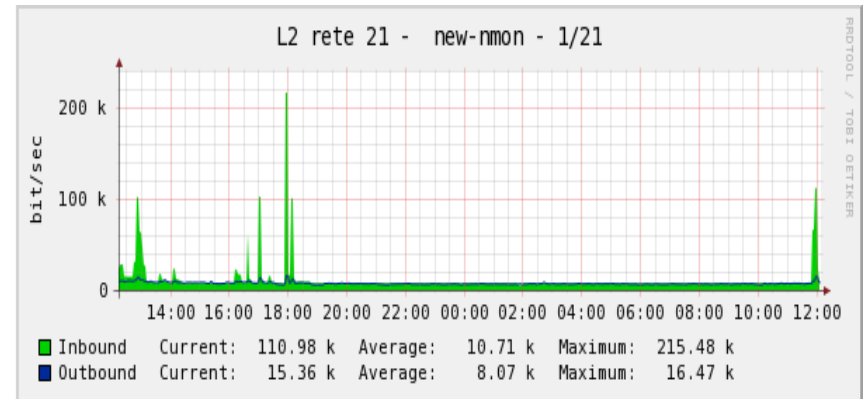
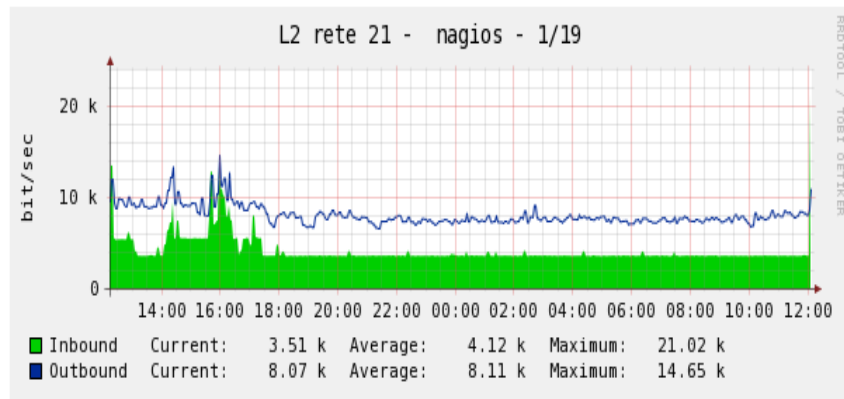
E' utile anche in situazioni in cui si vogliono distinguere traffici diversi dei quali si conosce l'origine o la destinazione .

Questo è bene per conoscere ad esempio il comportamento della rete in condizioni di QoS

# L'impatto sulla rete:

Per essere attendibile uno strumento di misura non deve influenzare il dato della misura stessa.

Per la rete l'impatto di questi due servizi e' veramente minimo:



Aggiunge a Cacti delle nuove funzionalità,  
permette maggiore integrazione con altri  
software.

<http://cactiusers.org/wiki/PluginArchitectureInstall>

Questo permette di usare Cacti come unico  
centro di accesso al sistema di monitoring

