GARR-X Progress
Infrastruttura digitale per promuovere ricerca, istruzione e competitività nel Sud

Potenziamento strutturale
Avviso D.D.274
del 15/02/2013

Ministero dell'Istruzione dell'Università e della Ricerca

PON Ricerca e Competitività 2007-2013 — Piano di Azione Coesione

Governo Italiano - Presidenza del Consiglio dei Ministri
Ministro per la Coesione Territoriale

GARR PROGRESS in Training

Giovanni Cesaroni GARR

Monitoring della rete GARR

Agenda

- GINS
  - Statistiche di traffico
  - Tool di monitoring
- Come monitorare la rete
  - SNMP poll
  - SNMP trap
  - Latenza
  - Temperature
  - Looking glass
  - LLDP
- «Hands on»
  - SNMP Trap con snmptrapd
  - SNMP Trap con nodejs
  - SNMP Poll esempi
  - RRD

GINS

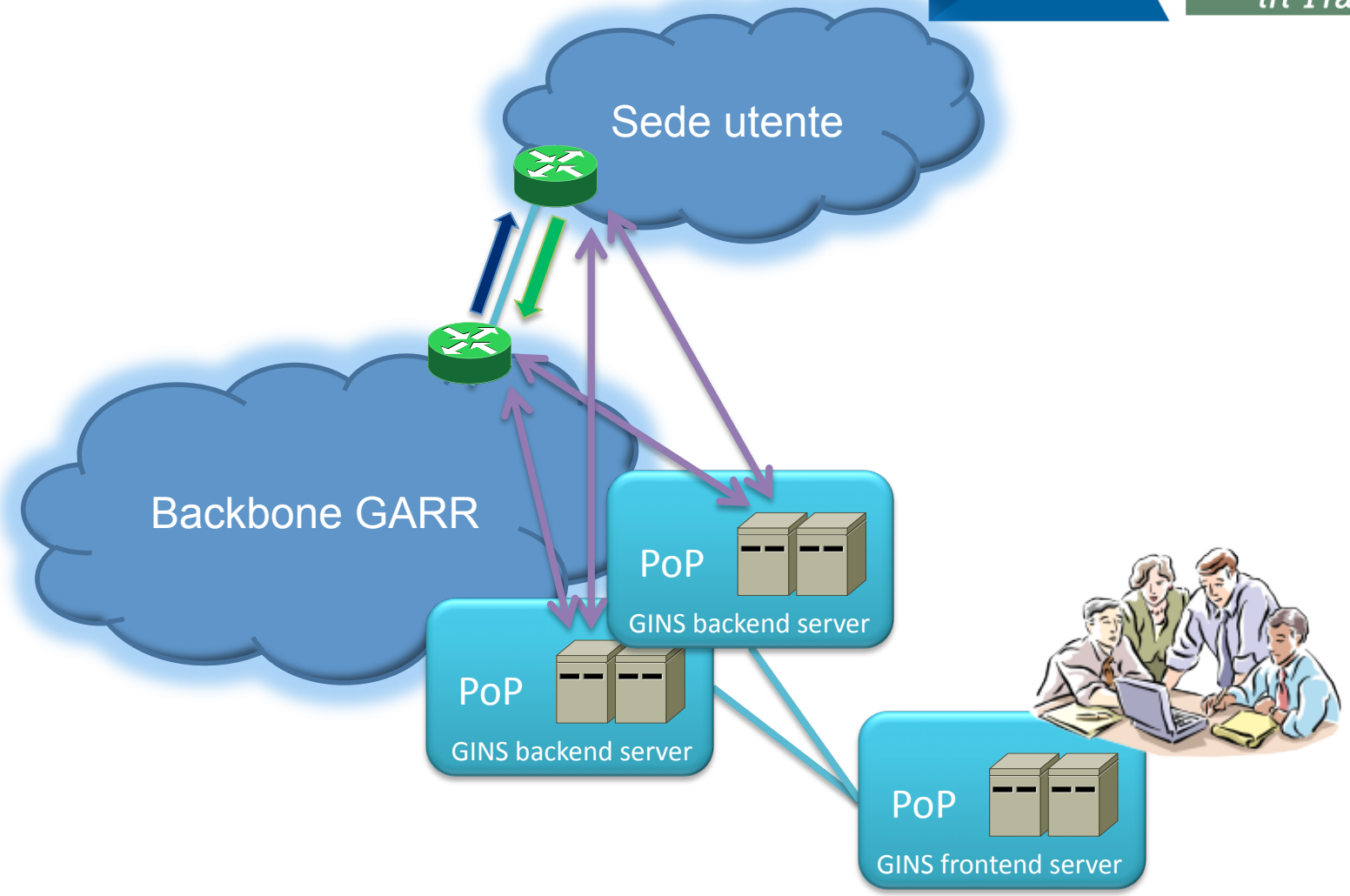
GARR Integrated Networking Suite

https://gins.garr.it/

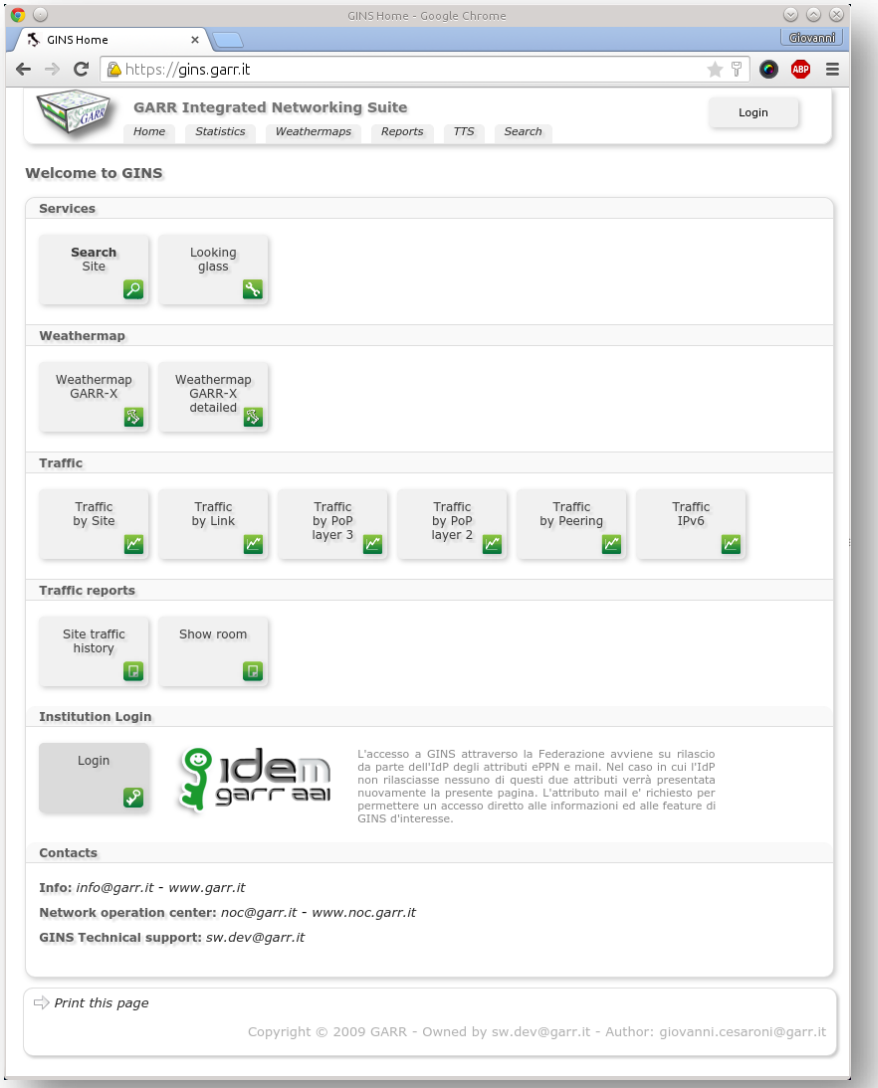
Scopi:

- Monitorare lo stato e le performance della rete
  - Connettivita' utenti, backbone, servizi ad ogni livello
  - Stato, performance, evoluzione storica
- Permettere al NOC, OPS di gestire «facilmente» le rete
  - TTS, reports, UIs, automatizzazione configurazione tools

Architettura

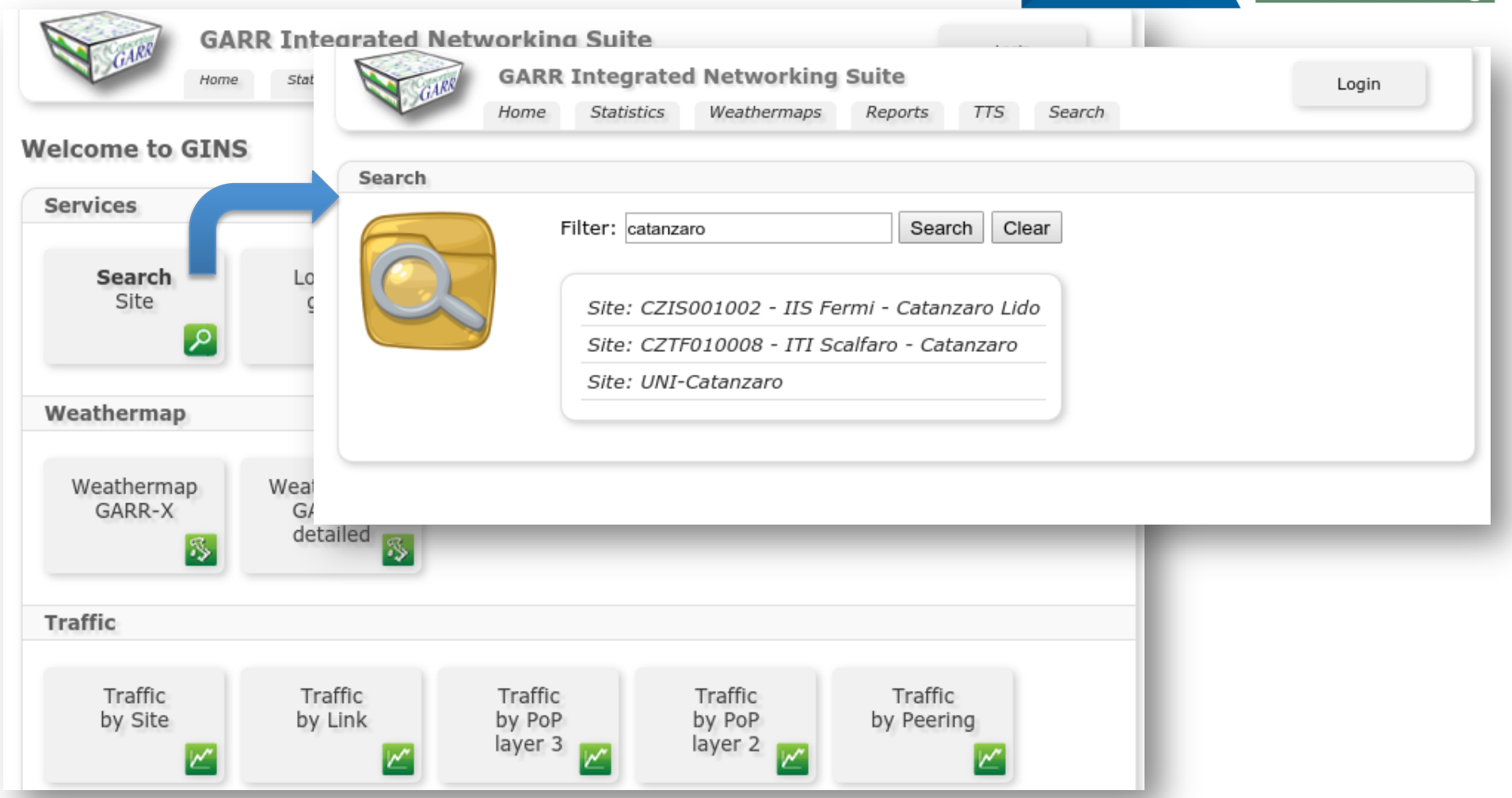


GINS home page



- Statistiche di traffico
- Weathermap
- Trouble tickets
- Reportistica
- Tools

Ricerca sede



Interfaccia sede

Statistiche aggregate dei link

Statistiche link

Trouble ticket

Interfaccia sede: trouble tickets

Show 10 entries Search:

ID	Start	End	Object	Ticket type	Problem type	Problem description	Problem fix	Site name	Site extended name	Key	Competence	Operatore
15780 Close	27/04/2015 17:00	27/04/2015 20:00	PoP Catanzaro-Germaneto	Planned maintenance	Other	Manutenzione programmata sul PoP di Catanzaro. Si prevede possibile assenza di connettivita' nella fascia oraria indicata.	Manutenzione conclusa.	CZIS001002 - IIS Fermi - Catanzaro Lido	CZIS001002 - IIS E. Fermi - Catanzaro Lido	SGP	Other	Gervasi
15616 Close	25/02/2015 15:04	26/02/2015 08:30	RC-CZ -- RX1-CT1 on rx1.ct1.garr.net	Incident	Fault	Assenza di connettivita'.	Connettivita' ripristinata a seguito del ripristino dell'energia elettrica.	CZIS001002 - IIS Fermi - Catanzaro Lido	CZIS001002 - IIS E. Fermi - Catanzaro Lido	SGP	User	Gervasi
15554 Close	02/02/2015 09:13	02/02/2015 10:44	CZIS001002 - IIS Fermi - Catanzaro Lido	Incident	Fault	Assenza di connettivita'	Ripristinata energia elettrica.	CZIS001002 - IIS Fermi - Catanzaro Lido	CZIS001002 - IIS E. Fermi - Catanzaro Lido	SGP	Supplier	Gervasi

