Strumenti di monitoring per la MAN universitaria pisana

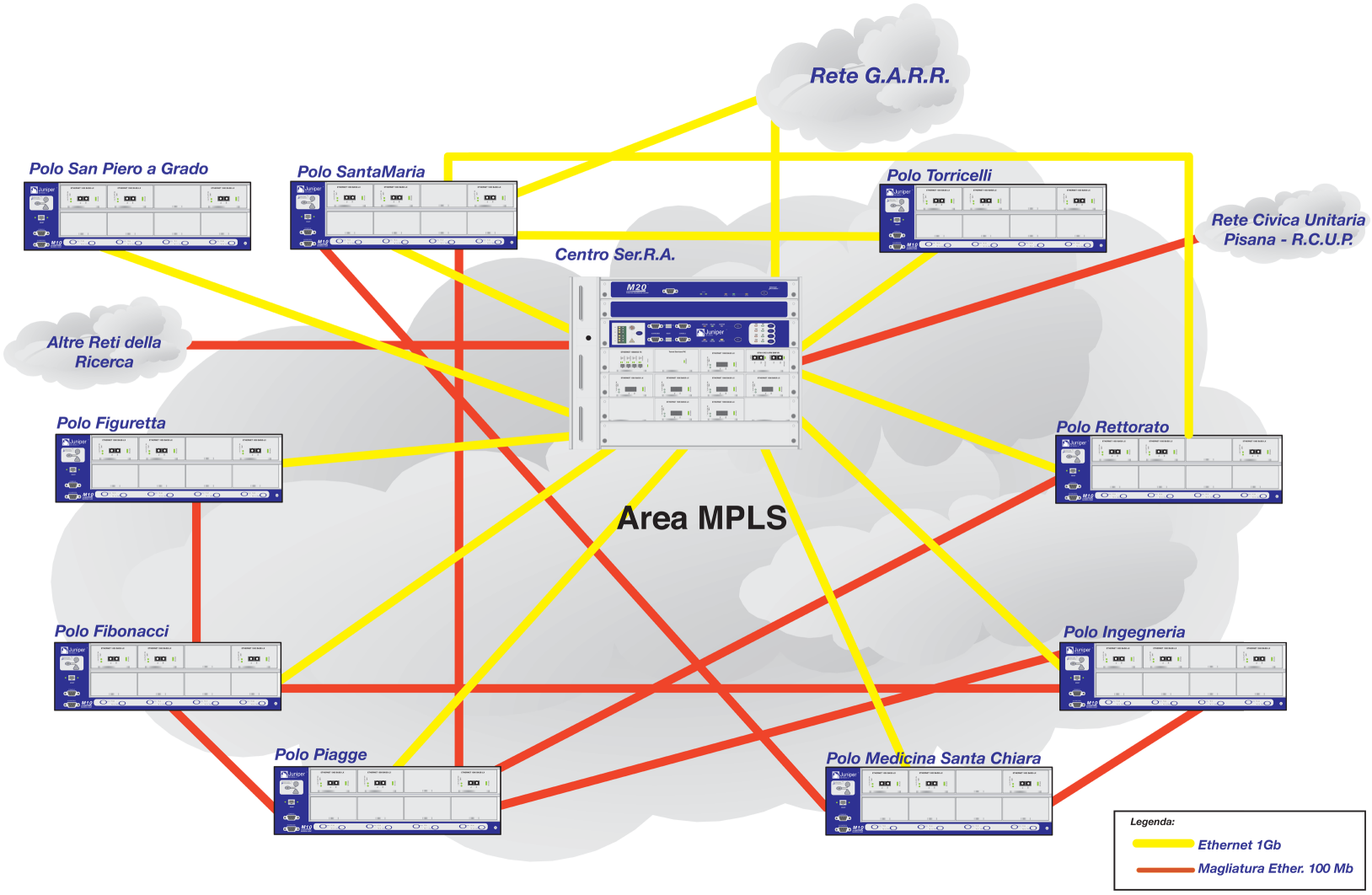
simone.spinelli@unipi.it

Garr-X il futuro della rete

Alcuni numeri...

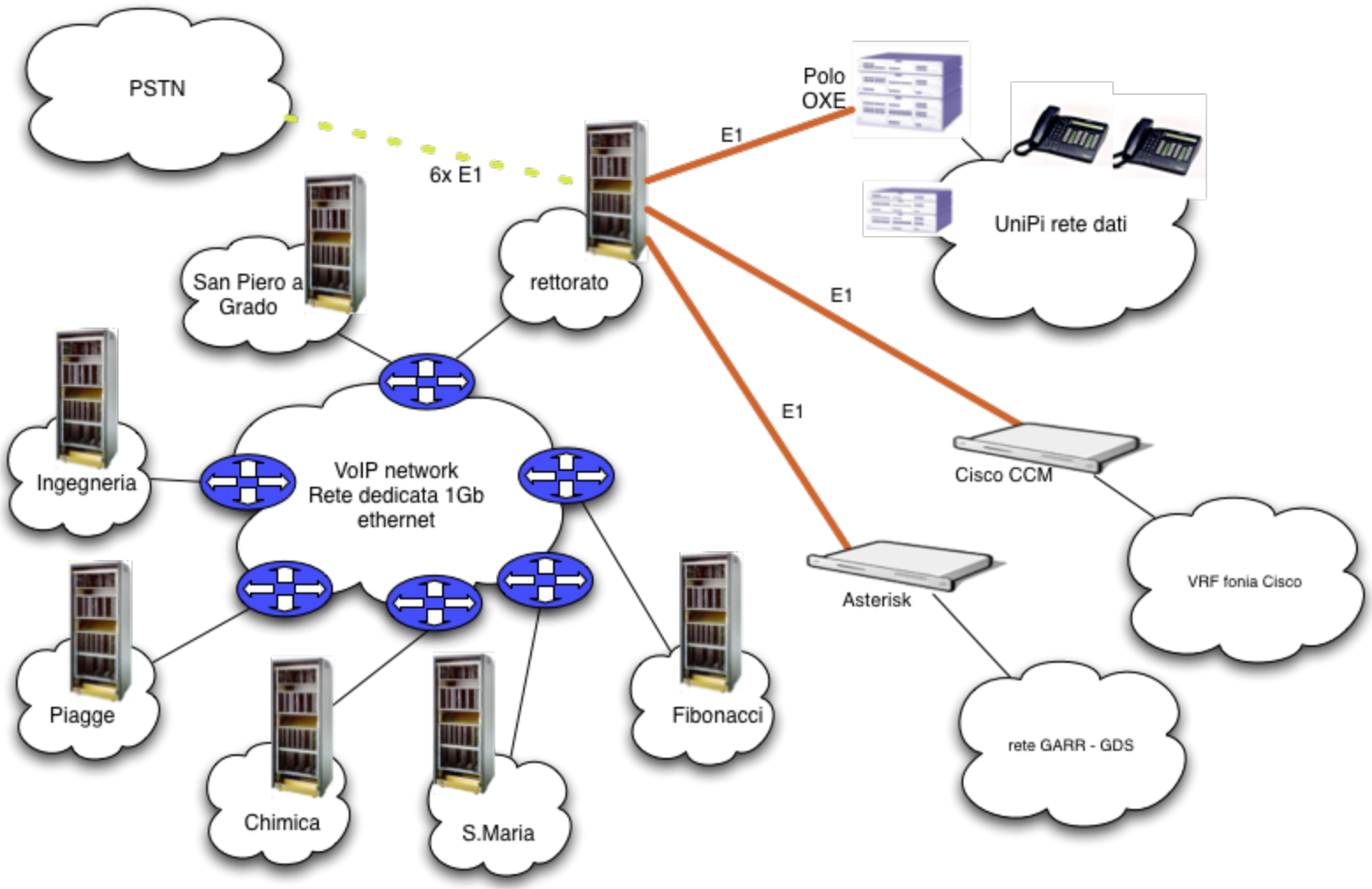
- Una rete Campus/MAN di proprietà basata su una infrastruttura in F.O. con circa 50Km. di canalizzazioni
- Circa 200 siti diversi raggiunti ciascuno con 8 diverse fibre per i seguenti servizi:
  - Dati
  - Voce
  - Amministrazione
  - Usi diversi
- Circa 80 Km. di cavi in F.O. stesi sul territorio
- 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