- **PHP Weathermap:**

Crea una weathermap a partire dal database di cacti

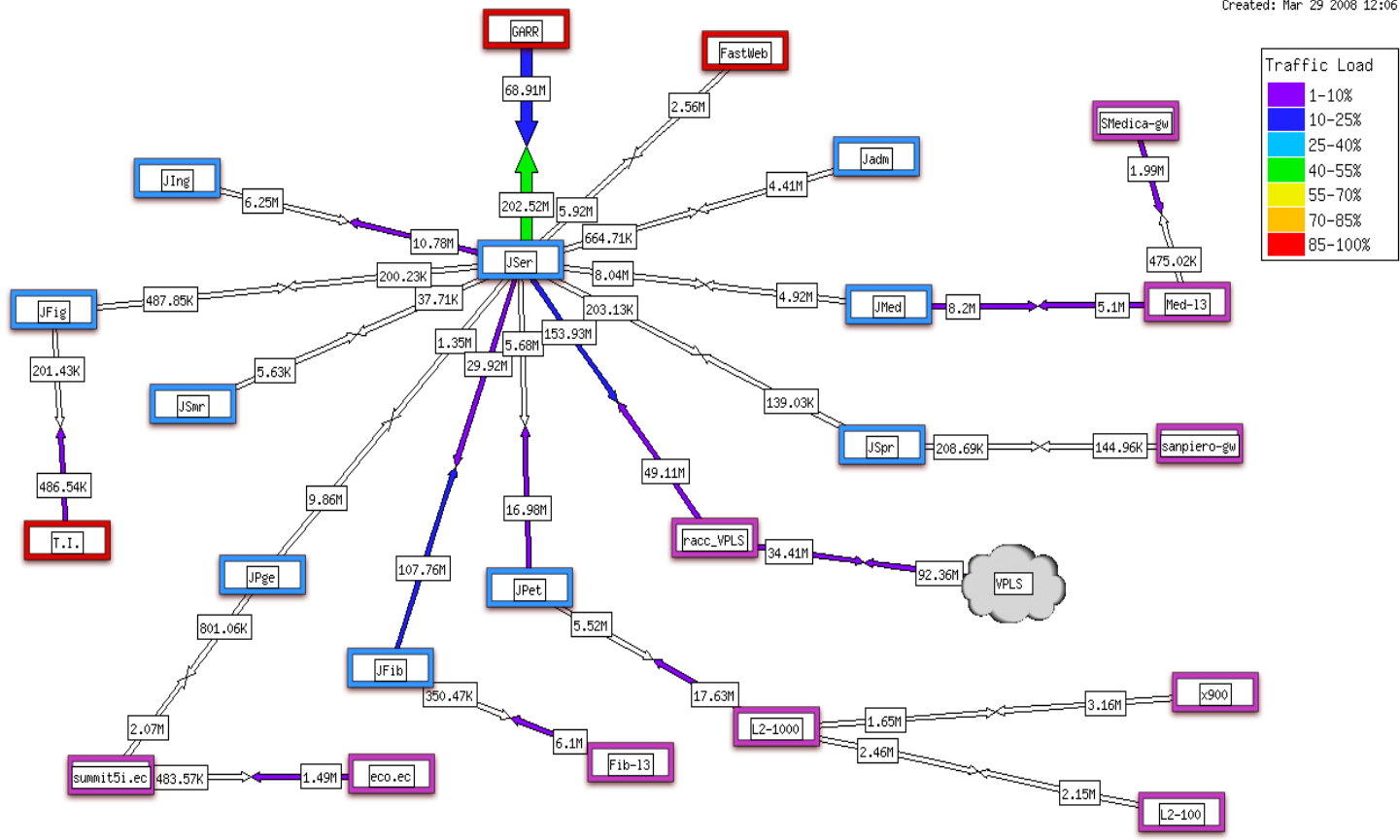
- **Ntop:**

Integra Ntop nell'interfaccia web di cacti

- **SuperLinks:**

Permette di creare tabs con link esterni così da integrare altri servizi ( ad esempio Nagios )