Showing 1 to 3 of 3 entries First Previous 1 Next Last

Oggetto del ticket

Problem/Fix

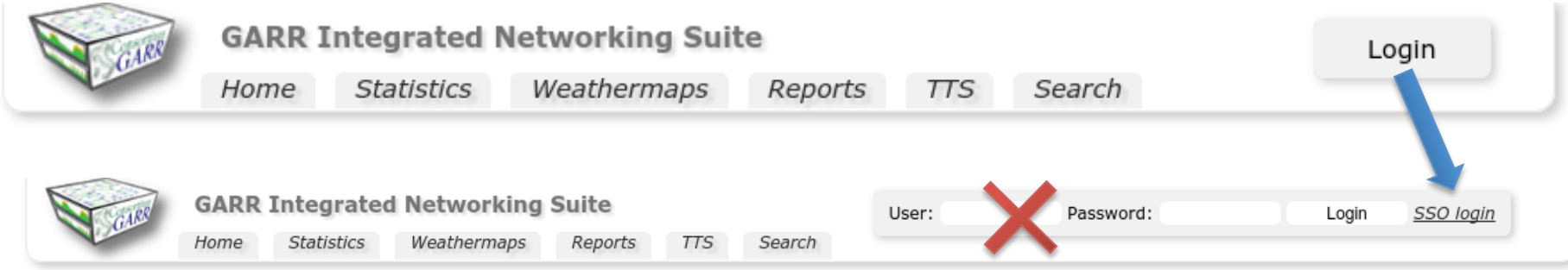
Sede

@NOC

AAI

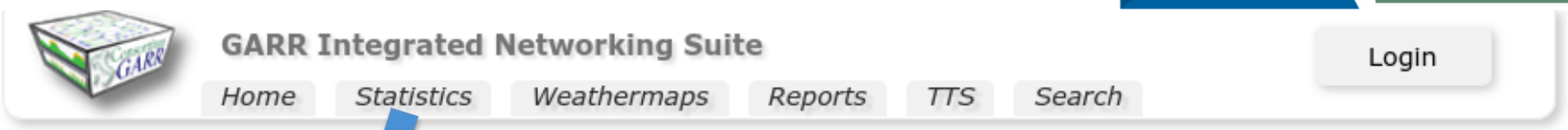
GINS e' un SP federato

Autenticazione



Autorizzazione

Statistiche di traffico



GINS Statistics

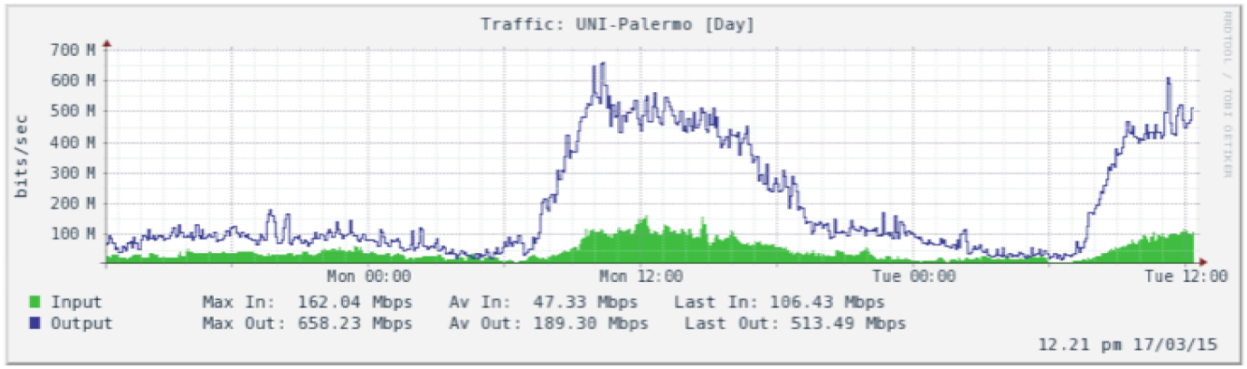
- Statistiche di traffico dei **link IP** per **utenza**
- Statistiche di traffico dei **link IP** per **PoP** di attestazione **layer 3**
- Statistiche di traffico dei **link IP** per **PoP** di attestazione **layer 2**
- Statistiche di traffico **aggregate** dei link IP per **utenza**
- Statistiche di traffico dei **Peering**
- Statistiche di traffico dei **Content services**
- Statistiche di traffico **IPv6**
- Statistiche di **temperatura** e **CPU load** apparati

Statistiche di traffico: aggregati

*Statistiche di traffico **aggregate** dei link IP per **utenza***

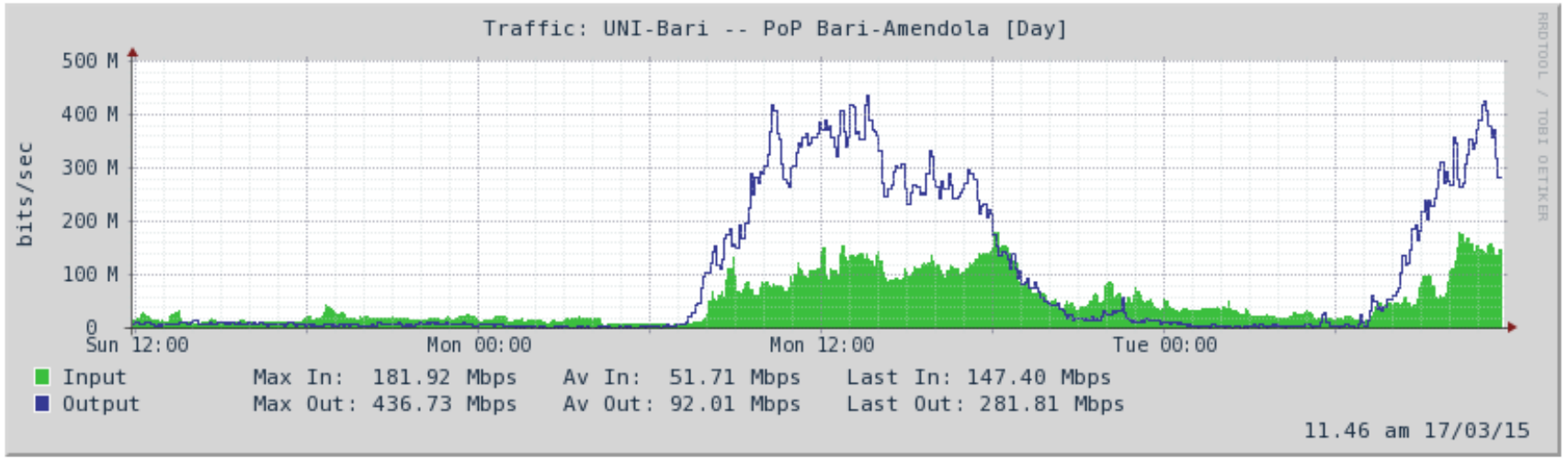
UNI-Palermo close

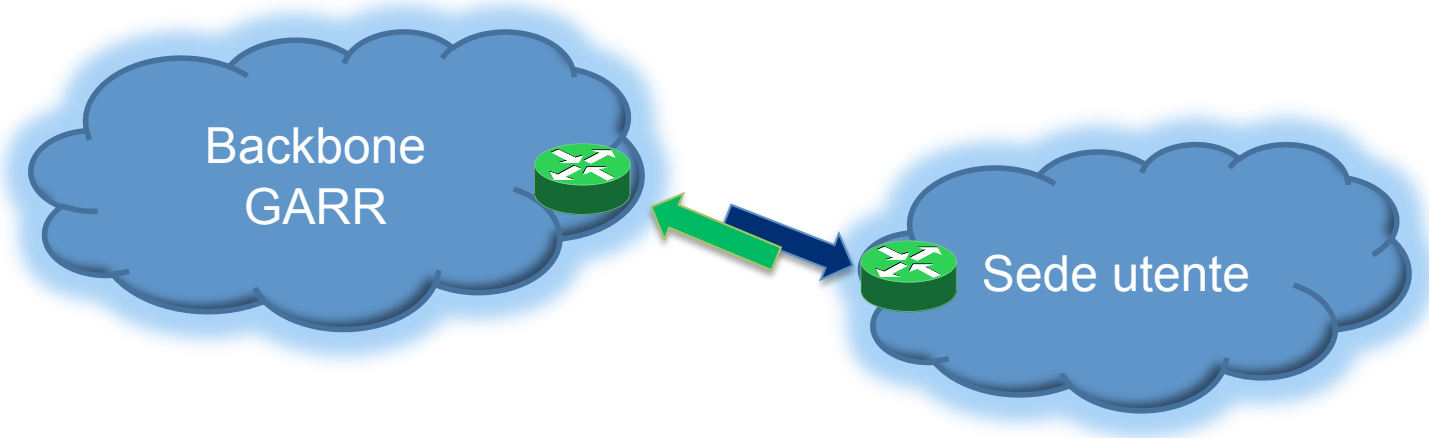
Link Name	Link Type	Equipment	IP Address	Interface	Url
e2e UNI-Palermo - sede di Agrigento - Polo Universitario di Villa Genuardi -- Uni-Palermo lato PA	DF 100Mbps FE	rx1.pa1.garr.net		ge-0/3/7.1010	
e2e UNI-Palermo - sede di Agrigento - Polo Universitario via Quartararo -- Uni-Palermo lato PA	DF 100Mbps FE	rx1.pa1.garr.net		ge-0/3/7.1011	
e2e UNI-Palermo - sede di Trapani -- Uni-Palermo lato PA	DF 100Mbps FE	rx1.pa1.garr.net		ge-0/3/7.1013	
UNI-Palermo -- PoP Palermo-Scienze	Direct 10Gbps 10GE	rx1.pa1.garr.net	193.206.137.209	xe-0/1/1.0	



Statistiche di traffico

Colori e direzioni del traffico:

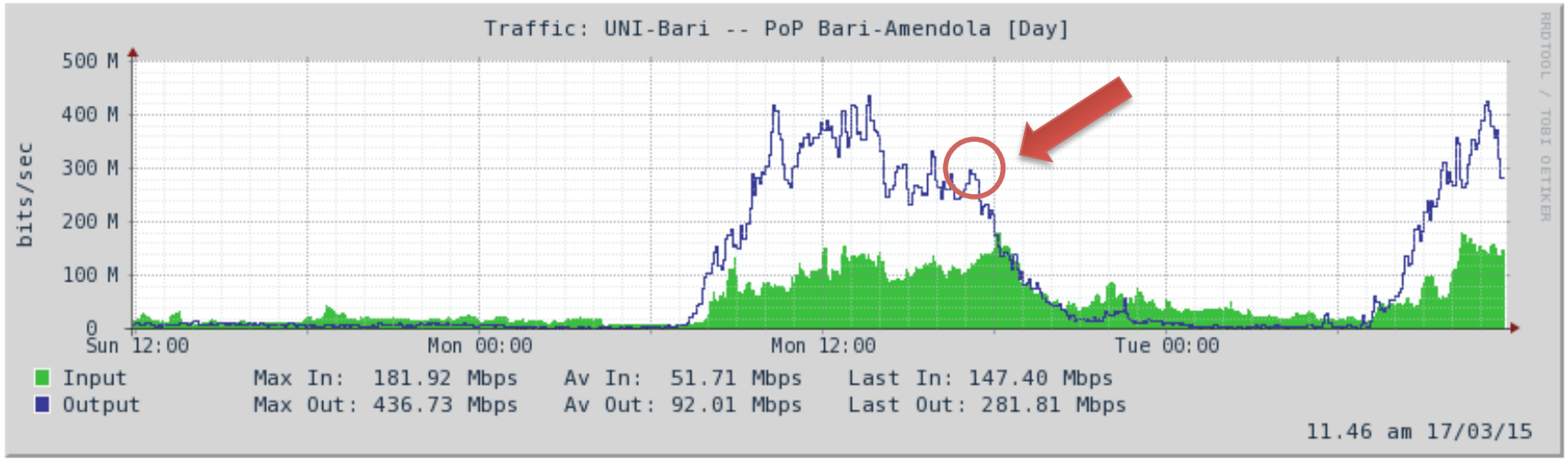




Statistiche di traffico

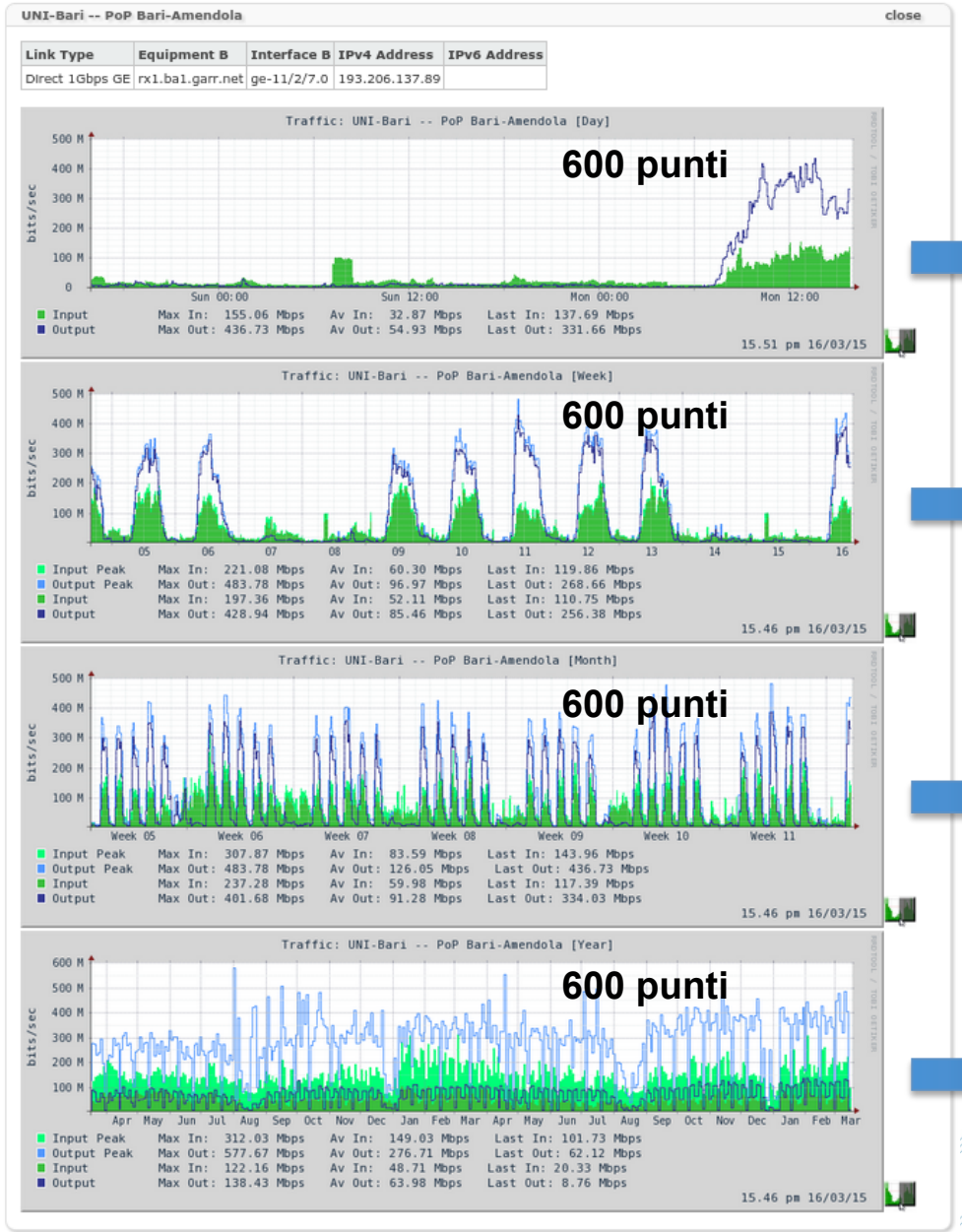
Valori:

- Lettura del contatore incrementale a 64 bit che conta Bytes passati su una porta
- Lettura ogni 5 minuti e computazione del bit rate



Sono veramente 300 Mbps ?
mediamente nei 5 minuti si,
ma potrebbero anche essere 600 Mbps per 2.5' e 0 per 2.5'

Statistiche di traffico



Lettura del contatore ogni 5 minuti

un punto ogni 5 minuti

un punto ogni mezz'ora
media e picco nella mezz'ora

un punto ogni 2 ore
media e picco sulle 2 ore

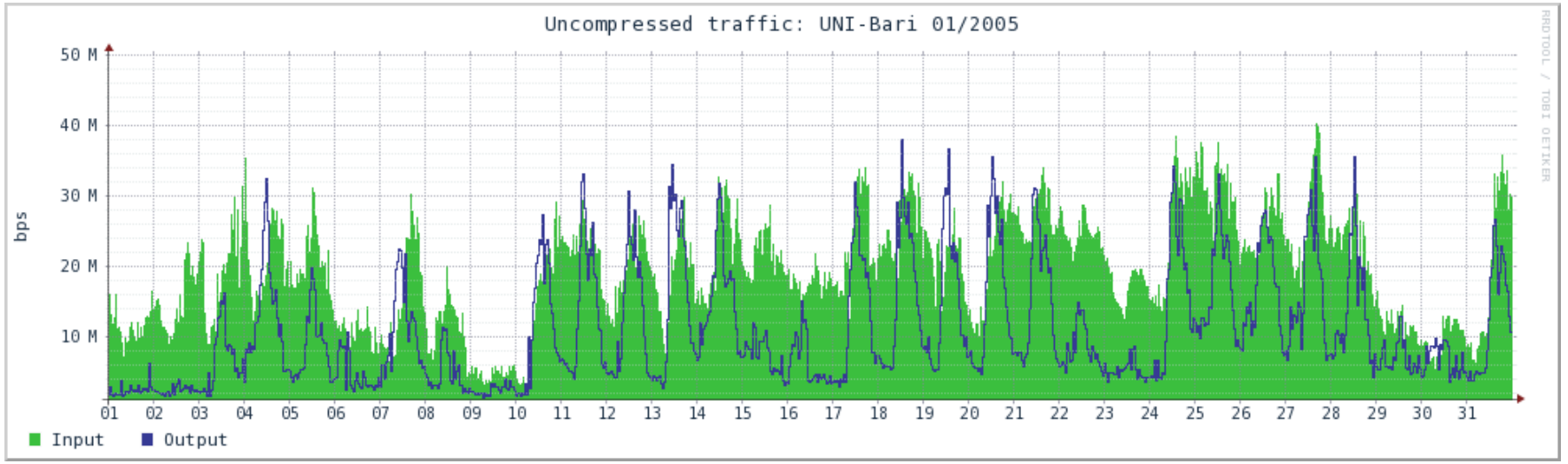
un punto ogni giorno
media e picco sulle 24 ore

compressione

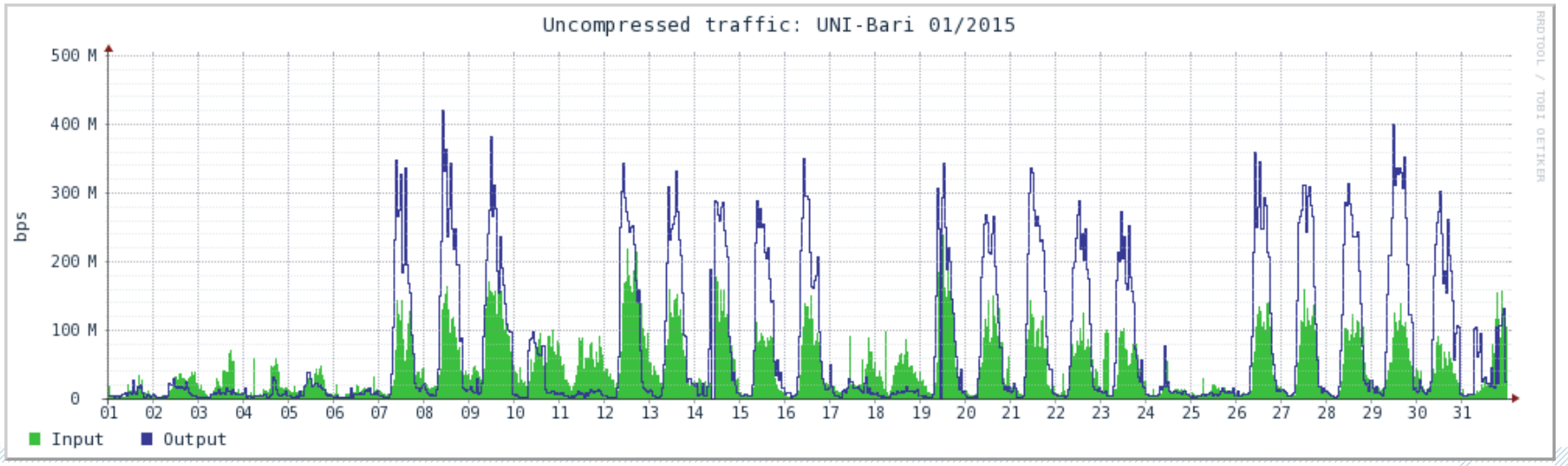
Statistiche non compresse

Reports > Statistiche di traffico non compresse

2005



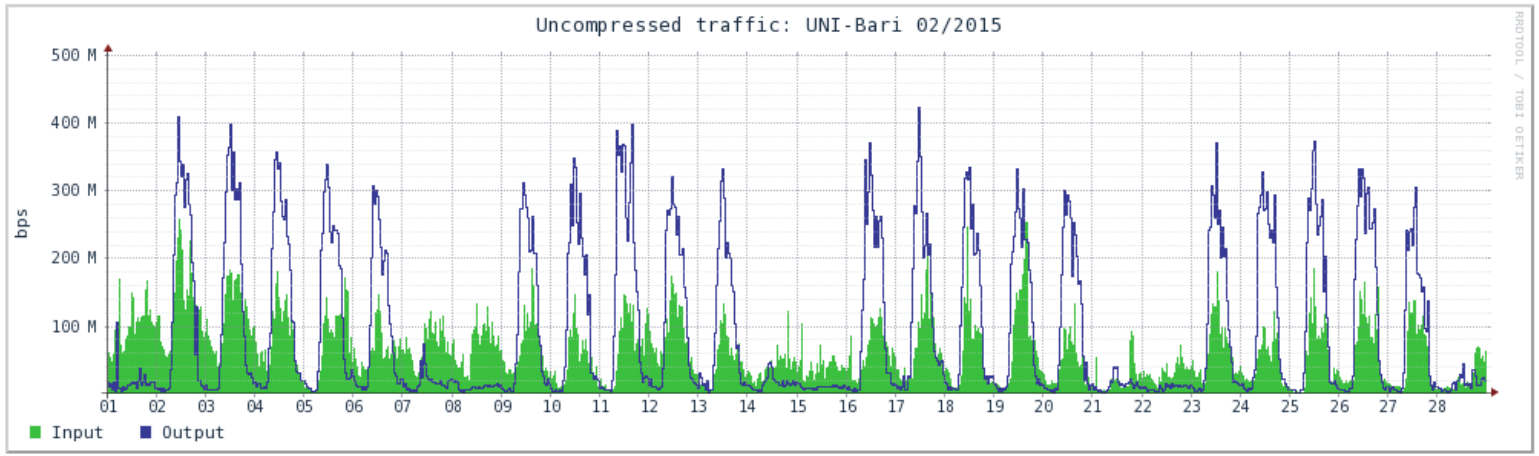
2015

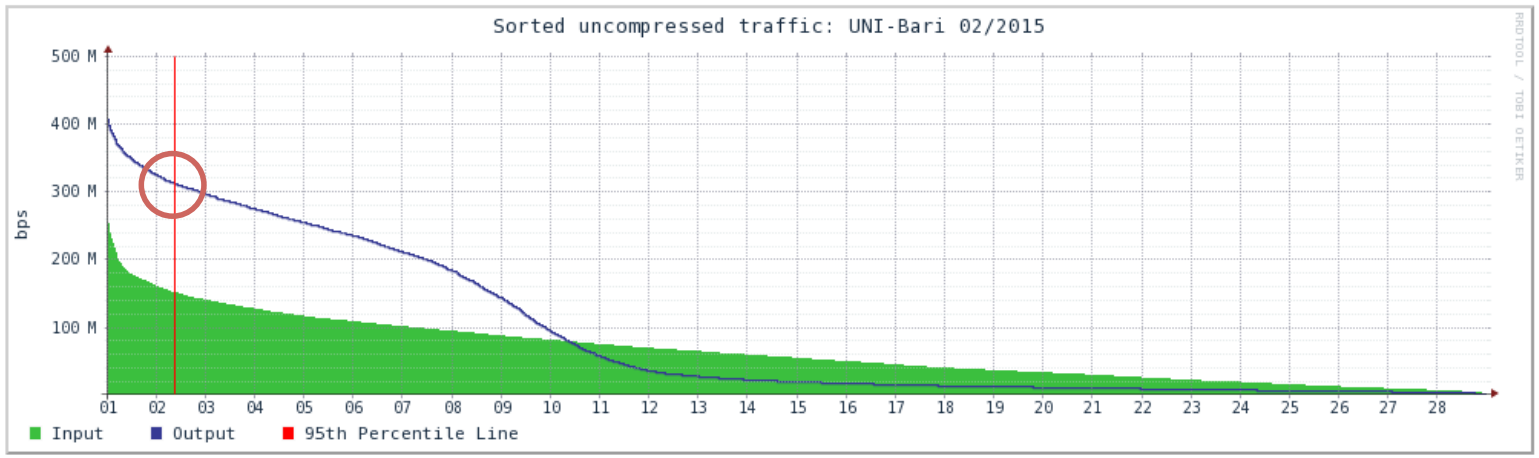


95° percentile

UNI-Bari

Month	Average In (Mbps)	Average Out (Mbps)	Max In (Mbps)	Max Out (Mbps)	Volume In (Tb)	Volume Out (Tb)	95th percentile In (Mbps)	95th percentile Out (Mbps)	95th percentile (Mbps)
02/2015	64.35	89.78	315.06	447.41	155.72	217.25	151.27	313.04	313.04





Statistiche non compresse

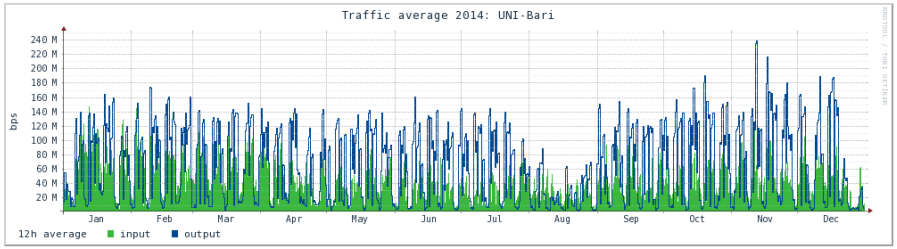
Reports > Statistiche di traffico non compresse