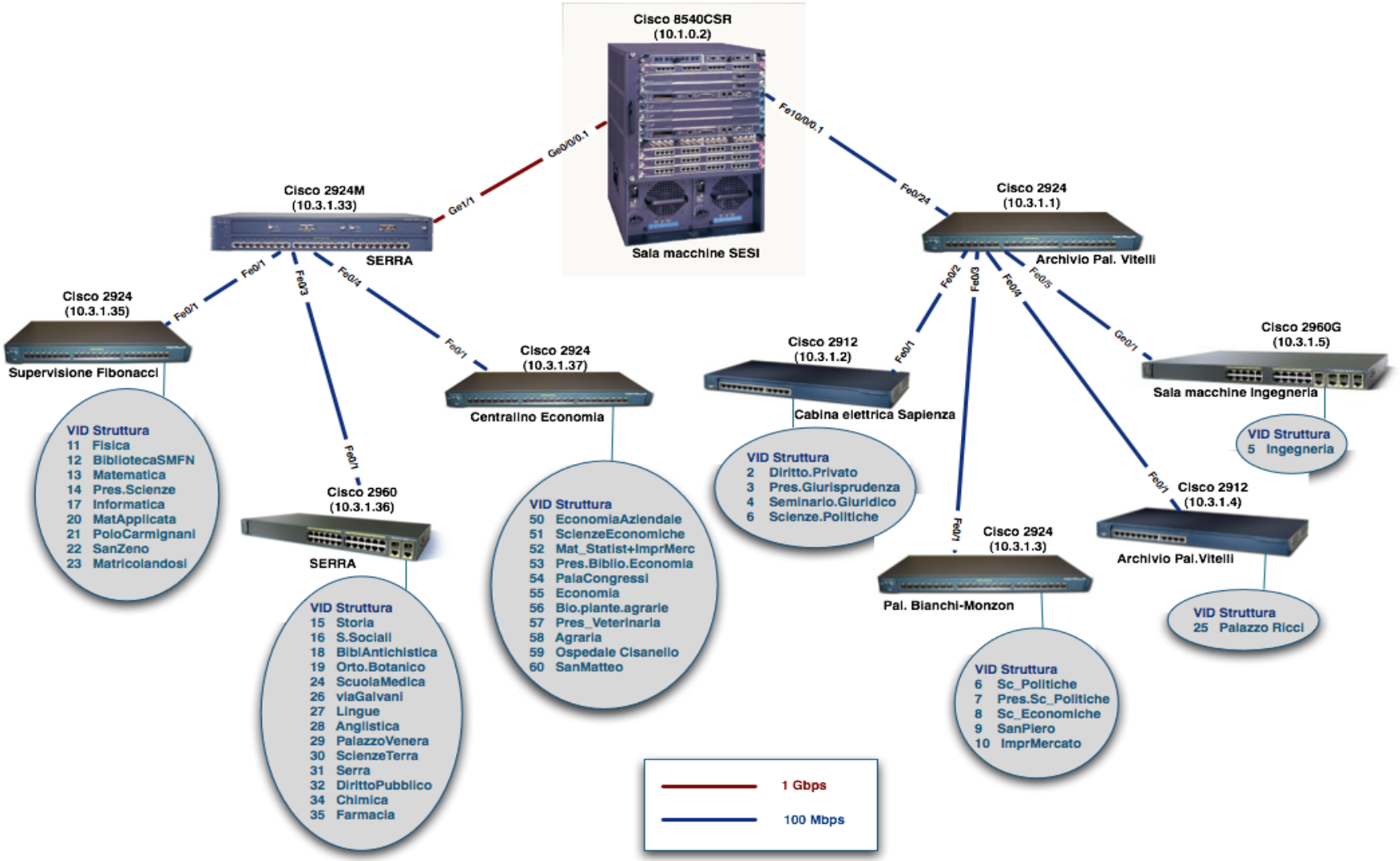


Garr-X il futuro della rete

La rete UniPi: la fonia



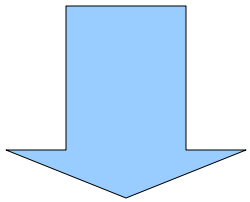
La rete amministrativa



Garr-X il futuro della rete

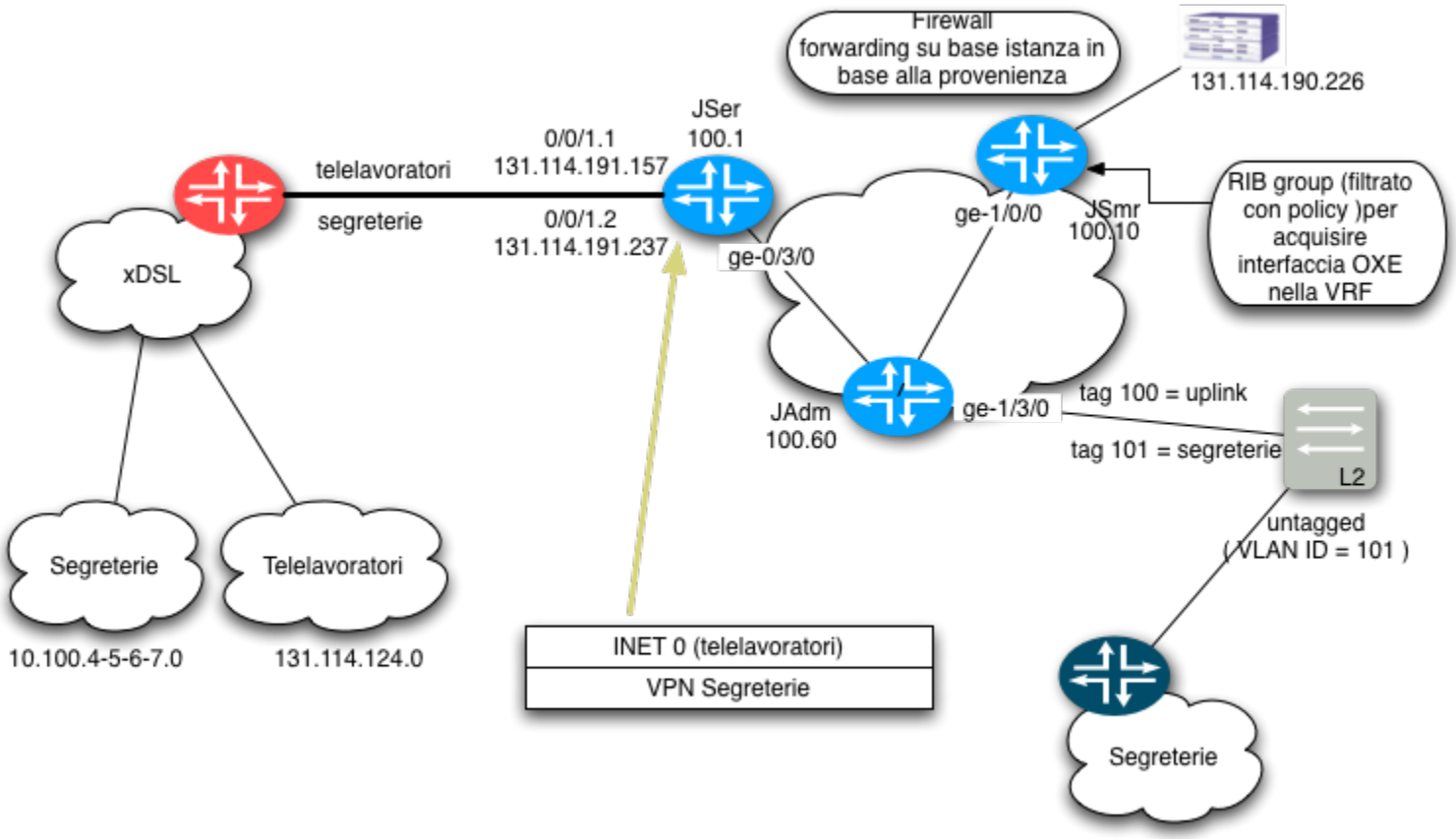
Una rete di comunità

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



I nostri obiettivi:

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 .

Le caratteristiche

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)

Le caratteristiche:

Abbiamo diviso il problema in tre fronti

Allarmistica :

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

Analisi del traffico:

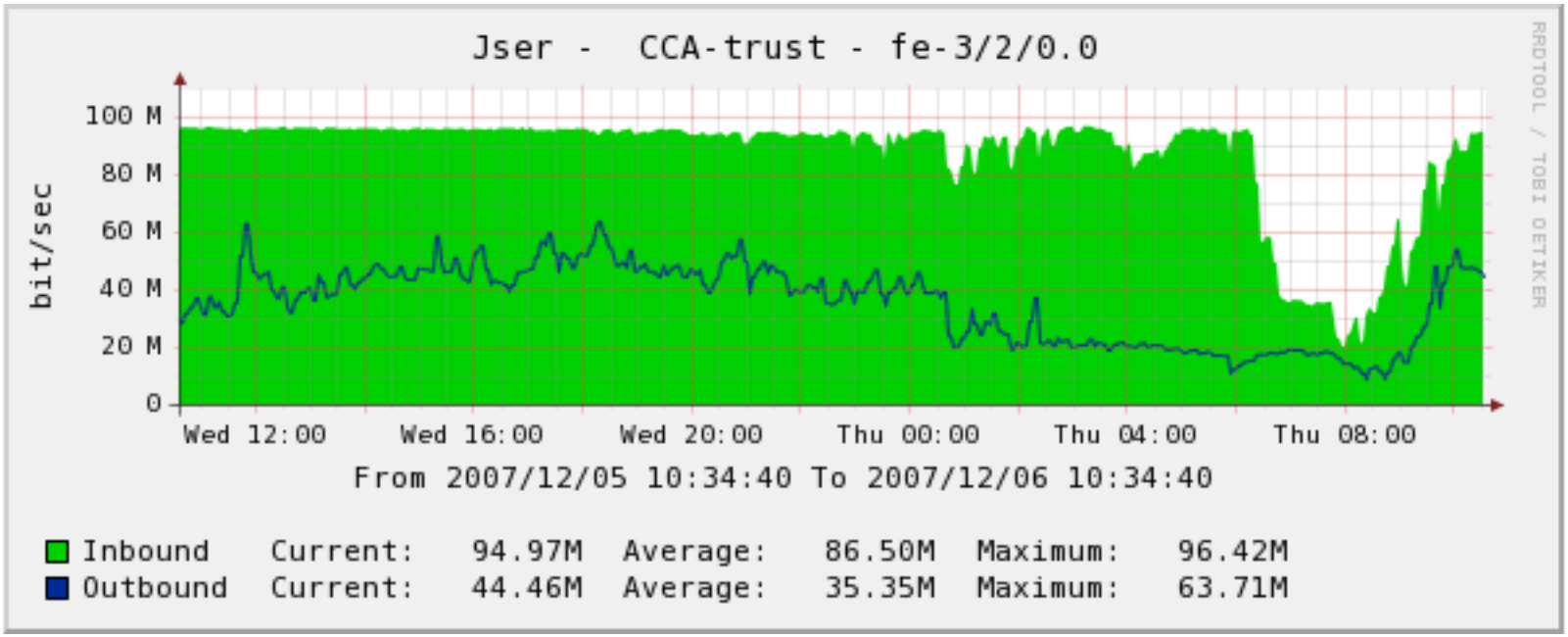
Permette di capire che traffico attraversa la nostra rete, se alcune categorie di traffico sono penalizzate rispetto ad altre, aiuta nella individuazione delle politiche di filtering e QoS . (ancora in fase di sviluppo)

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 situazione :

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 :