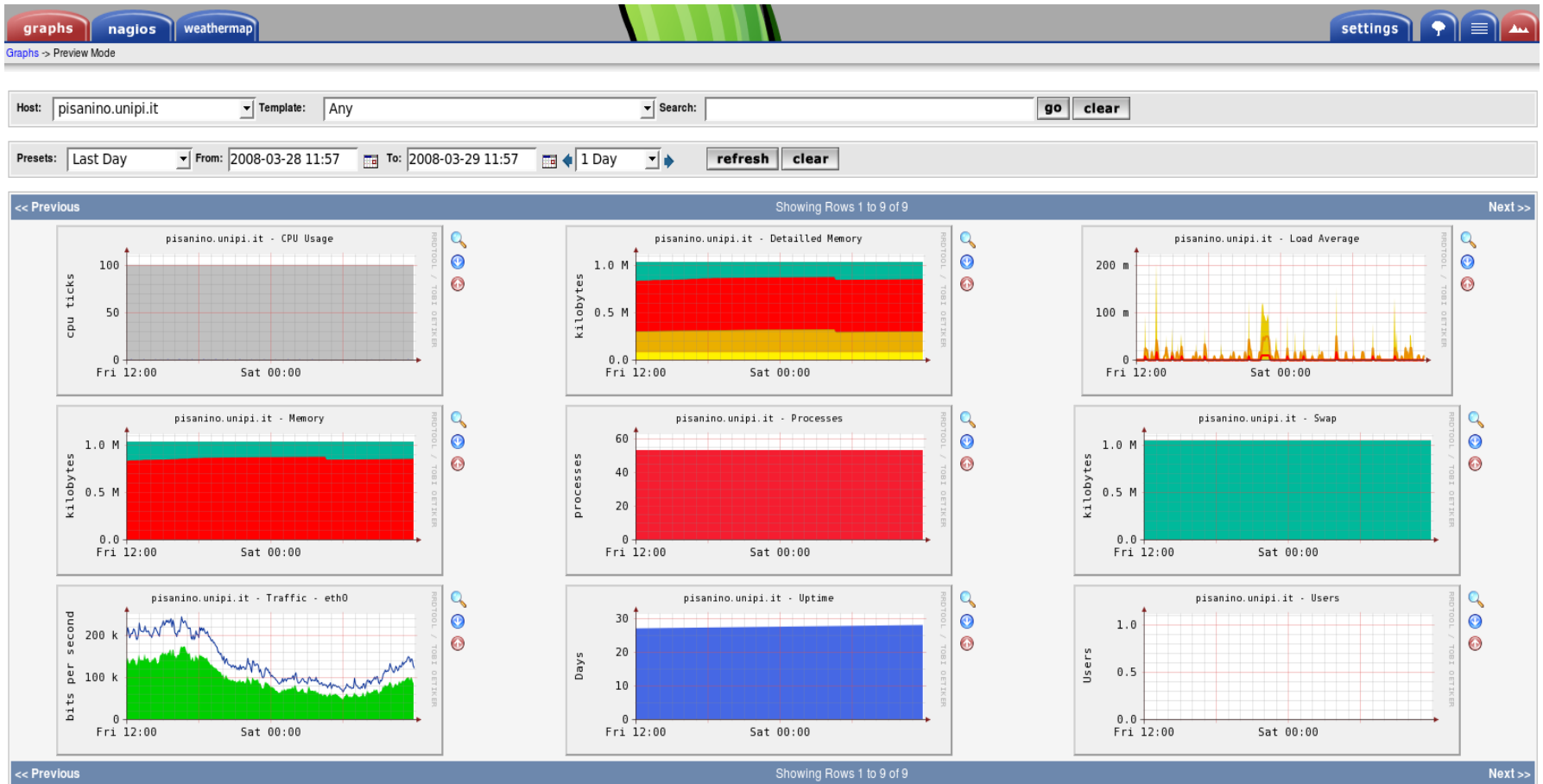




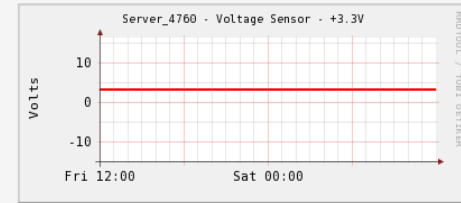
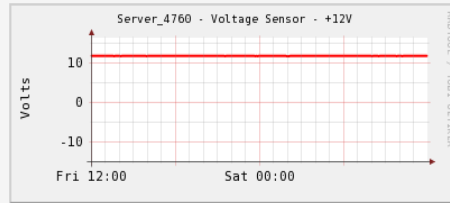
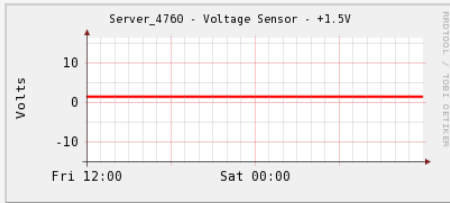
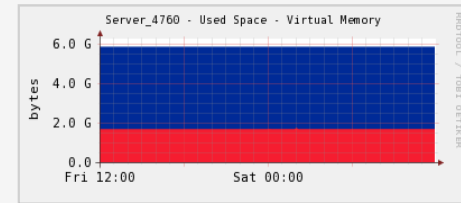
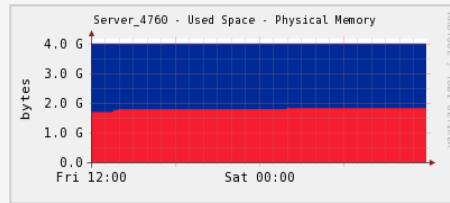
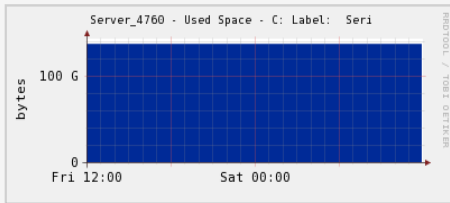