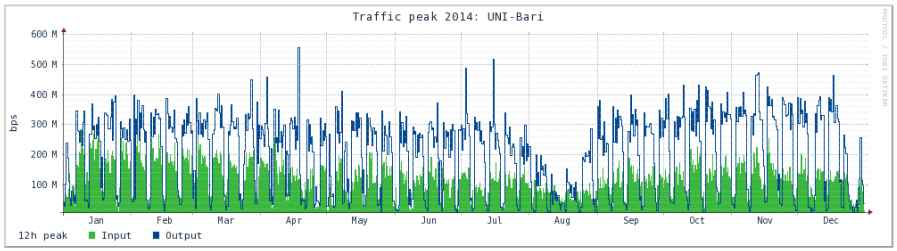
Uncompressed traffic Statistics:

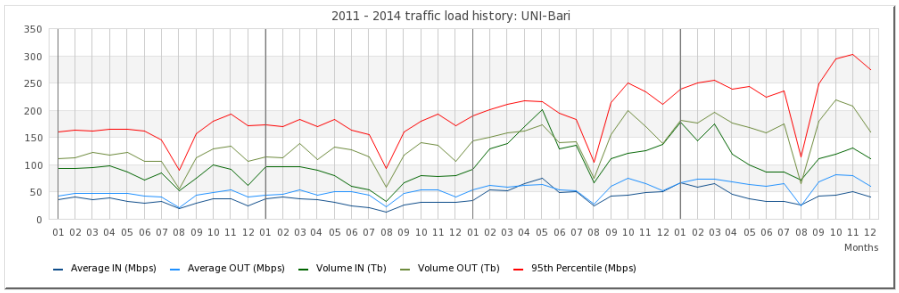
UNI-Bari

Month	Average In (Mbps)	Average Out (Mbps)	Max In (Mbps)	Max Out (Mbps)	Volume In (Tb)	Volume Out (Tb)	95th percentile In (Mbps)	95th percentile Out (Mbps)	95th percentile (Mbps)
01	66.74	67.78	309.91	394.81	178.80	181.57	176.41	238.31	238.31
02	59.56	72.88	275.26	398.58	144.13	176.36	167.90	249.81	249.81
03	65.44	73.22	313.35	449.56	175.07	195.89	157.12	255.27	255.27
04	46.03	68.29	256.74	555.07	119.33	177.05	132.39	239.22	239.22
05	37.45	63.04	206.96	409.87	100.34	168.89	109.45	243.23	243.23
06	33.35	61.29	191.83	371.84	86.45	158.89	97.16	224.21	224.21
07	32.40	65.45	173.48	516.78	86.81	175.34	95.18	235.34	235.34
08	26.95	24.65	116.22	287.43	72.21	66.04	61.16	114.87	114.87
09	42.72	69.43	188.20	397.39	110.75	180.01	110.17	249.25	249.25
10	44.77	81.80	228.66	431.37	120.11	219.44	119.34	294.00	294.00
11	50.28	80.39	254.02	471.49	130.35	208.42	134.65	303.04	303.04
12	41.65	59.95	204.83	462.72	111.58	160.60	109.33	274.41	274.41

	Average		Maximum		Total volume		Average percentile		
	Average In (Mbps)	Average Out (Mbps)	Max In (Mbps)	Max Out (Mbps)	Volume In (Tb)	Volume Out (Tb)	95th percentile In (Mbps)	95th percentile Out (Mbps)	95th percentile (Mbps)
Year	45.61	65.68	313.35	555.07	1435.93	2068.5	122.52	243.41	243.41







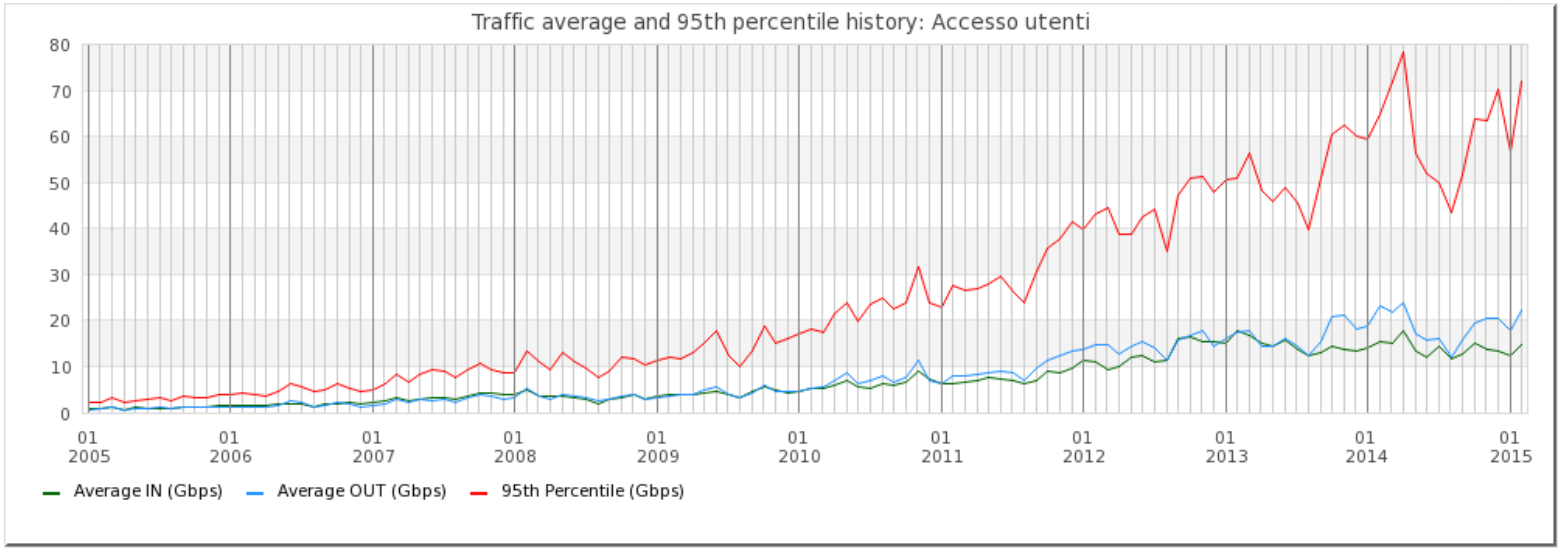
Dati mensili e annuali

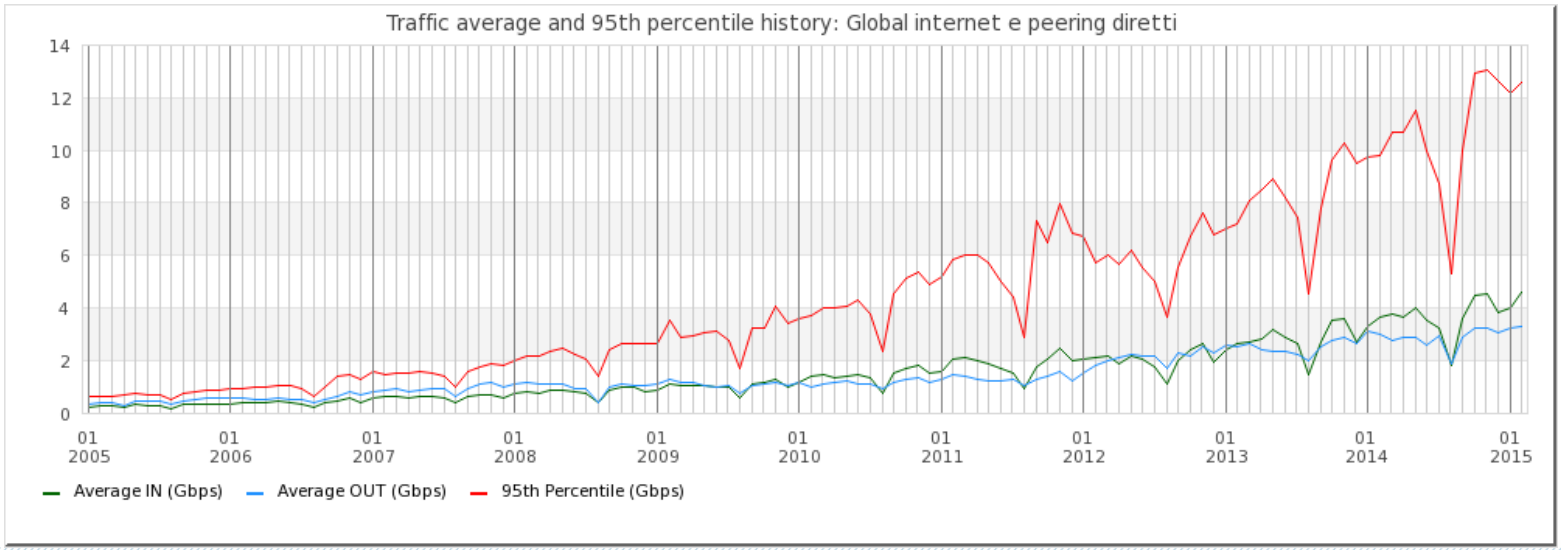
Grafico anno, media su 12 ore

Grafico anno, picchi su 12 ore

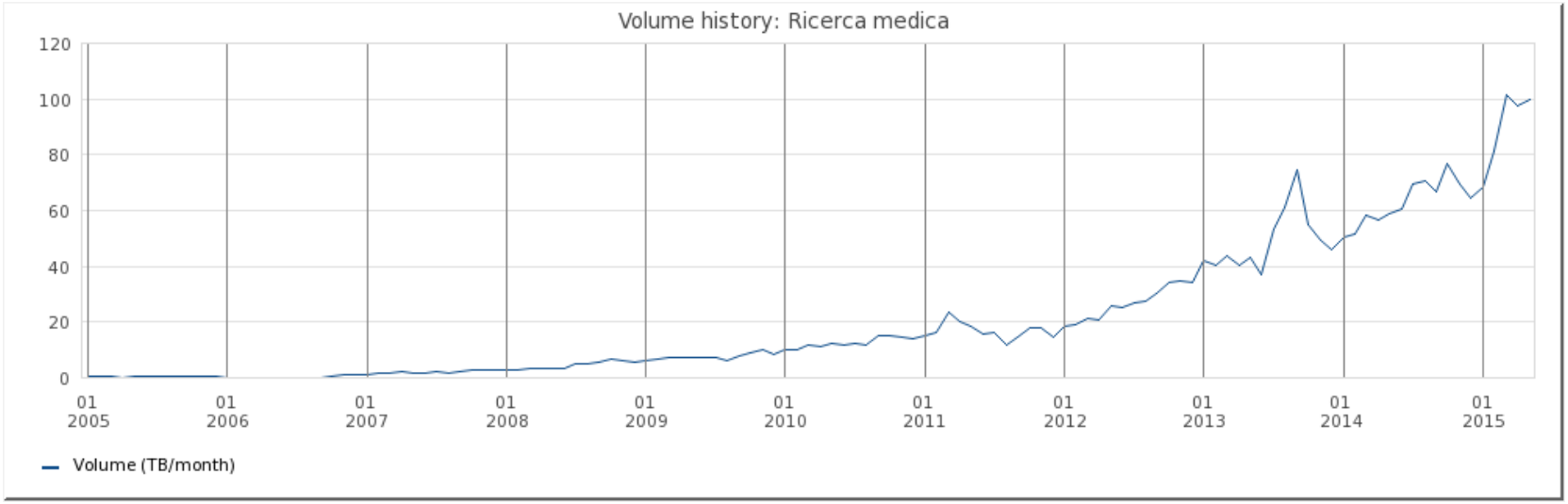
Evoluzione mensile su 4 anni

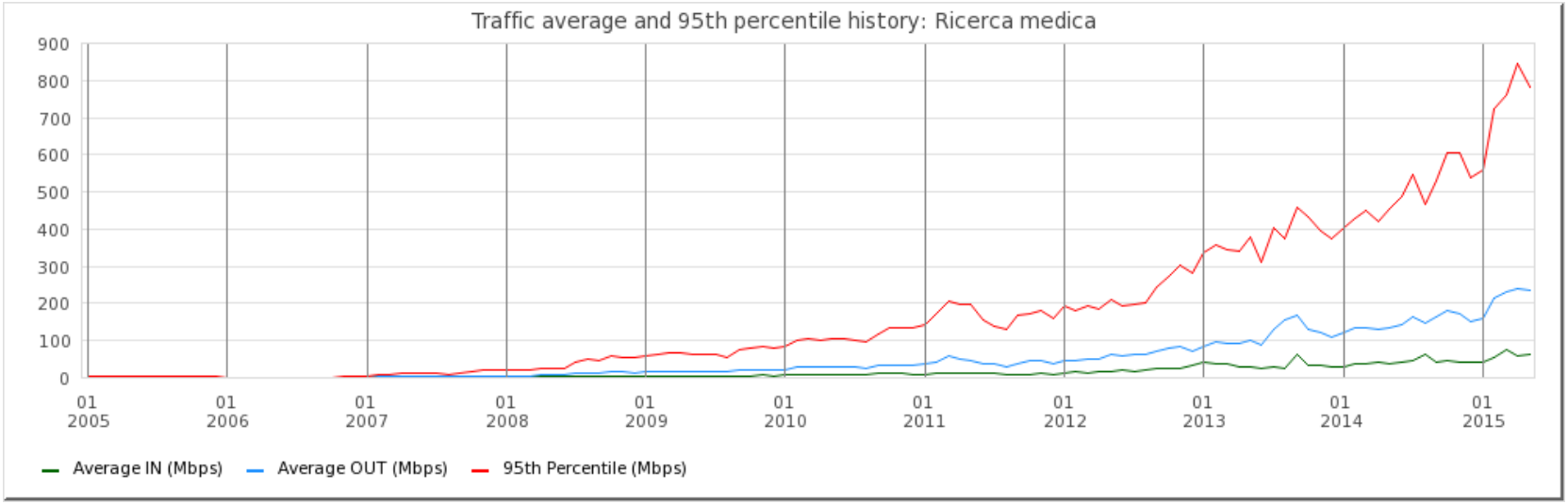
Evoluzione della connettivita’