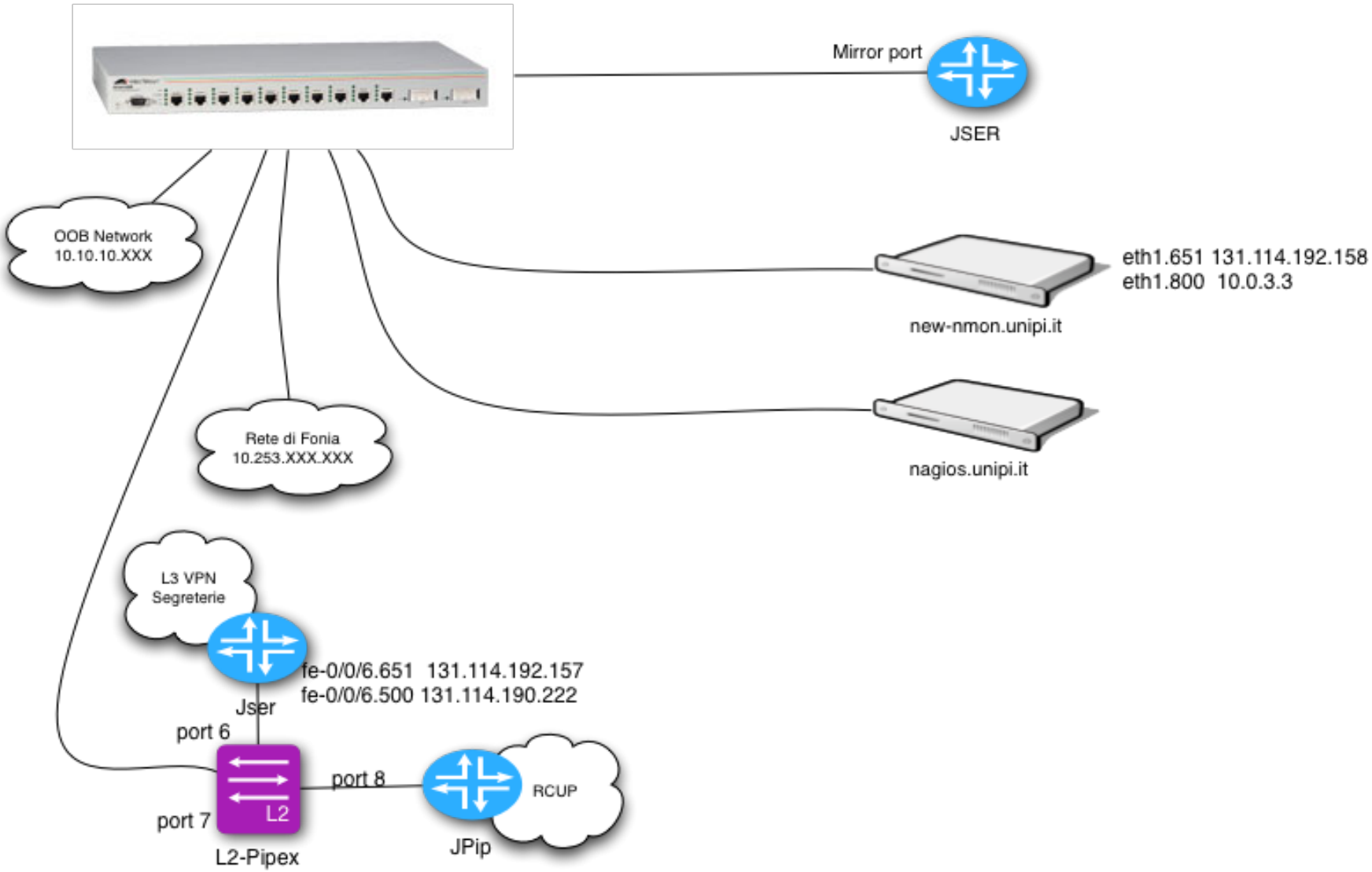
"Nagios Ain't Gonna Insist On Sainthood"

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

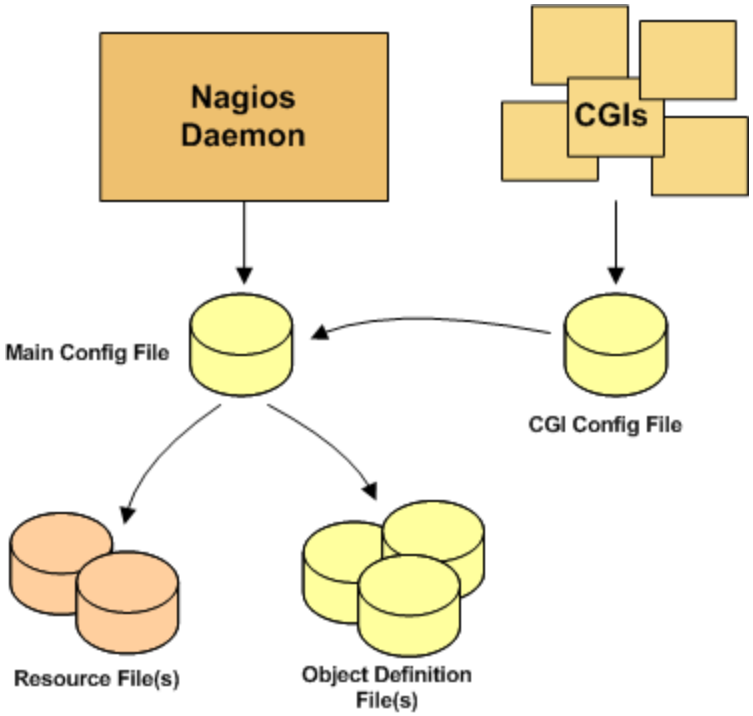
Per l'analisi del traffico di rete ci siamo orientati verso Ntop:

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

L'Hardware e la sua topologia



Nagios: architettura



- 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)

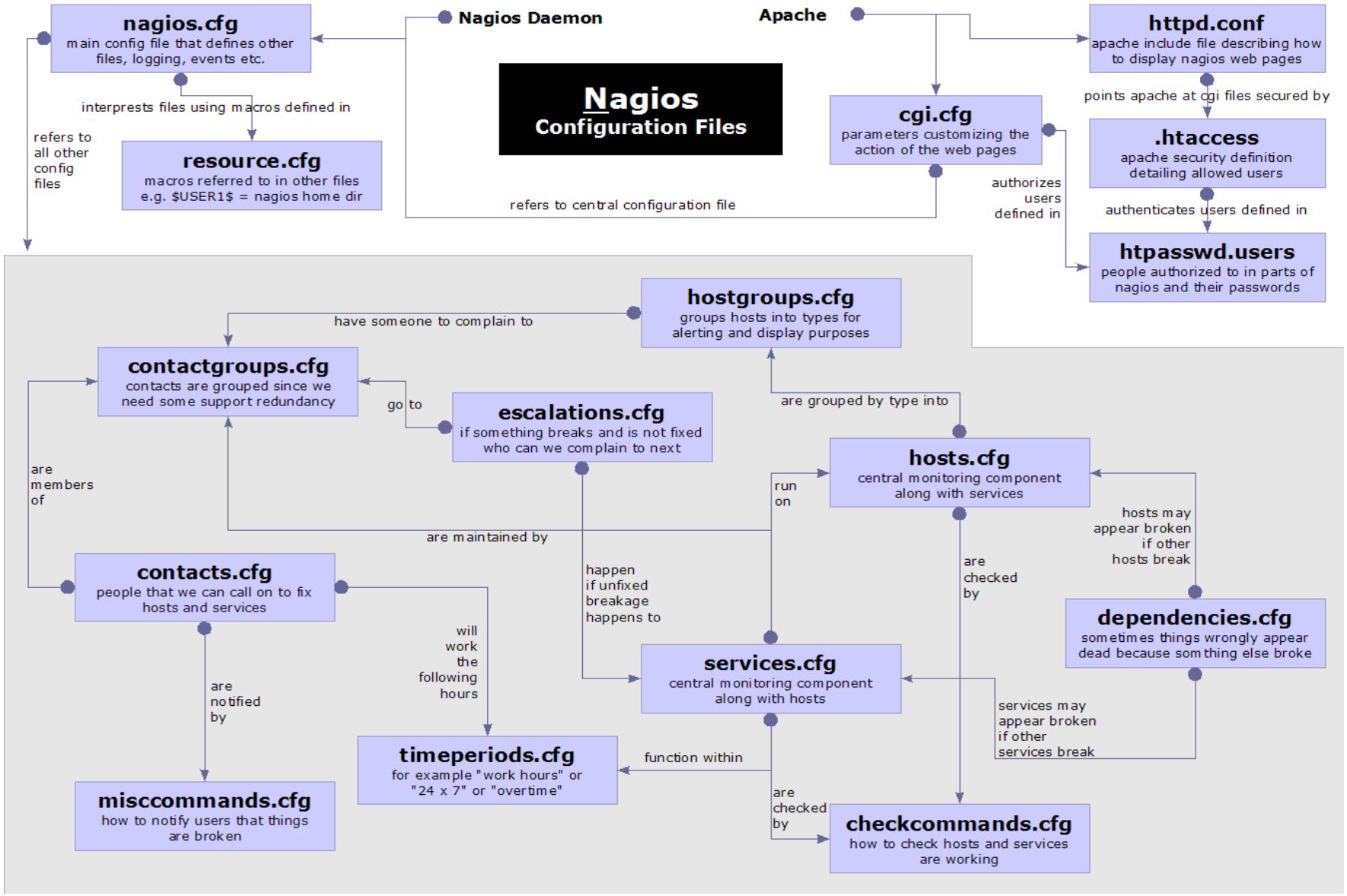
Nagios : Installazione

Dove reperire il codice:

- **www.nagios.org : nagios daemon, nrpe, plugin standard**
- **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



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:

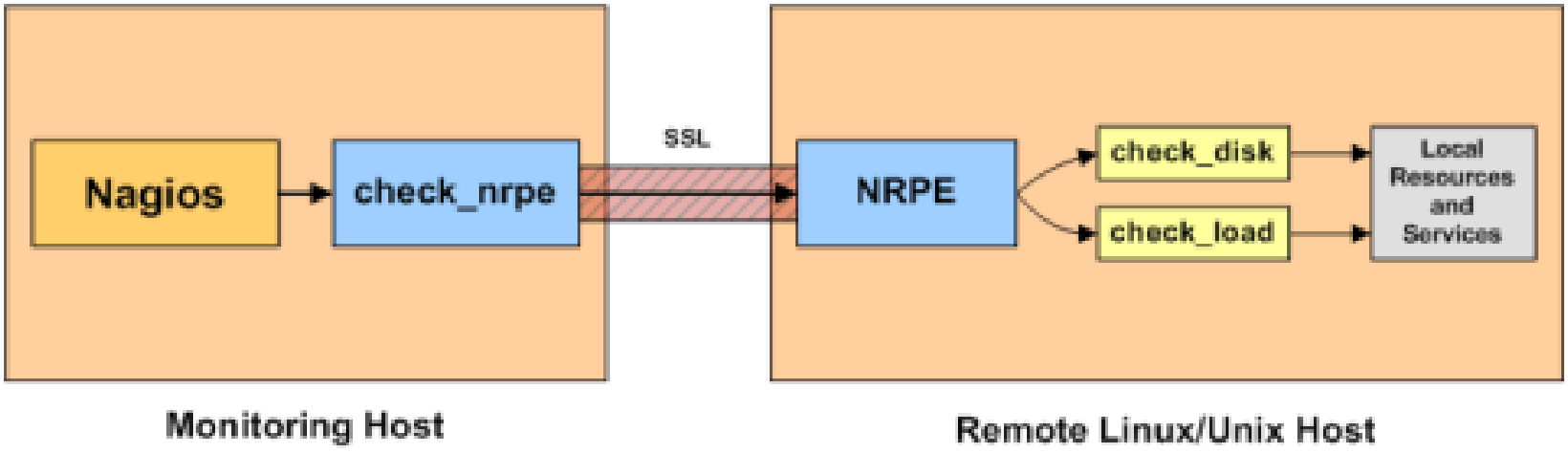
```
# Generic host definition template
define host{
 name                            generic-host
 notifications_enabled           1
 event_handler_enabled           1
 flap_detection_enabled          1
 process_perf_data               1
 retain_status_information       1
 retain_nonstatus_information    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
}
```