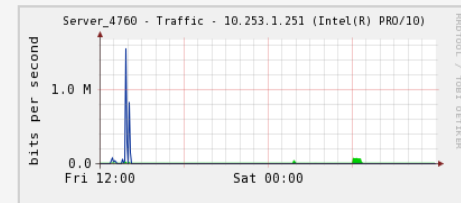
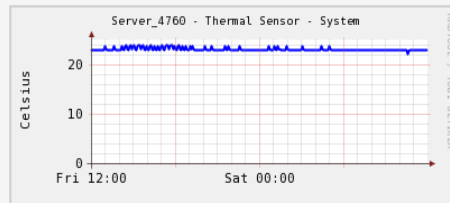
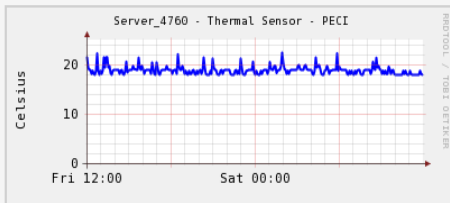
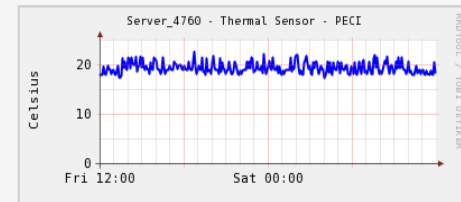
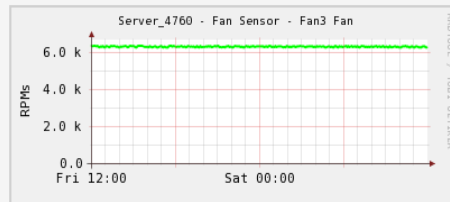
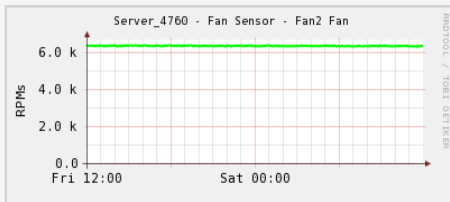
Garr-X il futuro della rete