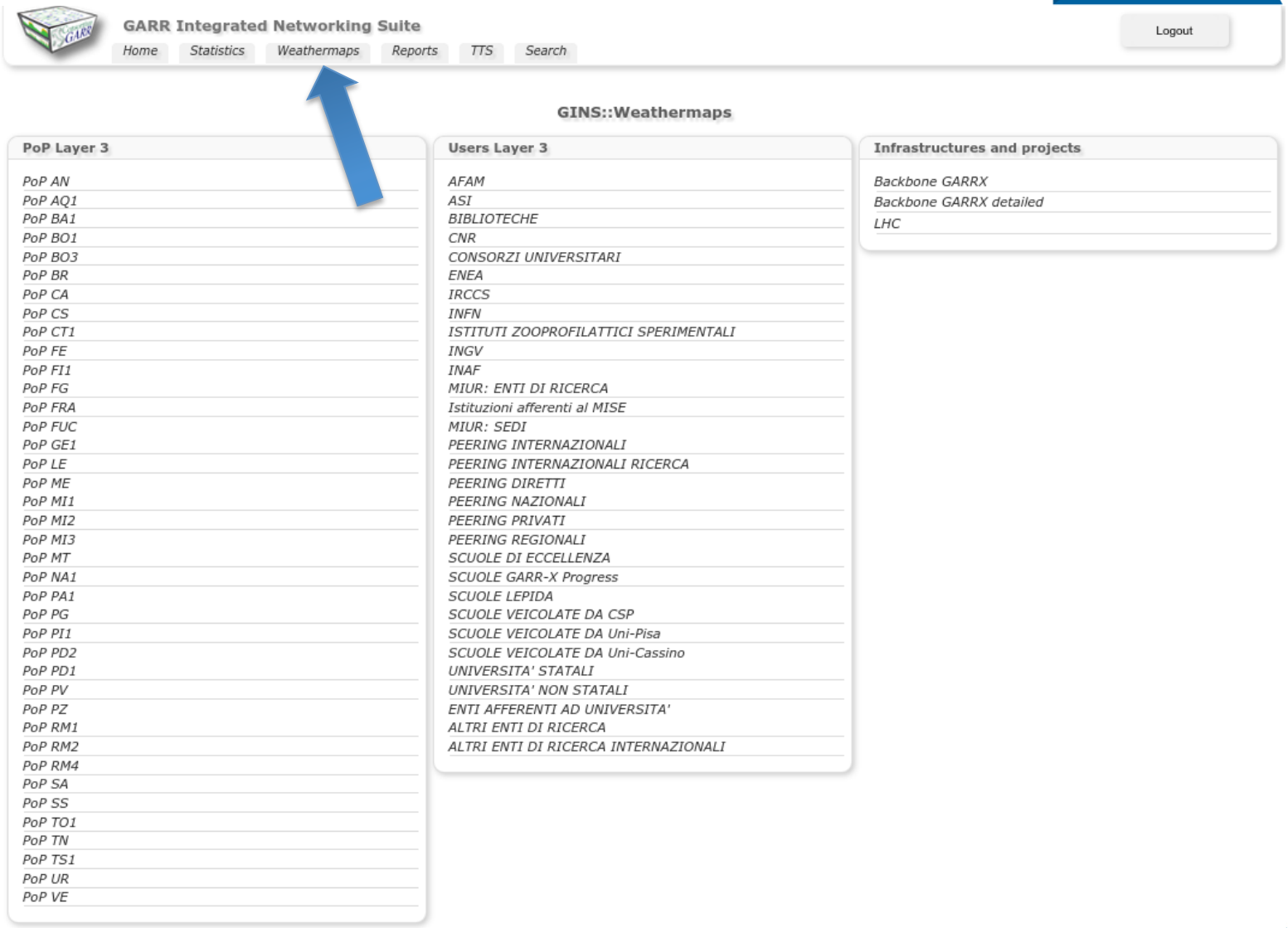


Evoluzione della connettivita’

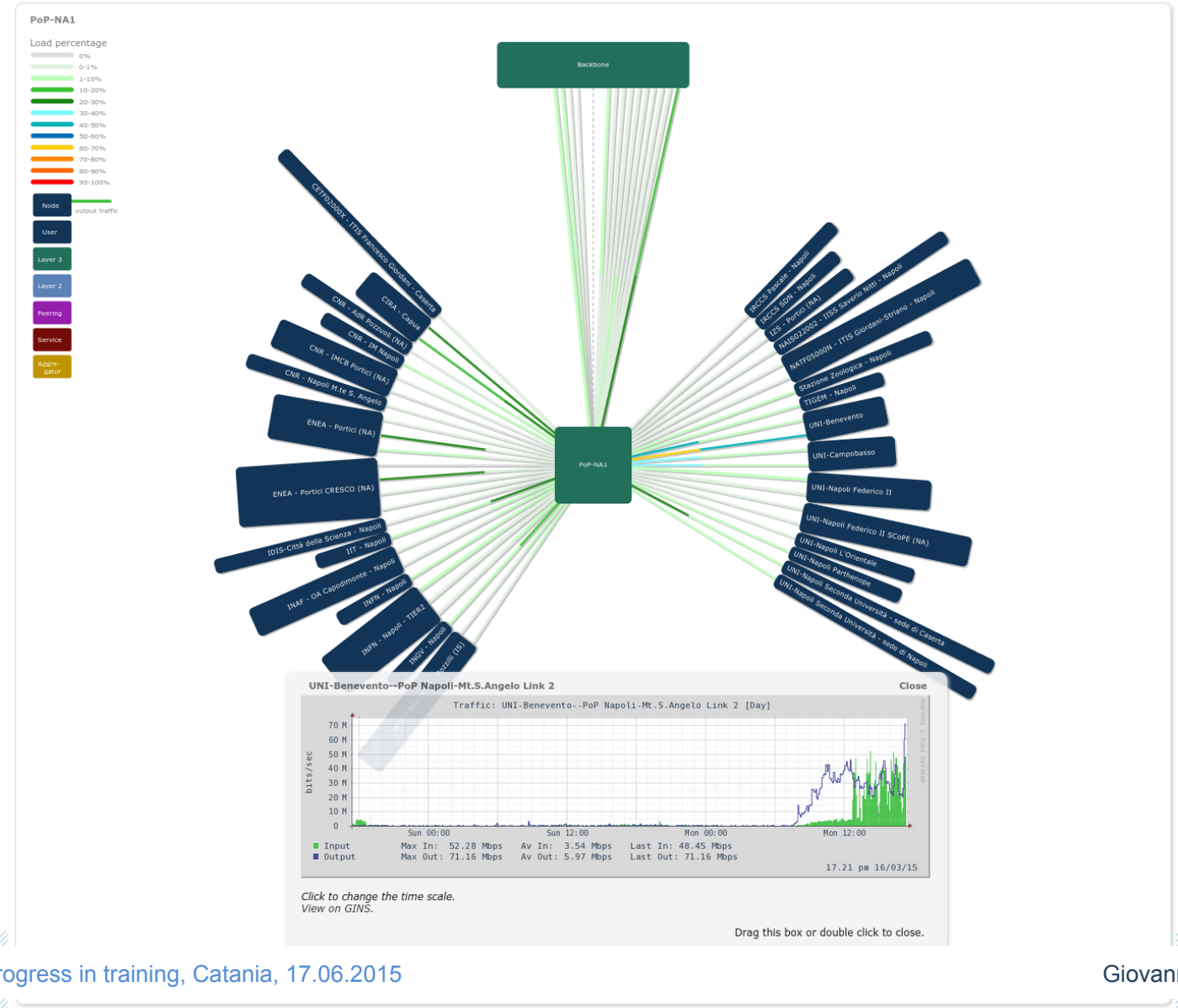




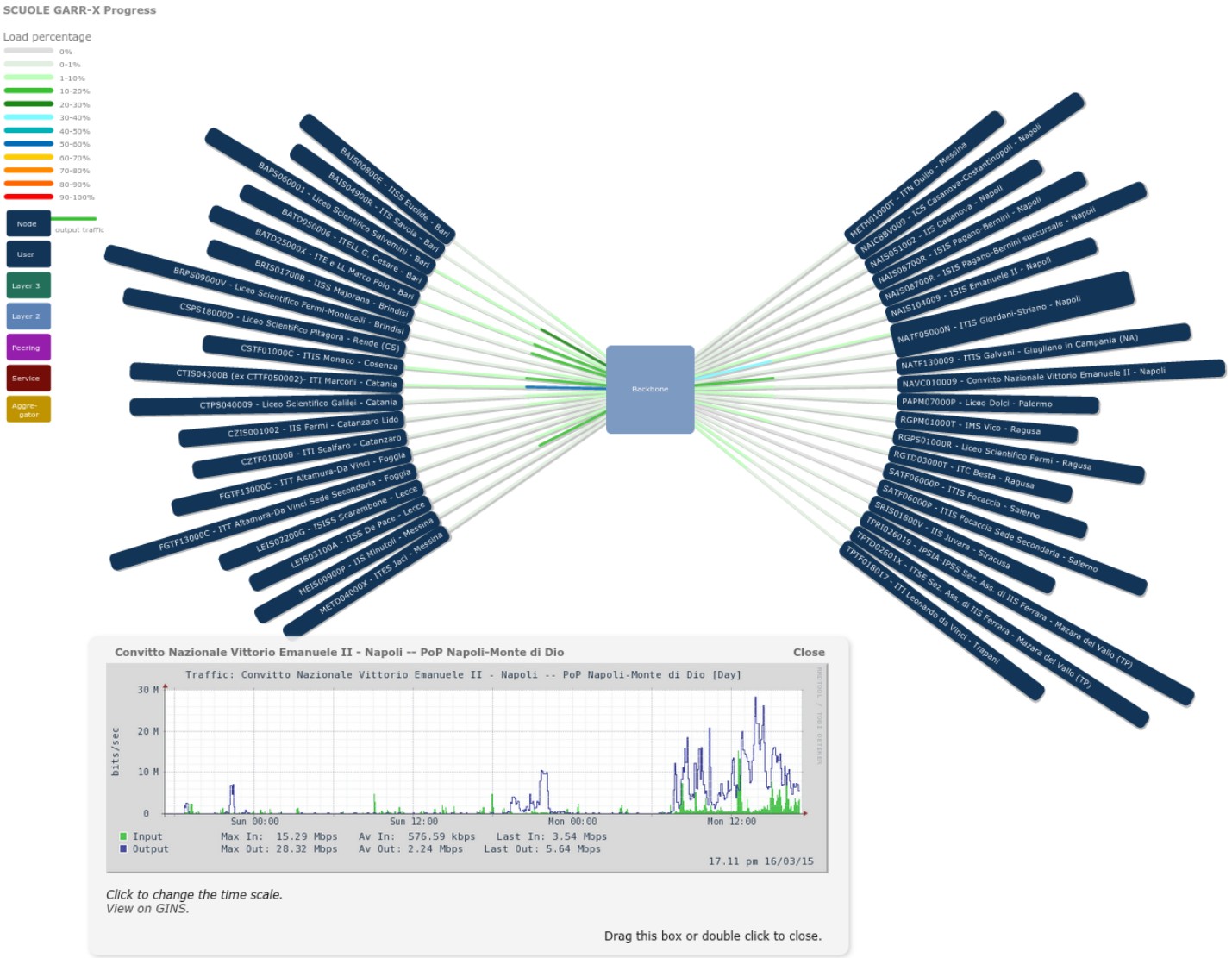
Weathermap


GARR Integrated Networking Suite
Home
Statistics
Weathermaps
Reports
TTS
Search
Logout
GINS::Weathermaps
PoP Layer 3
PoP AN
PoP AQ1
PoP BA1
PoP BO1
PoP BO3
PoP BR
PoP CA
PoP CS
PoP CT1
PoP FE
PoP FI1
PoP FG
PoP FRA
PoP FUC
PoP GE1
PoP LE
PoP ME
PoP MI1
PoP MI2
PoP MI3
PoP MT
PoP NA1
PoP PA1
PoP PG
PoP PI1
PoP PD2
PoP PD1
PoP PV
PoP PZ
PoP RM1
PoP RM2
PoP RM4
PoP SA
PoP SS
PoP TO1
PoP TN
PoP TS1
PoP UR
PoP VE
Users Layer 3
AFAM
ASI
BIBLIOTECHE
CNR
CONSORZI UNIVERSITARI
ENEA
IRCCS
INFN
ISTITUTI ZOOPROFILATTICI SPERIMENTALI
INGV
INAF
MIUR: ENTI DI RICERCA
Istituzioni afferenti al MISE
MIUR: SEDI
PEERING INTERNAZIONALI
PEERING INTERNAZIONALI RICERCA
PEERING DIRETTI
PEERING NAZIONALI
PEERING PRIVATI
PEERING REGIONALI
SCUOLE DI ECCELLENZA
SCUOLE GARR-X Progress
SCUOLE LEPIDA
SCUOLE VEICOLATE DA CSP
SCUOLE VEICOLATE DA Uni-Pisa
SCUOLE VEICOLATE DA Uni-Cassino
UNIVERSITA' STATALI
UNIVERSITA' NON STATALI
ENTI AFFERENTI AD UNIVERSITA'
ALTRI ENTI DI RICERCA
ALTRI ENTI DI RICERCA INTERNAZIONALI
Infrastructures and projects
Backbone GARRX
Backbone GARRX detailed
LHC