NRPE Nagios Remote Plugin Executor

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
        }
```

Come va...

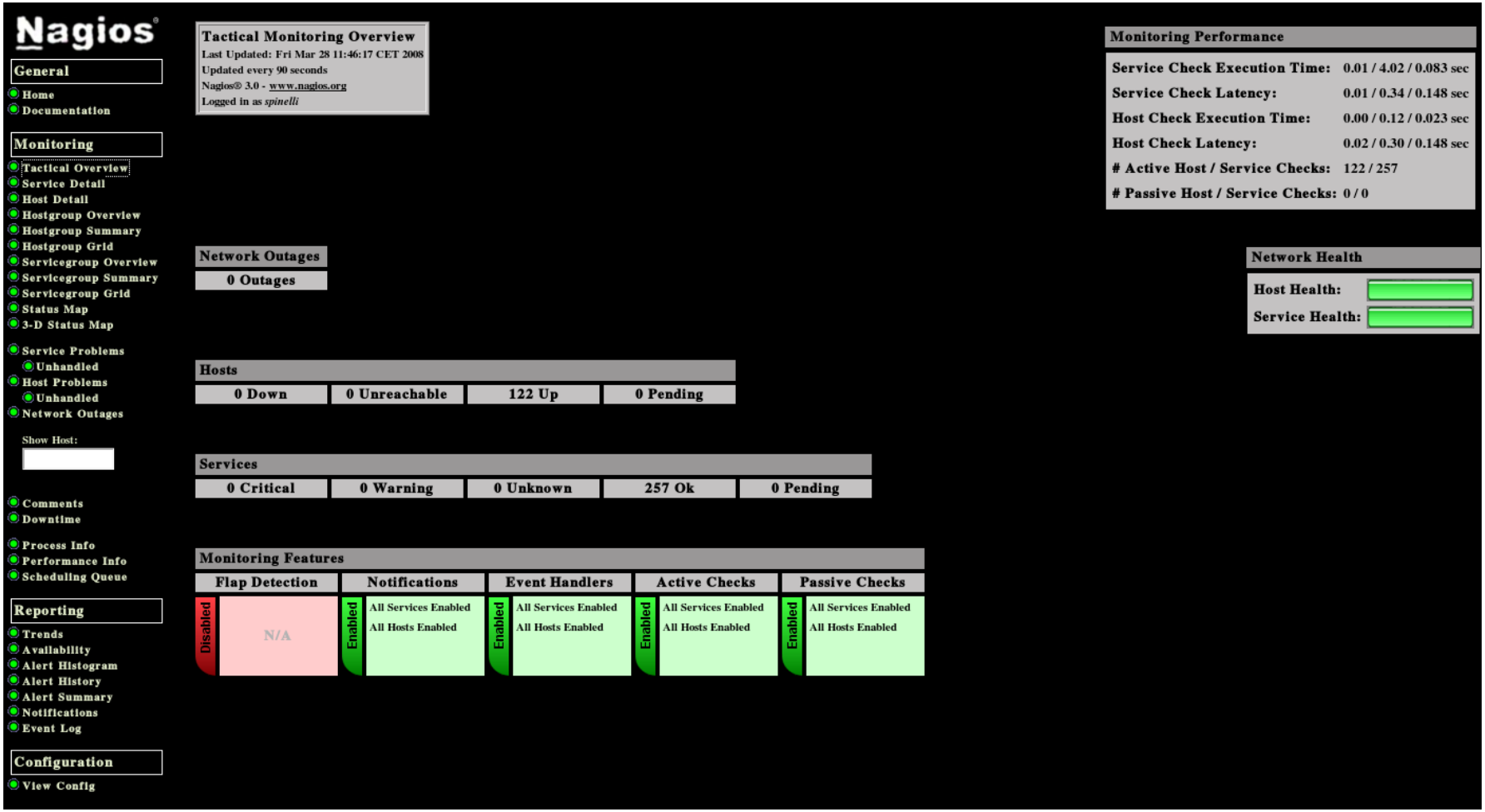
A nagios abbiamo affidato tutta l'allarmistica:

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

Che cosa fa per noi

- 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..)

Qualche screenshot... (1)



Qualche screenshot... (2)

Current Network Status
Last Updated: Fri Mar 28 11:46:50 CET 2008
Updated every 90 seconds
Nagios® 3.0 - 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
Amministrazione_Net (Amministrazione_Net)	10 UP	20 OK
Cisco_CCM (Cisco_CCM)	3 UP	3 OK
PtP_Fonia (PtP_Fonia)	5 UP	5 OK
Rete_OOB (Rete_OOB)	9 UP	9 OK
Routers (Routers)	12 UP	83 OK
Servers (Servers)	25 UP	69 OK
Switches (Switches)	17 UP	17 OK
Virtual_Boxes (Virtual_Boxes)	8 UP	8 OK
rete_OXE (rete_OXE)	7 UP	7 OK
rete_autenticata (rete_autenticata)	5 UP	5 OK
retefonia_CPU (retefonia_CPU)	12 UP	12 OK
retefonia_Router (retefonia_Router)	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
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	check_CPU_usage	OK	03-28-2008 11:42:44	21d 18h 27m 39s	1/4	5 Minute Avg CPU Usage is 4%
	check_bgp_with_CNR	OK	03-28-2008 11:45:21	21d 22h 36m 48s	1/4	BGP to CNR is Up
	check_bgp_with_Garr	OK	03-28-2008 11:46:33	21d 22h 35m 16s	1/4	BGP to Garr is Up
	check_bgp_with_Jadm	OK	03-28-2008 11:42:45	21d 22h 36m 47s	1/4	BGP to Jadm is Up
	check_bgp_with_Jfig	OK	03-28-2008 11:45:22	21d 22h 35m 15s	1/4	BGP to Jfig is Up
	check_bgp_with_Jing	OK	03-28-2008 11:46:34	0d 23h 40m 23s	1/4	BGP to Jing is Up
	check_bgp_with_Jmed	OK	03-28-2008 11:42:45	21d 22h 35m 14s	1/4	BGP to Jmed is Up
	check_bgp_with_Jpet	OK	03-28-2008 11:45:23	21d 22h 36m 45s	1/4	BGP to Jpet is Up