Garr-X il futuro della rete



# Screenshots (3)



<http://www.ntop.org/>

Ci siamo orientati verso la soluzione nBox: si tratta di una appliance preinstallata configurabile via web e ottimizzata per alti carichi di traffico .

Al momento ne abbiamo in campo una che analizza il traffico della rete autenticata degli studenti.

Come già detto, ci permetterà di affinare le nostre politiche di firewalling/QoS e di capire meglio come vengono utilizzate le risorse.

Welcome to nBox



- Configuration
  - General
  - Users
  - nTop
  - nProbe
  - SQL Database
  - IPMI
  - High-Avail.
  - Firewall
  - License
- Administration
  - Shell
  - Logout
  - Reboot
  - Shutdown
  - Services
  - Update
  - Configuration
- Diagnostics
  - IPerf
  - Network
  - Interfaces
  - Memory
  - Live Graphs
  - Information
  - Status

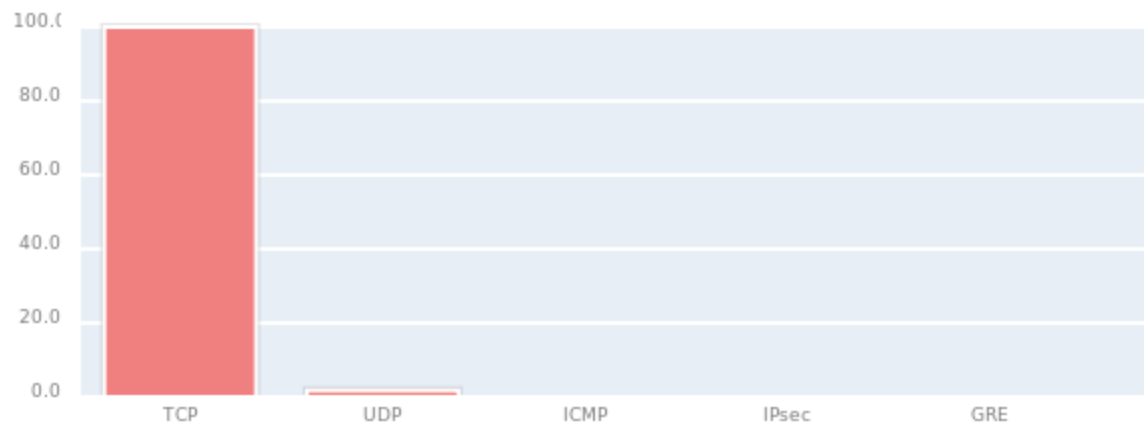
## General Configuration

General	
Host Name:	<input type="text" value="auth-nbox"/>
Timezone:	<input type="text" value="Europe/Rome"/>
NTP Server:	<input type="text" value="time.iien.it 0.debian.pool.ntp.org"/> <small>List of servers for remote time synchronization. Leave this field empty for no time synchronization. Time is synchronized at boot, every day, or whenever you <a href="#">restart</a> the ntpdate service.</small>
SSH Access:	<input type="radio"/> Inactive <input checked="" type="radio"/> Active <small>Enable/disable remote SSH access to your nBox. In any case your nBox will still be accessible via http/https.</small>
Telnet/FTP Access:	<input type="radio"/> Inactive <input checked="" type="radio"/> Active <small>Enable/disable remote telnet and FTP access to your nBox. Use these protocols as the last resort instead of SSH as they are not encrypted.</small> <b>NOTE:</b> for security reasons the root user cannot ftp/telnet to a remote box. Use a different <a href="#">user</a> instead.
PF_RING Acceleration:	<input type="radio"/> Inactive <input checked="" type="radio"/> Active <input type="text" value="128"/> <small>Enable/disable PF_RING packet capture acceleration. The "Bucket length" specifies the maximum packet length captured by PF_RING.</small> <b>NOTE:</b> please <a href="#">reboot</a> your nBox whenever you change this setting.
Primary (Management) Network Interface (eth0)	
IP Address:	Address: <input type="text" value="131.114.21.124"/> Netmask: <input type="text" value="255.255.255.0"/>
Default Gateway:	Address: <input type="text" value="131.114.21.8"/>
DHCP Client:	<input type="radio"/> Inactive <input checked="" type="radio"/> Active <small>If you enable DHCP support the above address fields are not used.</small>
IP Forwarding:	<input type="radio"/> Inactive <input checked="" type="radio"/> Active <small>Enable this facility if you want to use your nBox as a network router.</small>
Bridging (eth0 and eth1):	<input type="radio"/> Inactive <input checked="" type="radio"/> Active <small>Enable this facility for using your nBox in pass-through mode.</small> <b>NOTE:</b> using bridging you might reduce the nBox performance.
Further Interface Addresses	
Interface Address (eth1):	Address: <input type="text"/> Netmask: <input type="text"/> <small>Note: leave fields blank if you don't want to set an IP address.</small>
Interface Alias (eth0:1):	Address: <input type="text"/> <small>This field allows you to specify a secondary IP address on the management interface.</small>
DNS Service	

© 2002-07 nmon.net

## Global Protocol Distribution

Protocol	Data		Percentage			
<b>IP</b>	90.7 TBytes	100.0%	<b>TCP</b>	89.0 TBytes	98.2%	
			<b>UDP</b>	1.6 TBytes	1.8%	
			<b>ICMP</b>	18.5 GBytes	0%	
<b>IPsec</b>	252.8 MBytes	0%				
<b>GRE</b>	91.9 MBytes	0%				



console
graphs
Auth-nBox
nagios
weathermap

settings
🔍
☰
🏠

Auth-nBox
Logged in as admin (Logout)

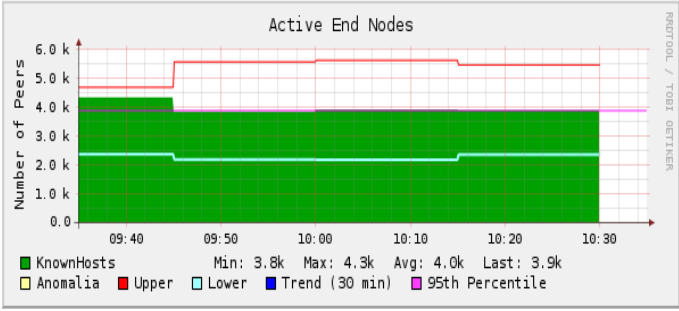
## ntop

About Summary All Protocols IP Utils Plugins Admin

(C) 1998-2008 - Luca Deri

### RRD Graph

Presets: ----- From:  To:  Update Graph



Report created on Mon Mar 31 10:35:07 2008 [ntop uptime: 61 days 0:03:24]  
 Generated by ntop v.3.3.5 [i686-pc-linux-gnu]  
 © 1998-2008 by Luca Deri, built: Jan 13 2008 19:35:36.  
 Listening on [eth0,NetFlow-device.2] for all packets (i.e. without a filtering expression)  
 Web reports include only interface "NetFlow-device.2"



Ci sono ancora altre questioni che vogliamo affrontare :

- Supporto alle SNMP Trap (Nagios) per la gestione degli incidenti sia sulla rete dati che sulla rete di fonia
- Grafici delle risorse delle centrali telefoniche
- Integrazione con il syslog centralizzato e Splunk
- Notifiche via SMS
- Integrazione fra i due sistemi
- Alta affidabilità/clustering delle piattaforme di monitoring
- Terminare l'installazione degli nBox su tutti i nodi di backbone

# Grazie per l'attenzione...