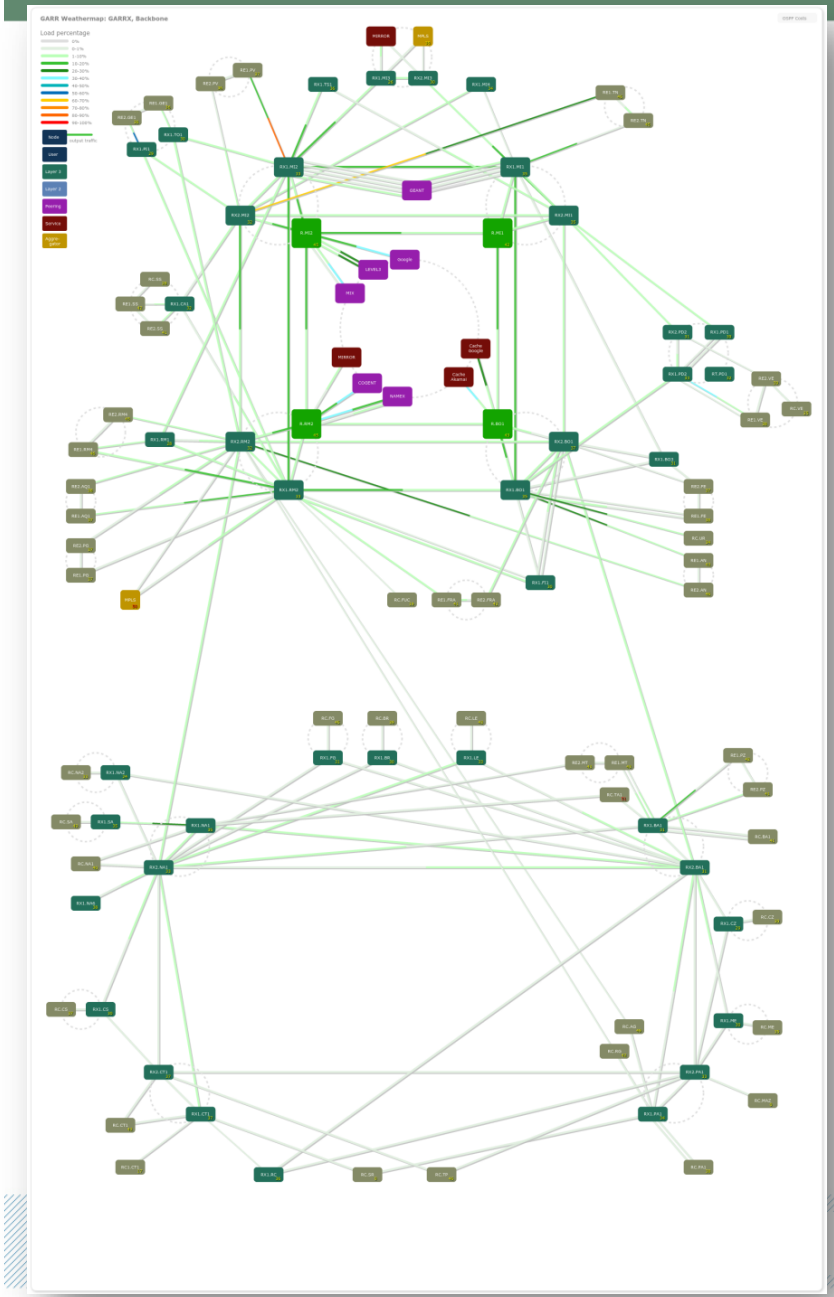
Weathermap: PoP Layer 3

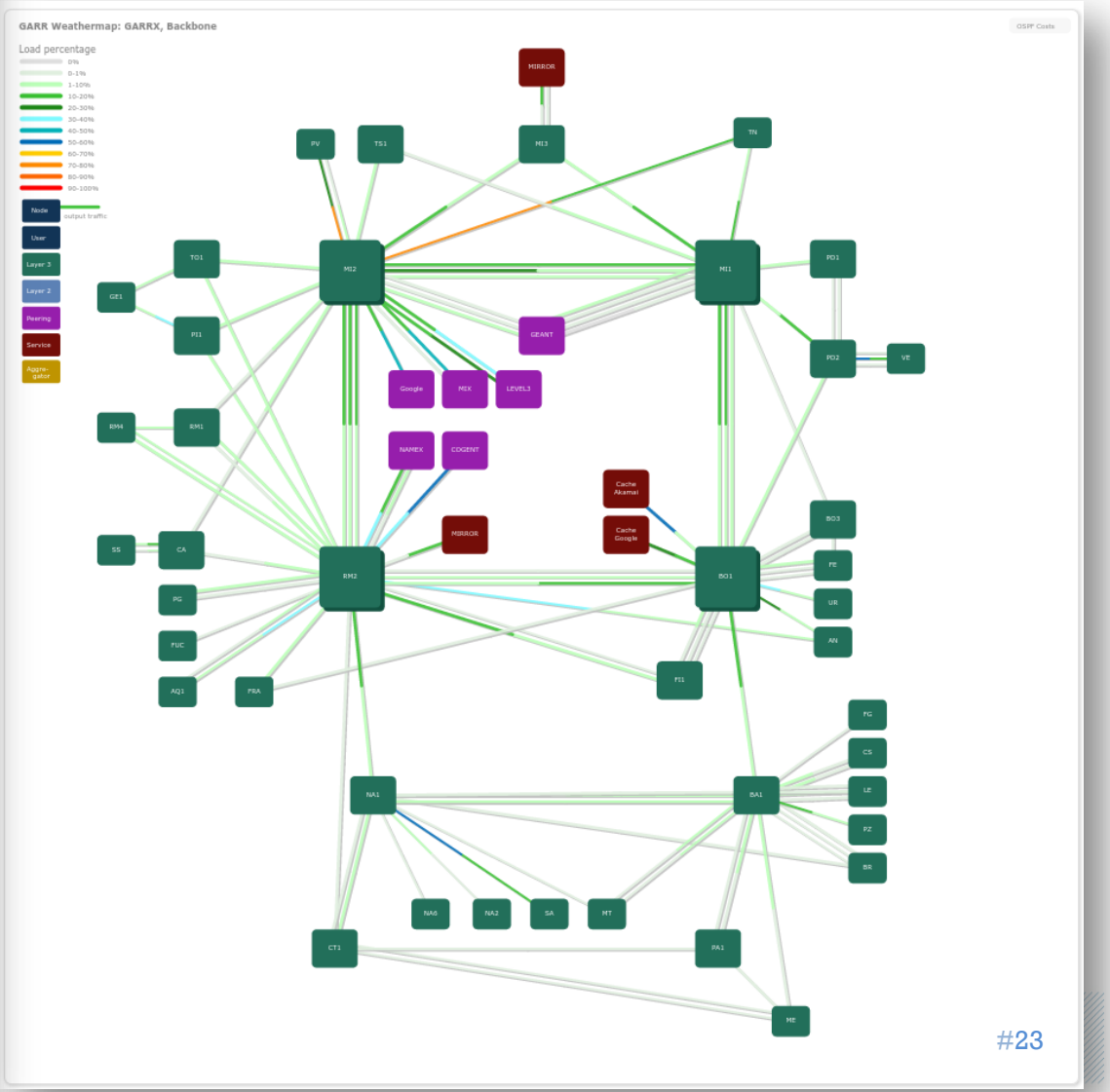


Weathermap: utenti



Weathermap: backbone





Statistiche di traffico

GINS

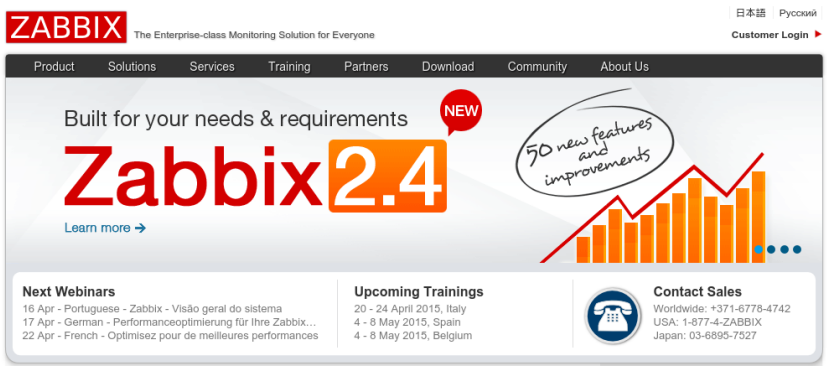
Frontend
Middleware
Backend

MRTG
MULTI ROUTER TRAFFIC GRAPHER

RRDtool
logging & graphing

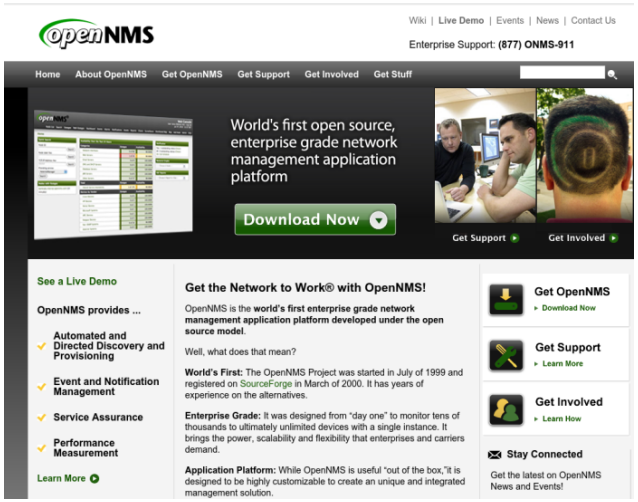
Backend

http://www.zabbix.com/



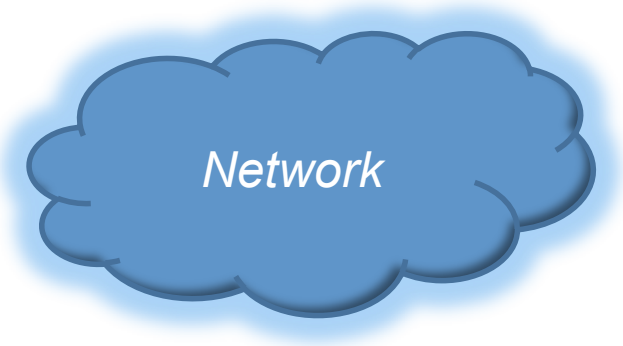
http://www.cacti.net/

http://www.opennms.org/



Tool di monitoring

- Cosa controlliamo:
  - Variazioni di traffico
  - Raggiungibilita' ICMP
  - Stato degli apparati e delle porte
  - Errori sulle interfacce
  - Stato degli LSP MPLS
  - Stato delle VPN L2/L3
  - Sessioni BGP e prefissi
  - Allarmi LACP, IMA
  - Allarmi Chassis specifici
  - Soglie temperature



Tool di monitoring

Actions: TTS | Show blacklist | Show history | Tools: eMon alarms [9-91] | BGP alarms [52] | IMA alarms [0] | LACP alarms [12] | MPLS alarms [5] | e2e alarms [0]