	check_bgp_with_Jpge	OK	03-28-2008 11:46:34	21d 22h 35m 13s	1/4	BGP to Jpge is Up
	check_bgp_with_Jpip	OK	03-28-2008 11:42:46	21d 22h 36m 44s	1/4	BGP to Jpip is Up
	check_bgp_with_Jsmr	OK	03-28-2008 11:45:24	21d 22h 35m 12s	1/4	BGP to Jsmr is Up
	check_bgp_with_Jspr	OK	03-28-2008 11:46:35	21d 22h 36m 43s	1/4	BGP to Jspr is Up
	check_bgp_with_Nodalis	OK	03-28-2008 11:42:47	21d 22h 35m 11s	1/4	BGP to Nodalis is Up
	check_bgp_with_RCU	OK	03-28-2008 11:45:24	21d 22h 36m 42s	1/4	BGP to RCU is Up
	check_bgp_with_jfib	OK	03-28-2008 11:46:36	21d 22h 35m 10s	1/4	BGP to JFib is Up
	check_isis_with_GARR	OK	03-28-2008 11:42:48	17d 21h 54m 50s	1/4	Link to GARR is Up
	check_isis_with_Jadm	OK	03-28-2008 11:45:25	17d 21h 57m 13s	1/4	Link to Jadm is Up
	check_isis_with_Jfib	OK	03-28-2008 11:46:37	20d 18h 48m 30s	1/4	Link to Jfib is Up
	check_isis_with_Jing	OK	03-28-2008 11:42:49	0d 23h 39m 6s	1/4	Link to Jing is Up
	check_isis_with_Jmed	OK	03-28-2008 11:45:26	17d 21h 57m 12s	1/4	Link to Jmed is Up
	check_isis_with_Jpet	OK	03-28-2008 11:46:38	17d 20h 42m 44s	1/4	Link to Jpet is Up
	check_isis_with_Jpge	OK	03-28-2008 11:42:50	17d 21h 54m 48s	1/4	Link to Jpge is Up
	check_isis_with_Jsmr	OK	03-28-2008 11:45:27	17d 21h 57m 11s	1/4	Link to Jsmr is Up
	check_isis_with_Jspr	OK	03-28-2008 11:46:39	17d 21h 55m 59s	1/4	Link to Jspr is Up
	check_ospf_with_rete20	OK	03-28-2008 11:42:50	21d 0h 0m 56s	1/4	Link to rete20 is Up
	ping	OK	03-28-2008 11:47:28	164d 19h 12m 5s	1/5	PING OK - Packet loss = 0%, RTA = 0.58 ms

Qualche screenshot... (4)

Current Network Status
Last Updated: Fri Mar 28 11:48:22 CET 2008
Updated every 90 seconds
Nagios® 3.0 - 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

Report di disponibilità

Hostgroup Availability Report