Alarms

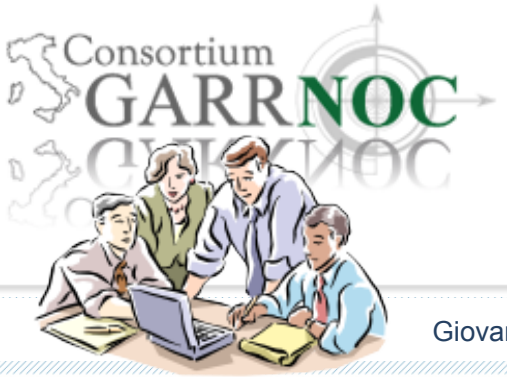
Chassis alarms: ok

Users links

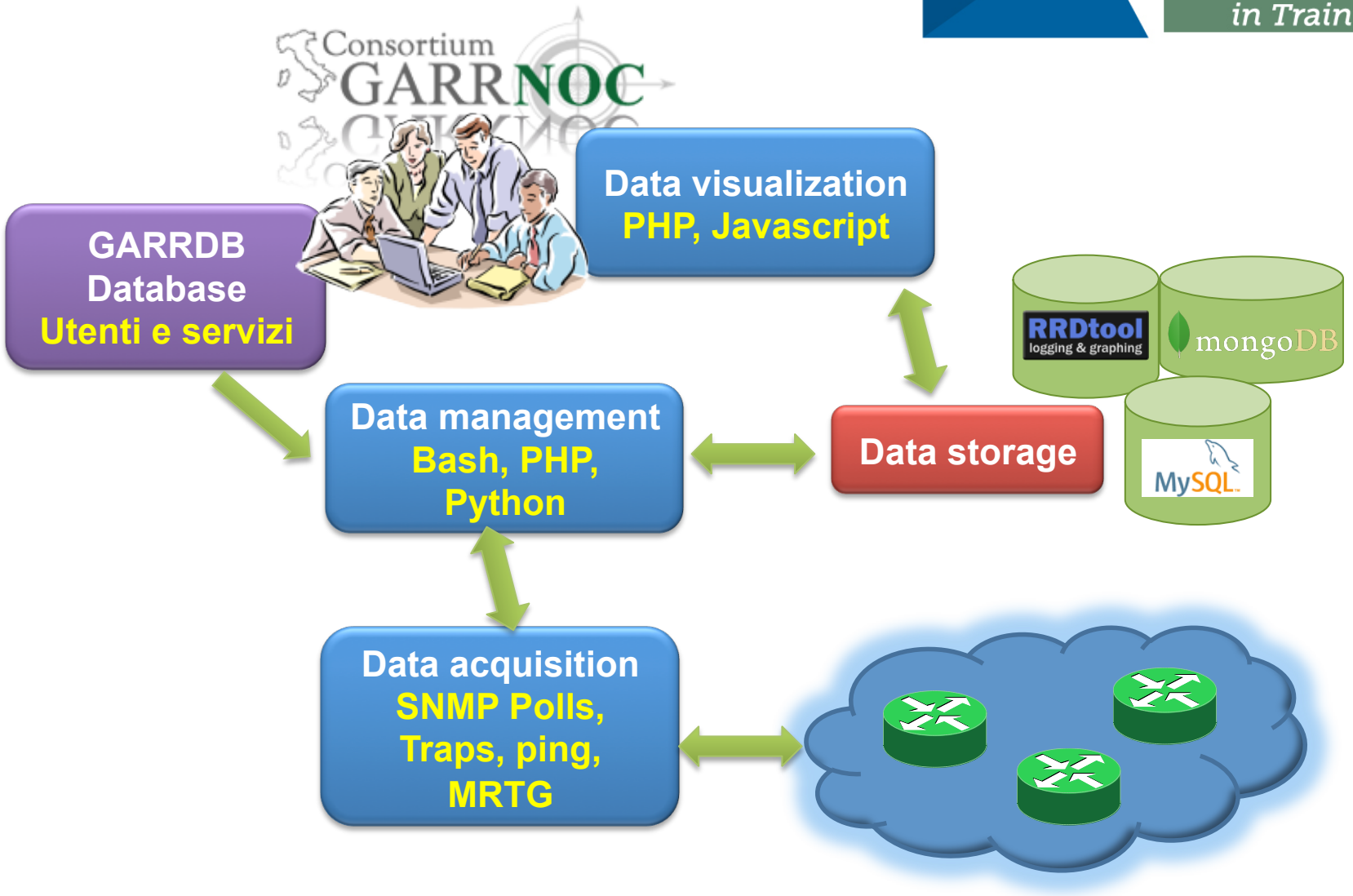
Id	Name	Date	Router interface	IP	I/O	Pg	eM	Tr	St	St	Hi	BL	TBL	TTS
5294	CINECA-PRACE - Casalecchio di Reno (BO) -- PoP Milano-Lancetti	17/03/2015 18:07	rx1.mi1.garr.net xe-1/0/0.0	10.31.1.122	1.6 1.83					+	+	+	+	New
5504	Liceo Scientifico Vercelli - Asti -- CSP Torino	17/03/2015 14:58	rx1.to1.garr.net xe-0/0/0.117		0 0					+	+	+	+	New
4923	Registro ccTLD.it -- PoP Pisa-Torricelli	14/03/2015 23:22	rx1.pi1.garr.net ae7.13	193.206.136.58	185.36 1.07					+	+	+	+	15674 bataloni 13/03 14:54 Lorenzo Rossi: disattivato la sessione BGP IPv4 tra l'AS2597 e l'AS137. Stiamo rivedendo tutta la nostra architettura di rete in seguito ad alcuni problemi che abbiamo sperimentato. In questo transitorio vorrei mantenere down il transito IPv4 con l'AS137 al fine di semplificare l'analisi di alcune situazioni. 15674 bataloni 13/03 14:54 Aperto ticket
4972	ITST Fermi - Frascati -- PoP Roma Tiziì	13/03/2015 14:49	rx1.rm2.garr.net ge-2/3/7.640	193.206.131.30	0.27 0.23					+	+	+	+	New
3395	e2e FEDERICA GARR-PSNC	10/03/2015 09:37	sw01.mil.it.net.fp7-federica.eu ge-0/0/0.0	194.132.52.86	0 0.19					+	+	+	+	15662 dambrosio 10/03 12:23 Problem with one of switches where these FEDERICA lines are terminated, due to power outage.
4193	ENEA - Frascati -- PoP Frascati-Fermi backup	09/03/2015 08:40	re2.fra.garr.net ge-1/1/3.923	193.206.136.194	0.27 0.05					+	+	+	+	15656 pellegri 09/03 08:56 volevo avvisarvi che a breve spegneremo il router di backup della sede ENEA Frascati per permettere l'inserimento e i test di un nuovo firewall. La valutazione durera' qualche giorno, per cui si prevede di riaccendere il router di backup il prossimo mese.
5441	NATO M&S COE - Roma -- PoP Roma-Sapienza backup	17/02/2015 12:00	rx1.rm1.garr.net ge-11/2/9.623	193.206.132.166	0.38 0.2					+	+	+	+	15591 dambrosio 17/02 16:14 Contattato APM per richiesta abilitazione ICMP
5644	SSBAR - Roma - Terme di Diocleziano -- PoP Roma-Tiziì	27/01/2015 12:07	rx2.rm2.garr.net ge-4/3/2.647	193.204.217.214	0.27 0.09					+	+	+	+	15535 dambrosio 27/01 14:57 In attesa dell'installazione del router in sede utente

Legenda:

Id	URI database
In, Out	traffico in Kbps
Stat	verifica stato dell'acquisizione delle statistiche - URI statistiche
Ping	esito del ping
eMon	verifica stato della porta fisica da eMon
Trap	verifica l'arrivo di trap LINK_DOWN nell'ultima ora da TrapMon
Aggr Traf	verifica traffico aggregato dei link - URI statistiche aggregate
Colori esito test:	negativo positivo non attivo
BL	manda in blacklist
TBL	manda in blacklist temporaneamente (1 ora)



GINS architettura



Come monitorare la rete

- Interrogare gli apparati



SNMP poll

- Ascoltare gli eventi generati dagli apparati



SNMP trap

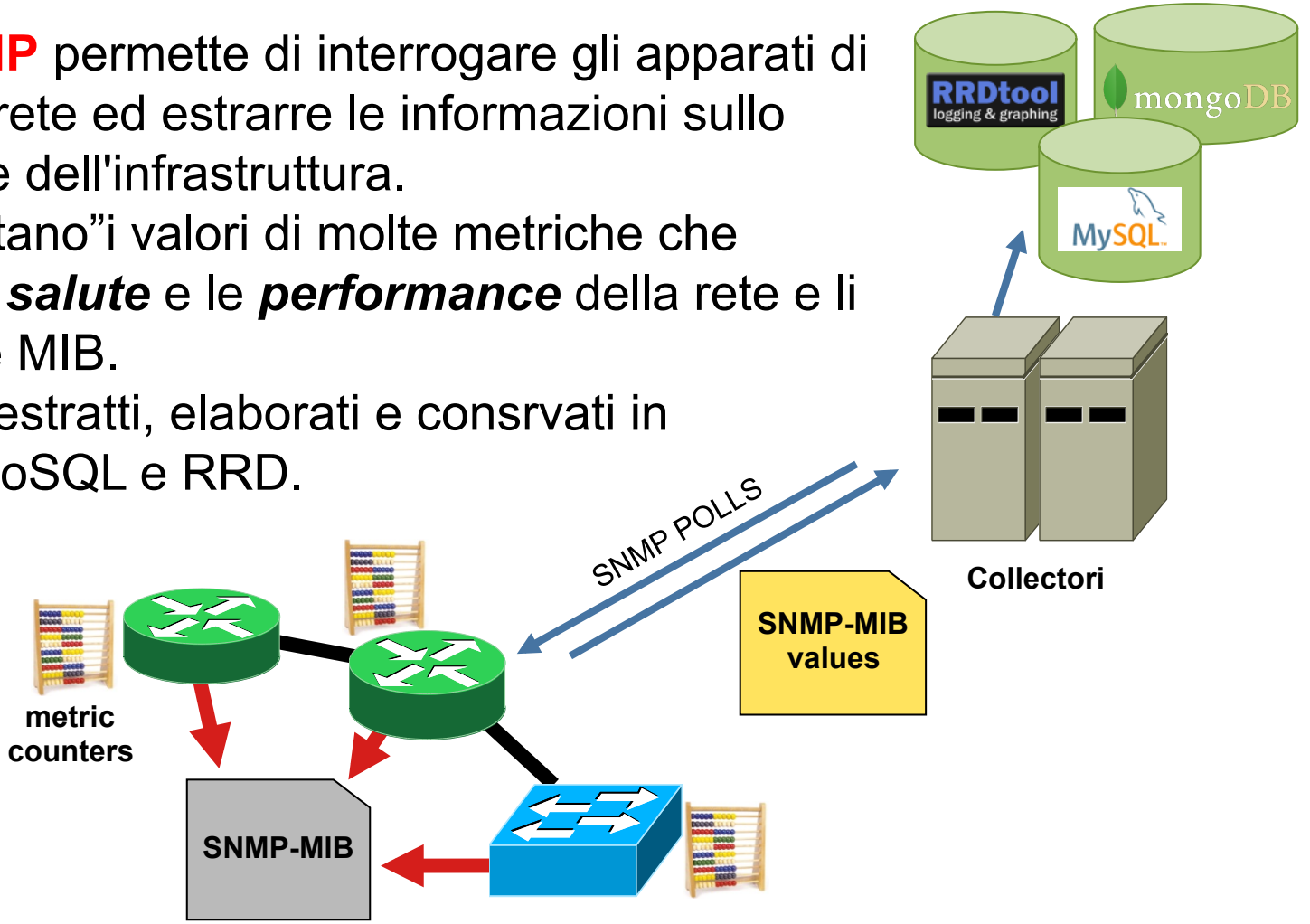
- Misurare le prestazioni



Active measuring

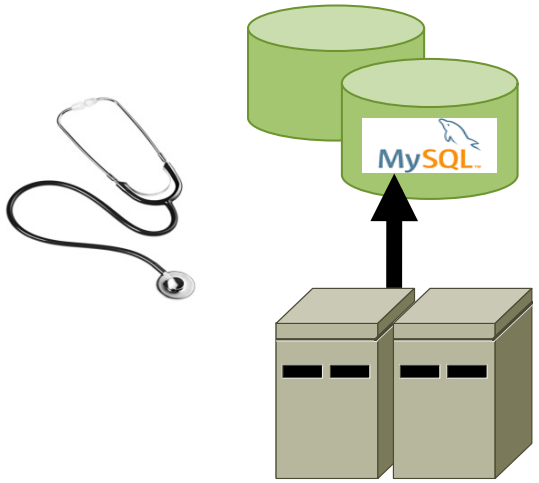
Interrogare la rete: SNMP Poll

Il protocollo **SNMP** permette di interrogare gli apparati di ogni livello della rete ed estrarre le informazioni sullo stato dei servizi e dell'infrastruttura.
Gli apparati “contano”i valori di molte metriche che caratterizzano la ***salute*** e le ***performance*** della rete e li conservano nelle MIB.
I valori vengono estratti, elaborati e consrvati in database SQL, noSQL e RRD.

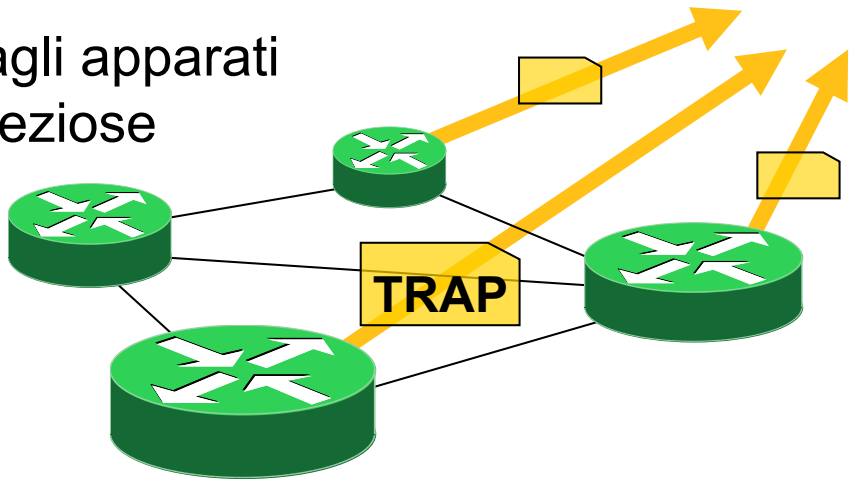


Ascoltare la rete: SNMP Trap

Le TRAP SNMP sono dei messaggi generati dagli apparati al verificarsi di ***eventi critici***.
Vengono “tradotti” e collezionati per poi essere analizzati.
Gli eventi possono riguardare il fault di apparati o di servizi, ma anche il superamento di soglie (es. Temperature, livelli ottici).
Vengono inviate direttamente dagli apparati di rete, fornendo informazioni preziose quando si presenta un problema in rete, prima che gli altri sistemi se ne accorgano.