Last Updated: Sat Mar 29 12:08:09 CET 2008
Nagios® 3.0 - 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]

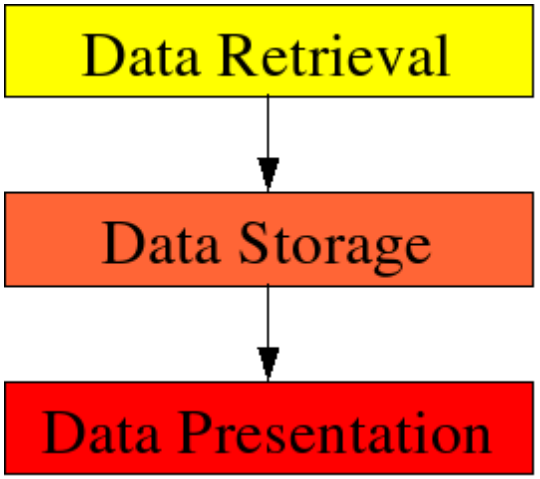
First assumed host state: Unspecified
First assumed service state: Unspecified
Report period: This Year
Backtracked archives: 4
Update

Hostgroup 'Routers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Jadm	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Jfib	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Jfig	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Jing	99.497% (99.497%)	0.503% (0.503%)	0.000% (0.000%)	0.000%
Jmed	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Jpet	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Jpge	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Jser	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Jsmr	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Jspr	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
sdh-gw	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
sumbra	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%

Cacti

- 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



Cacti: installazione

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

Che cosa puo' graficare:

- Il traffico e gli errori per le interfacce degli apparati di rete
- Contatori di varia natura

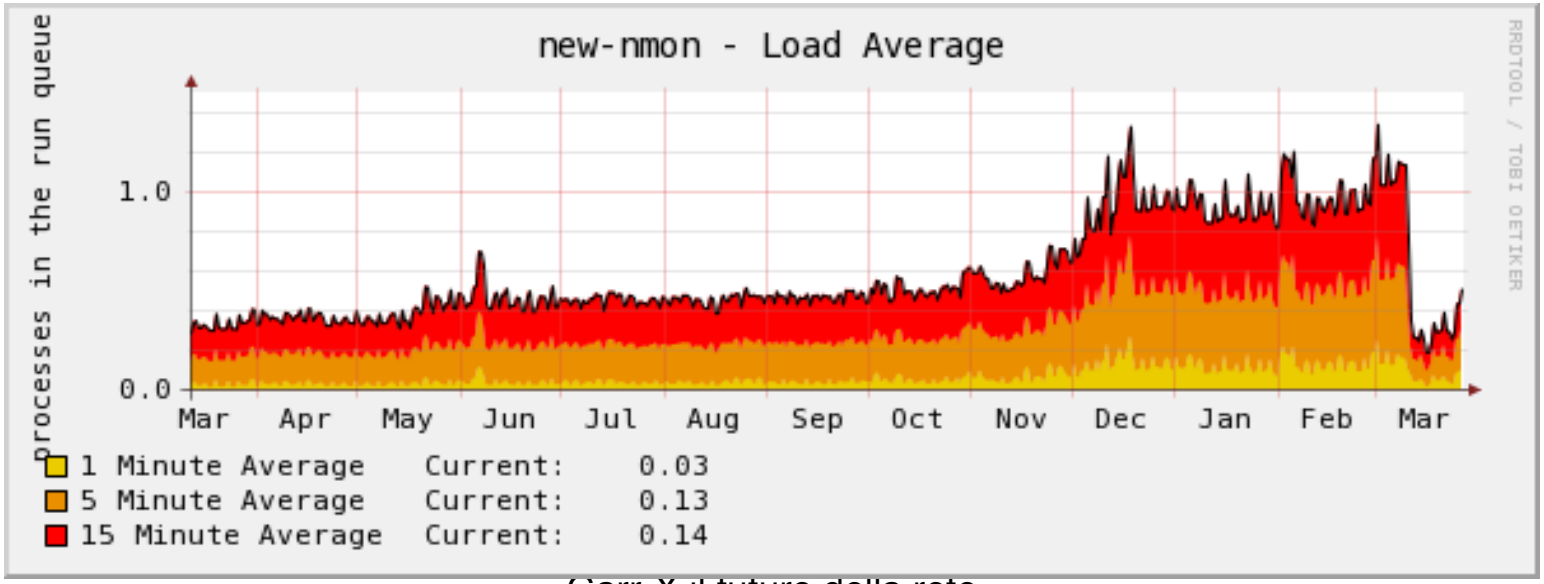
- Temperature (dischi, CPU, ecc...)
- LoadAverage e spazio disco
- Occupazione RAM
- Tensioni, velocità ventole
- Qualsiasi variabile venga passata...

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.

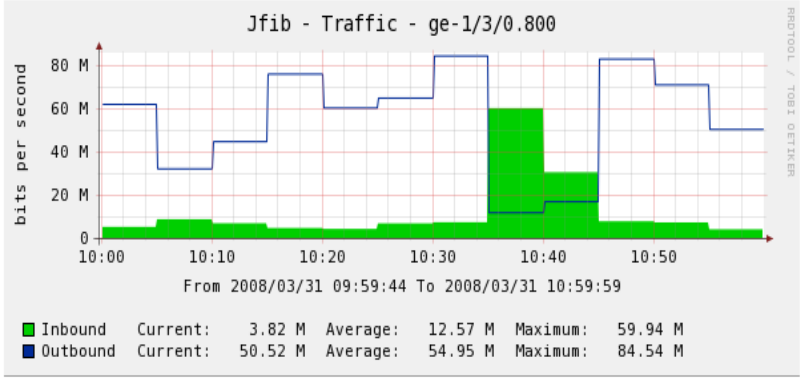
Al momento monitoriamo 93 hosts con 844 grafici, ma il sistema puo' ancora crescere...

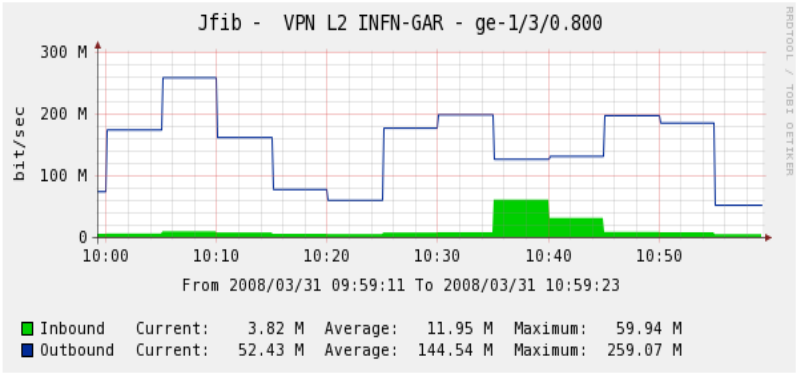


Curiosità:

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:

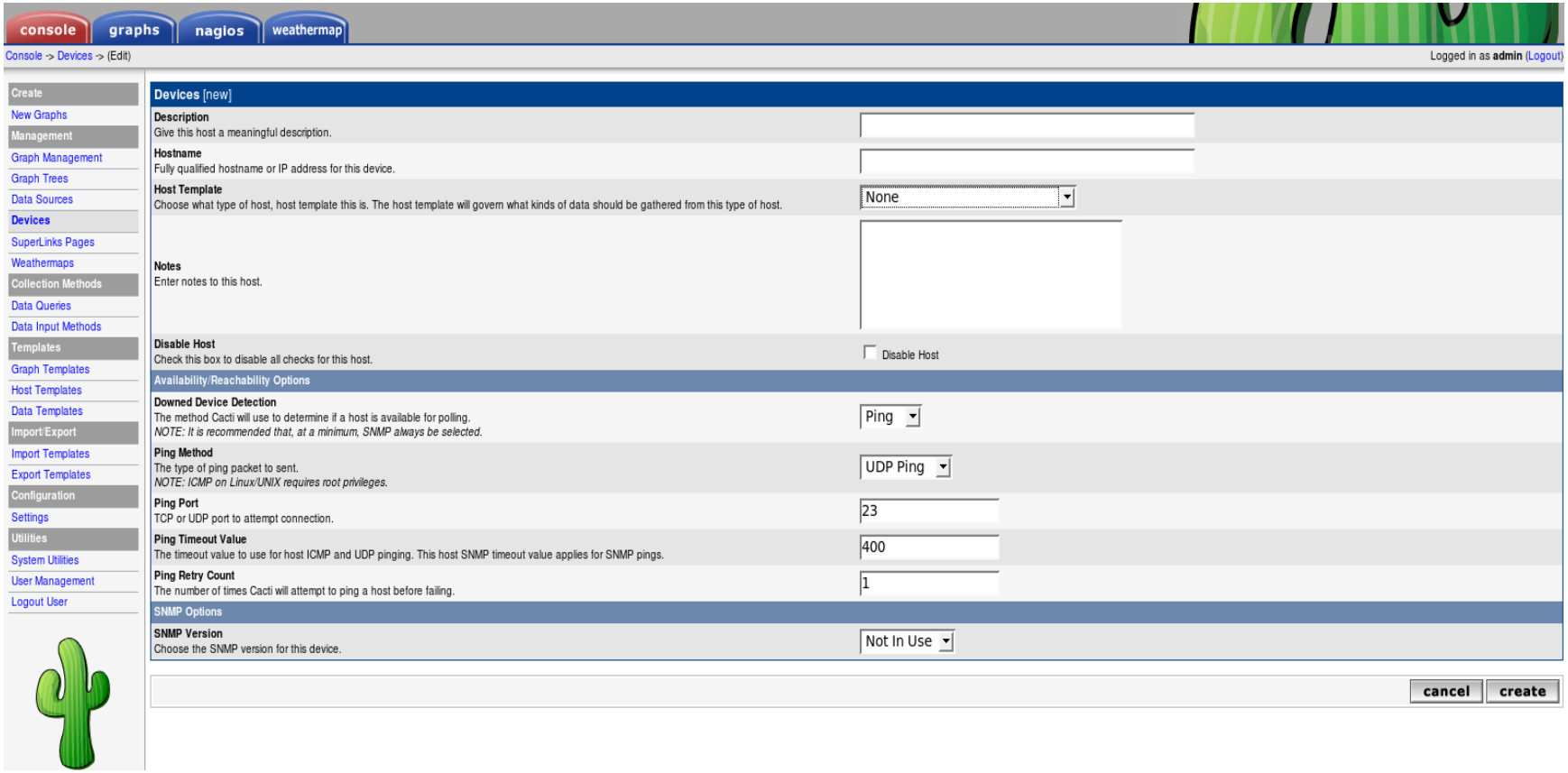




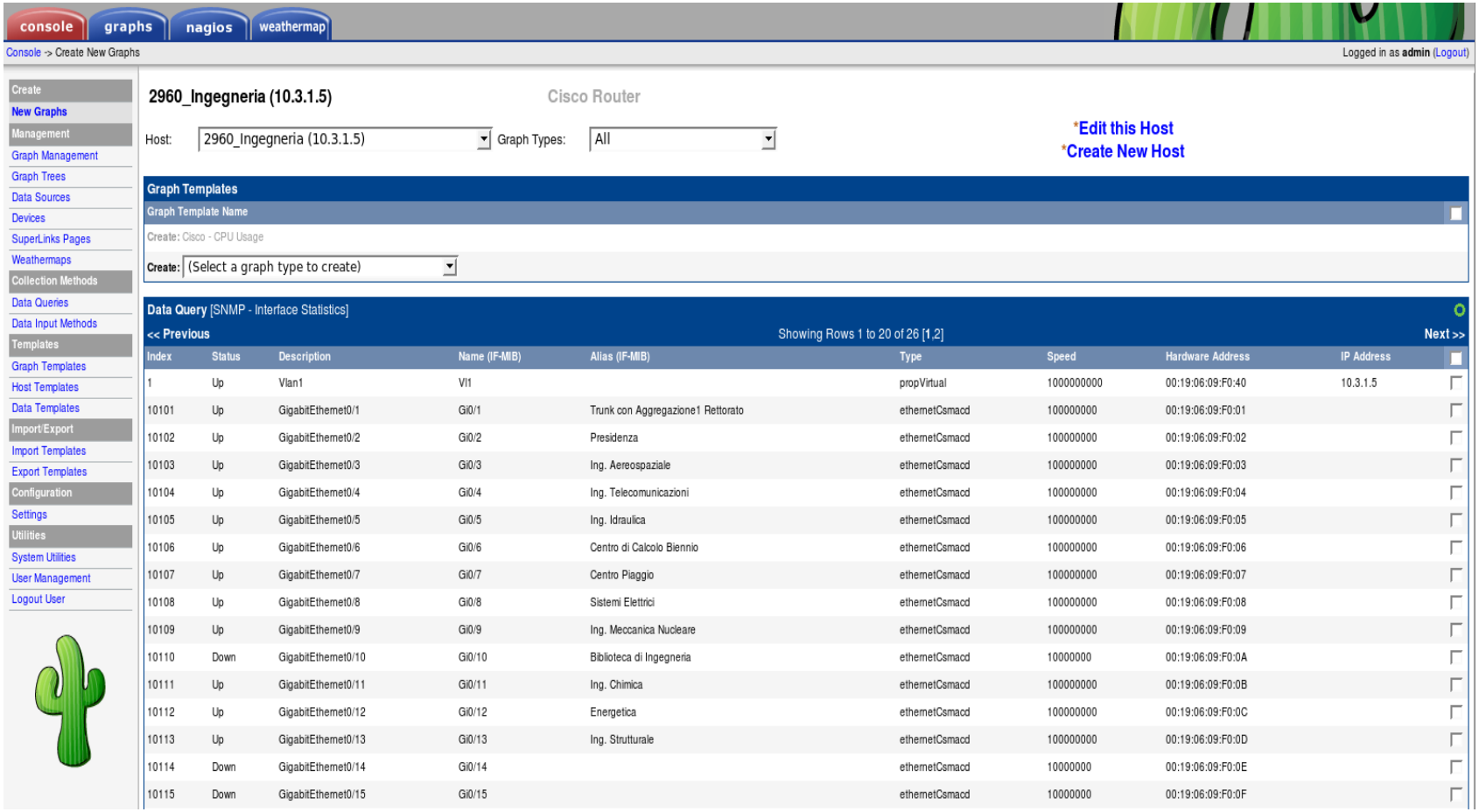
I templates

- 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

Creazione di un device



Creazione di un grafico



Reti virtualizzate

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

Reti virtualizzate

- 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 .

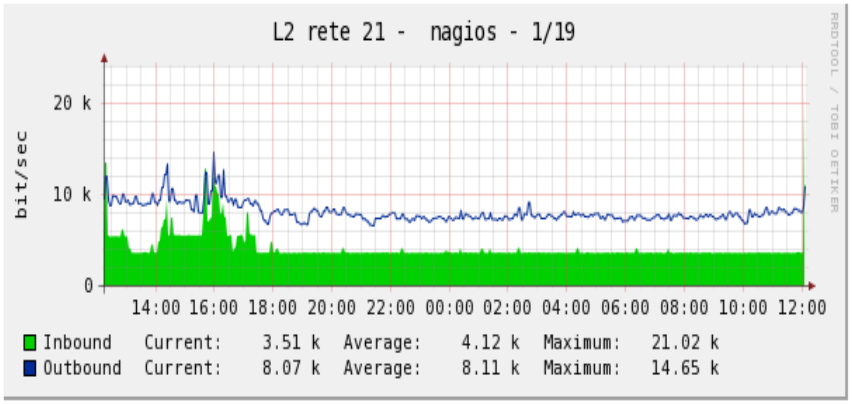
E' utile anche in situazioni in cui si vogliono distinguere traffici diversi dei quali si conosce l'origine o la destinazone .

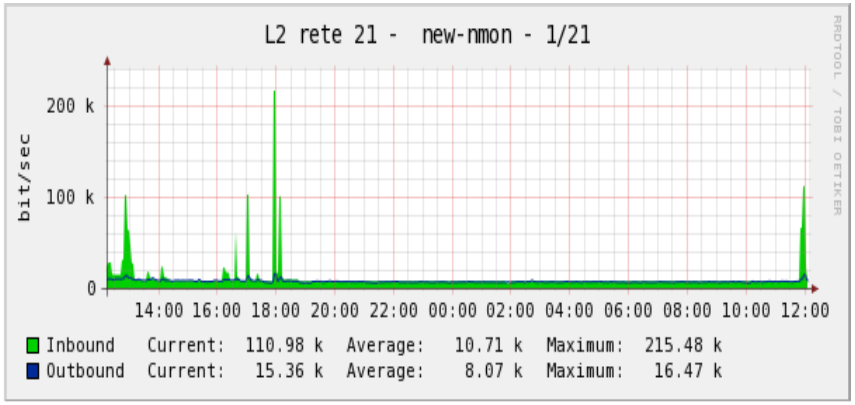
Questo è bene per conoscere ad esempio il comportamento della rete in condizioni di QoS

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:





Cacti Plugin Architecture

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

Alcuni plugin interessanti

- **PHP Weathermap:**

Crea una weathermap a partire dal database di cacti

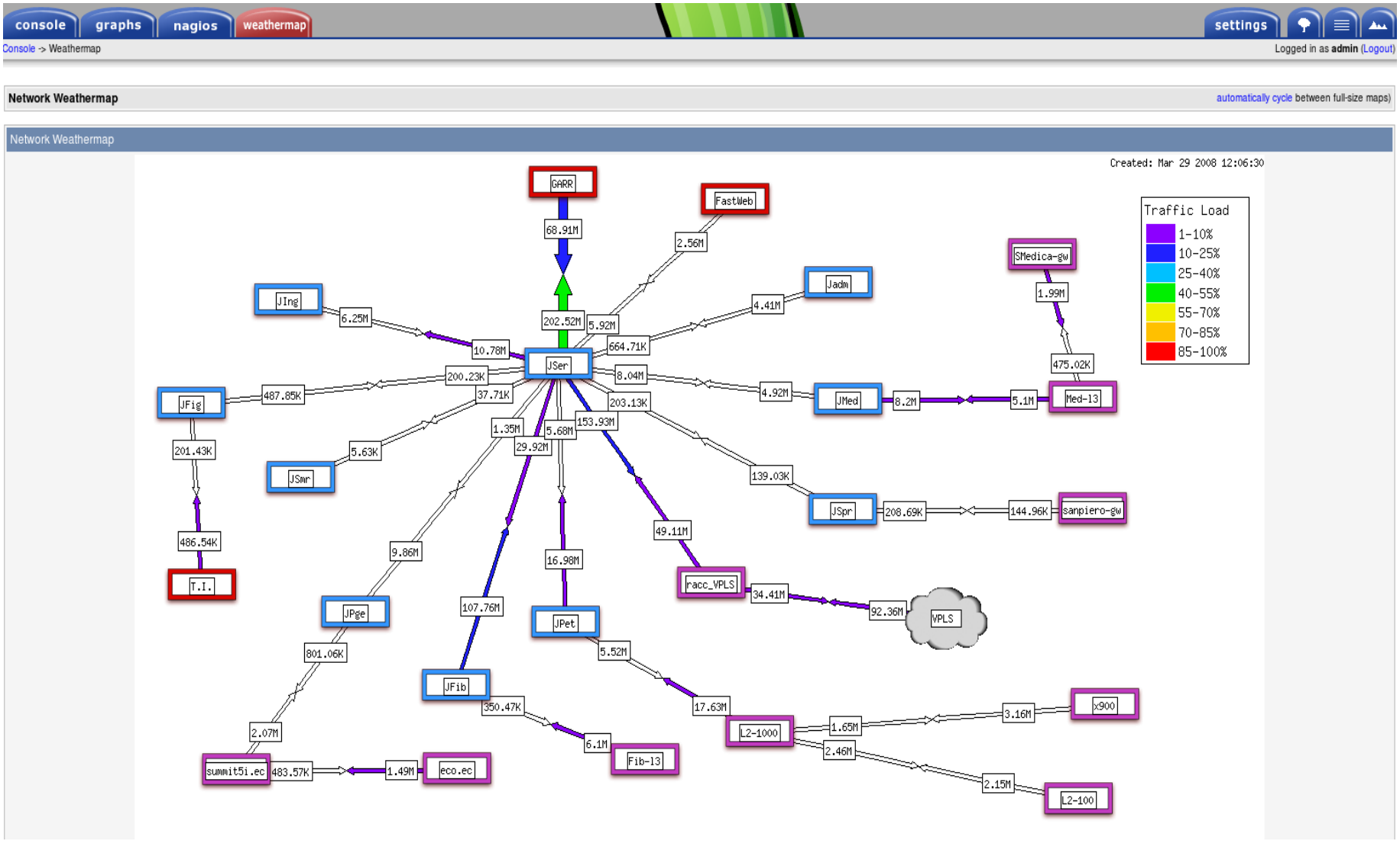
- **Ntop:**

Integra Ntop nell'interfaccia web di cacti

- **SuperLinks:**

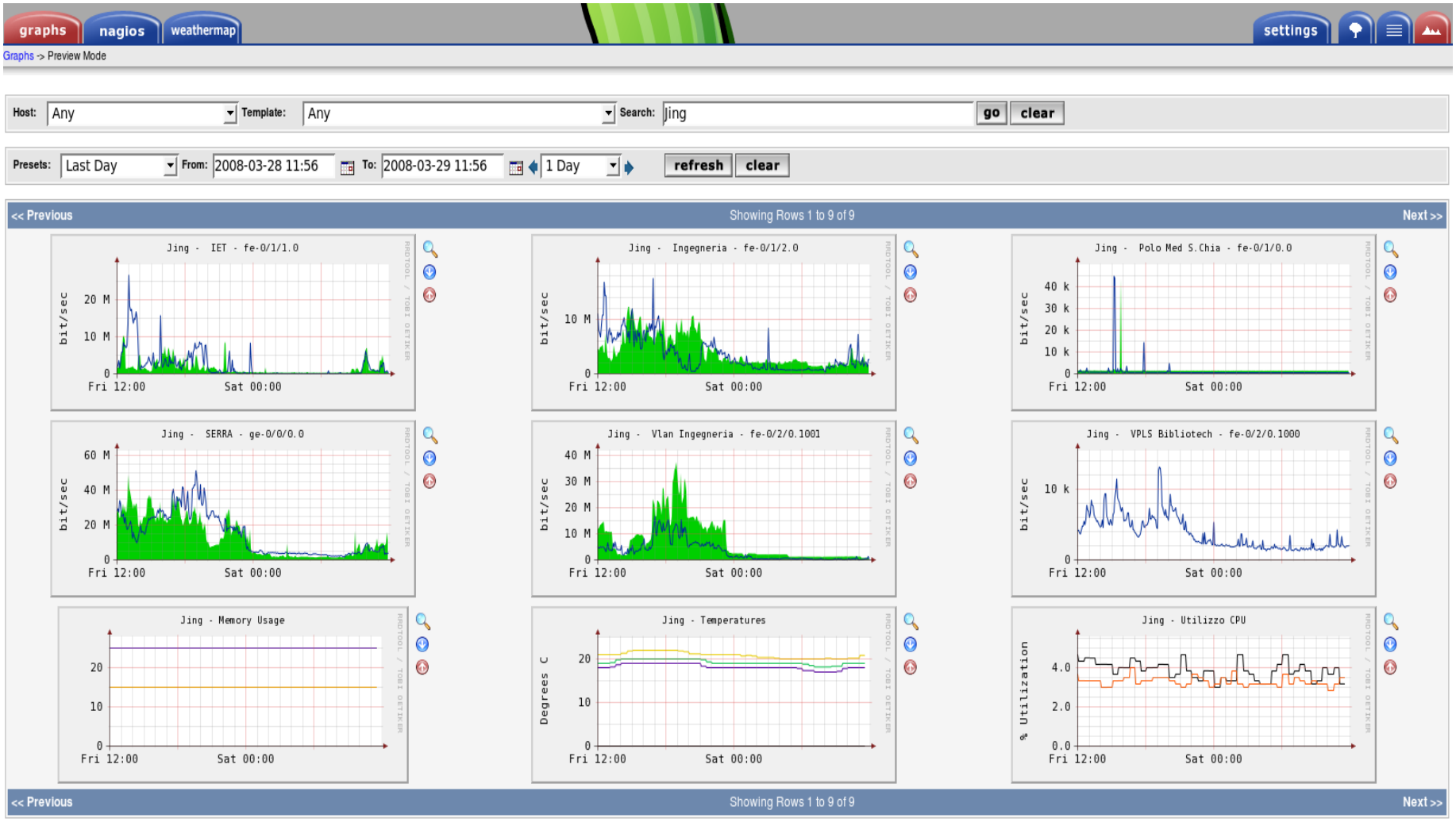
Permette di creare tabs con link esterni cosi da integrare altri servizi (ad esempio Nagios)

La nostra WeatherMap

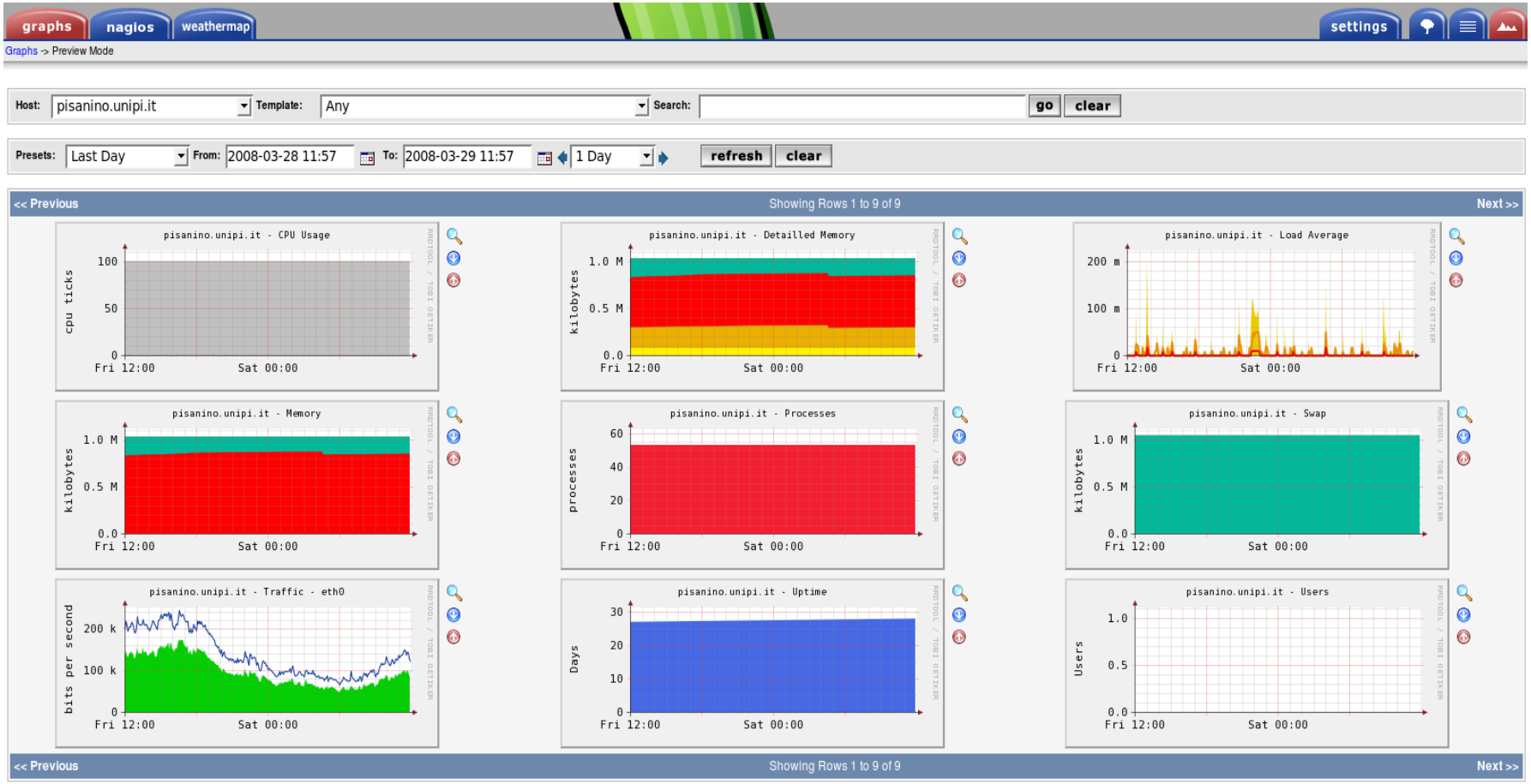


Garr-X il futuro della rete

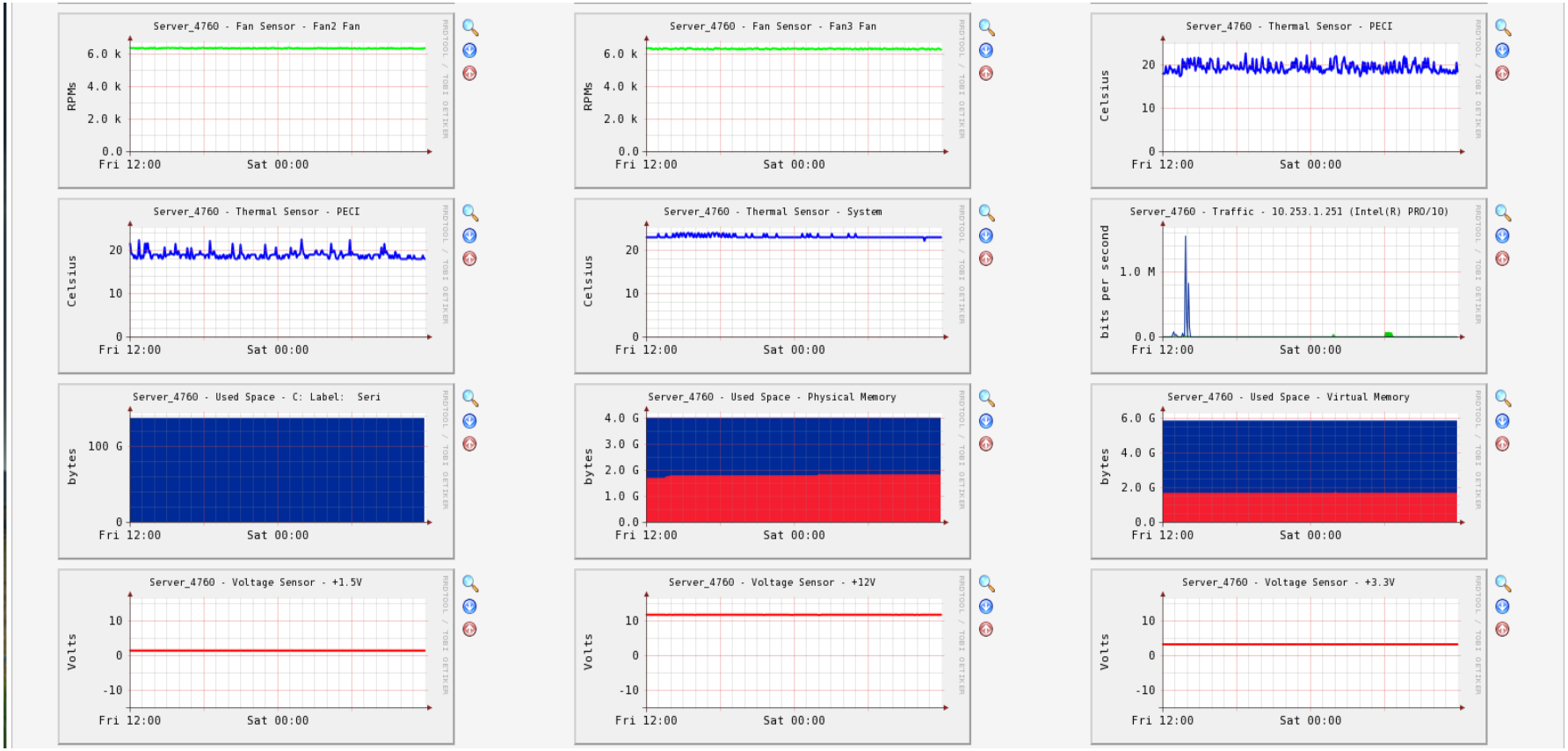
Screenshots (1)



Screenshots (2)



Screenshots (3)

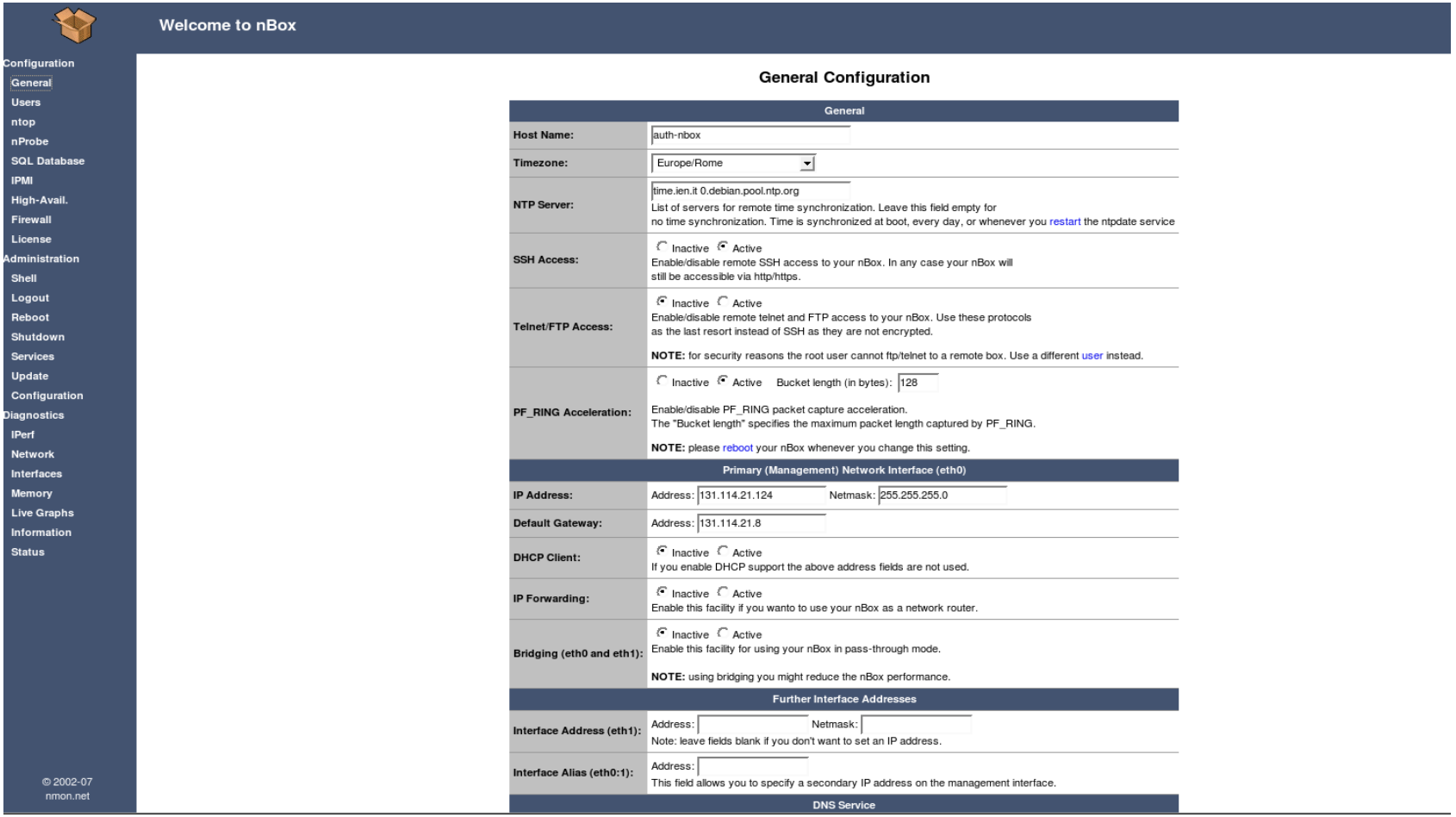


NTop

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

Qualche screenshot (1)

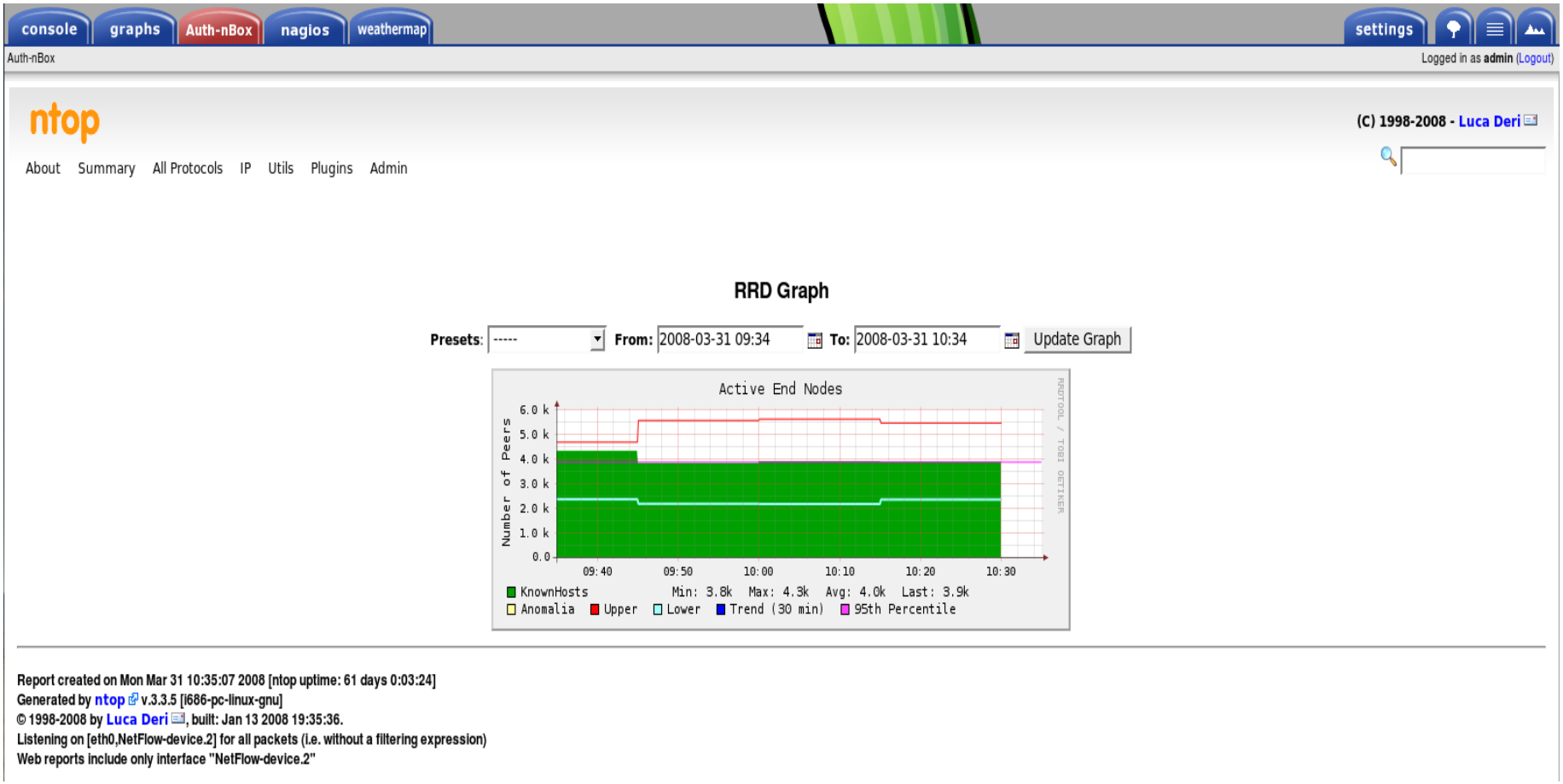


Qualche screenshot (2)

Global Protocol Distribution

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

Qualche screenshot (3)



In futuro...

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...