Collettori



Ascoltare la rete: SNMP Trap

- Cosa ascoltare:
  - Approccio mirato:

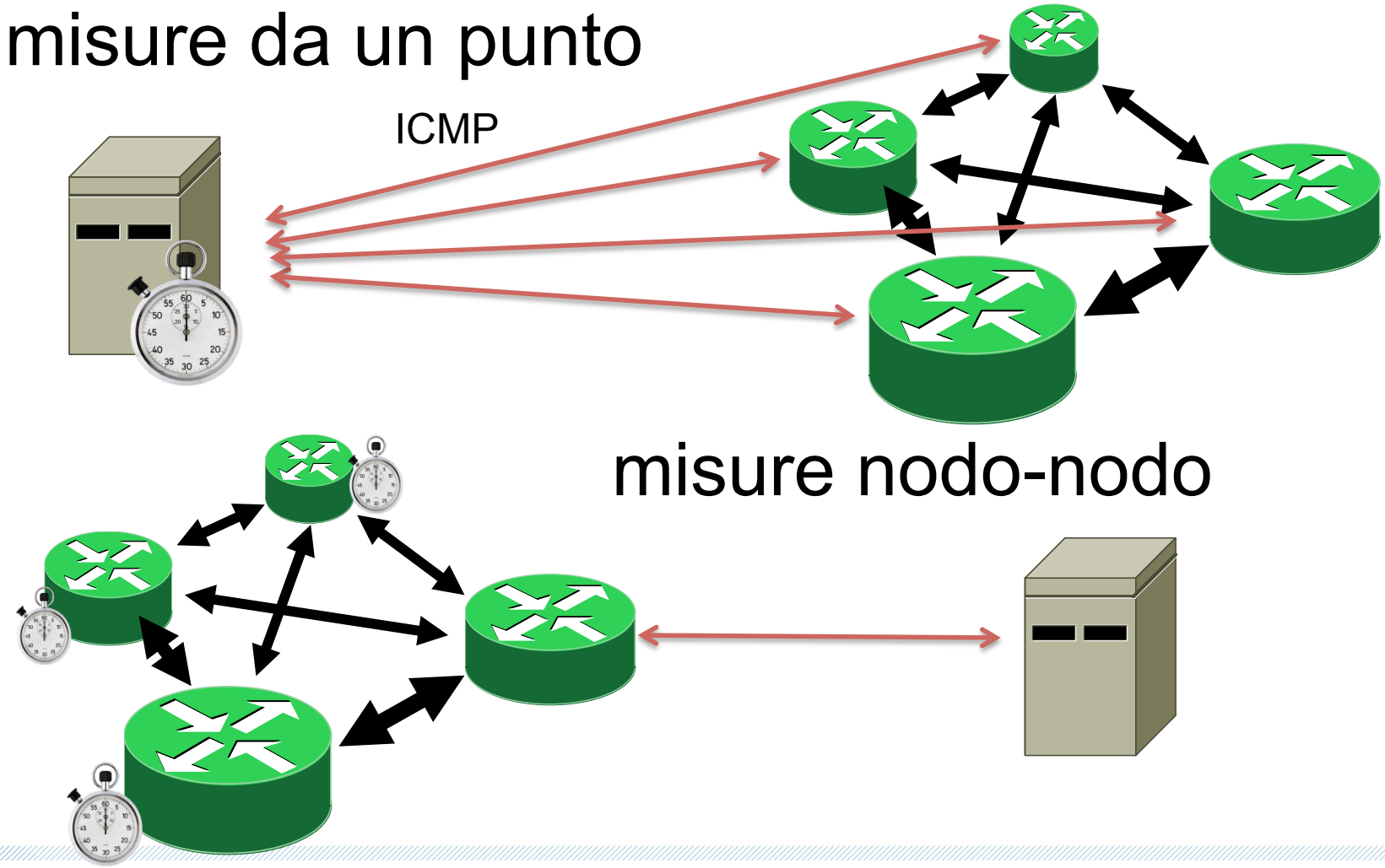
    configurare apparati per inviare Trap per eventi specifici
  - Approccio aperto e complesso:

    inviare tutto, classificare, analizzare

```
trap-group space {
    categories {
        authentication;
        chassis;
        link;
        routing;
        startup;
    }
}
```

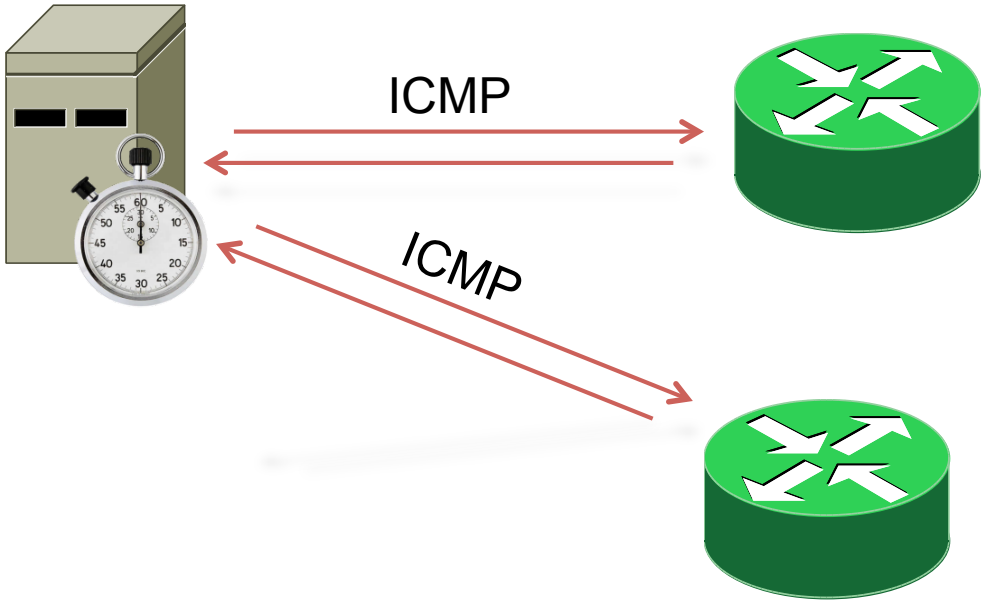
- Come ascoltare:
  - Snmptrapd
  - Event driven tools, esempio nodejs (LAB)

Latency



Latency

- Misura da un punto

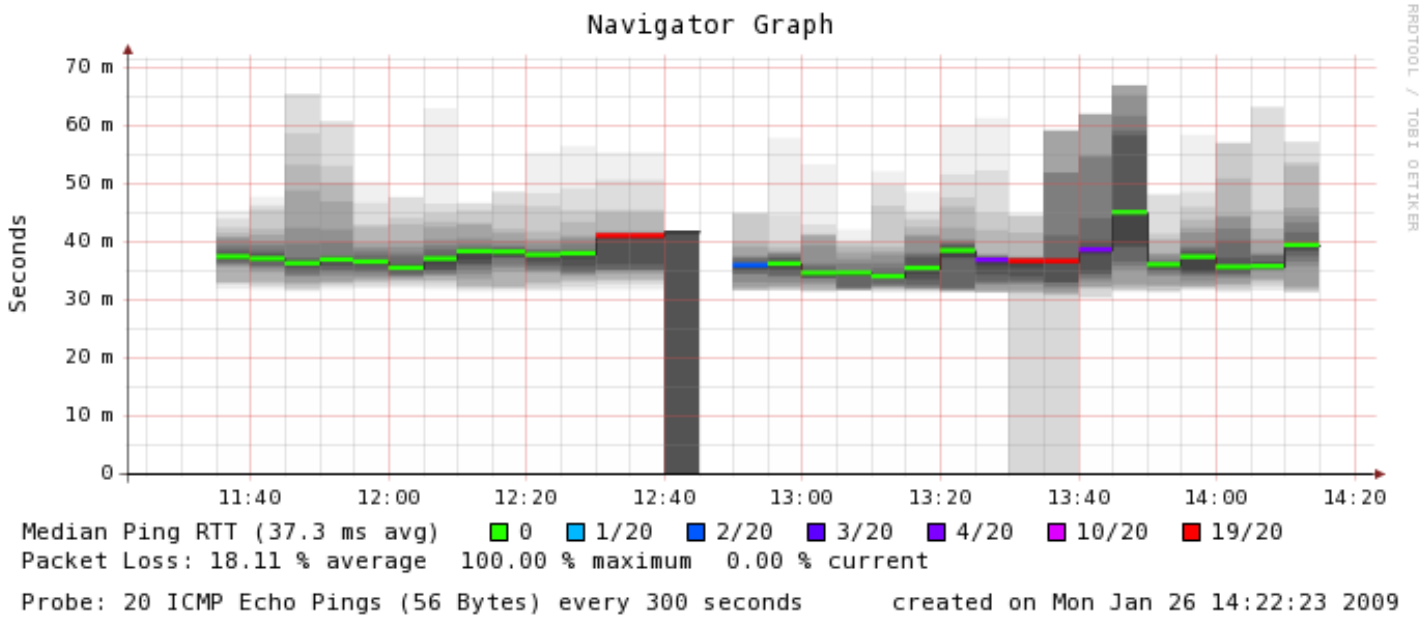


Tool scelto:

smokeping

http://oss.oetiker.ch/smokeping/

Latency



- Round Trip Time fluctuations
- Packet Loss pecentage

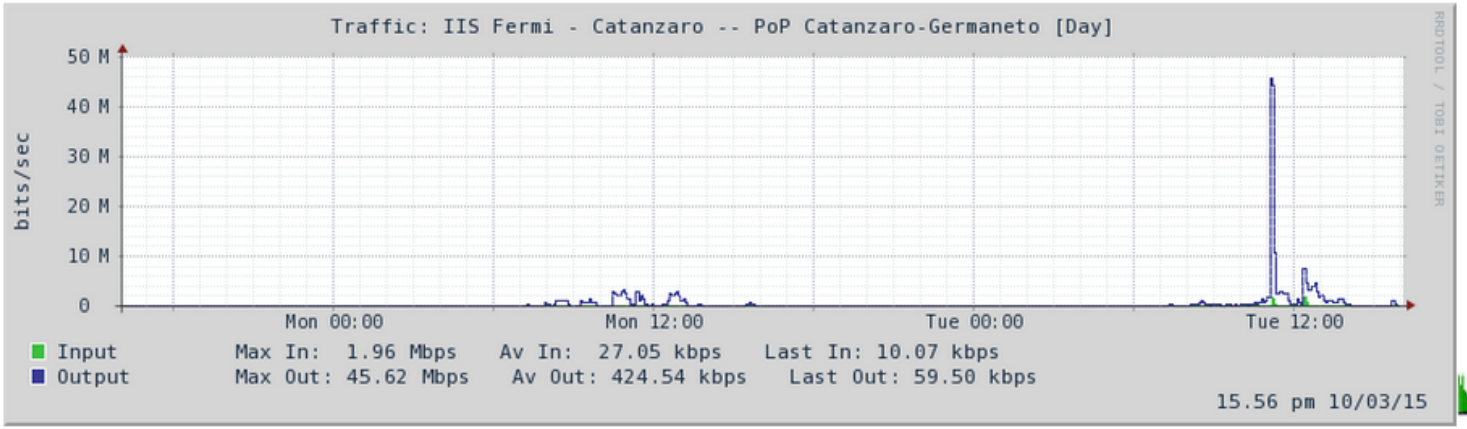
Latency

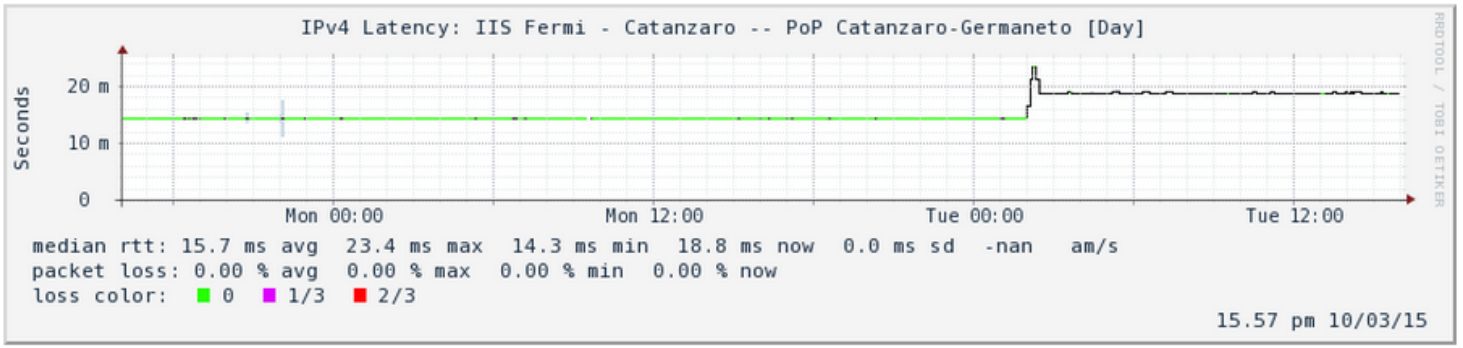
Statistiche di traffico

Time scale: *Day* *Week* *Month* *Year* *5 Year* Metrics: *IPv6* *Latency* *Traffic sum* Actions: *Set as default* *Get this url*

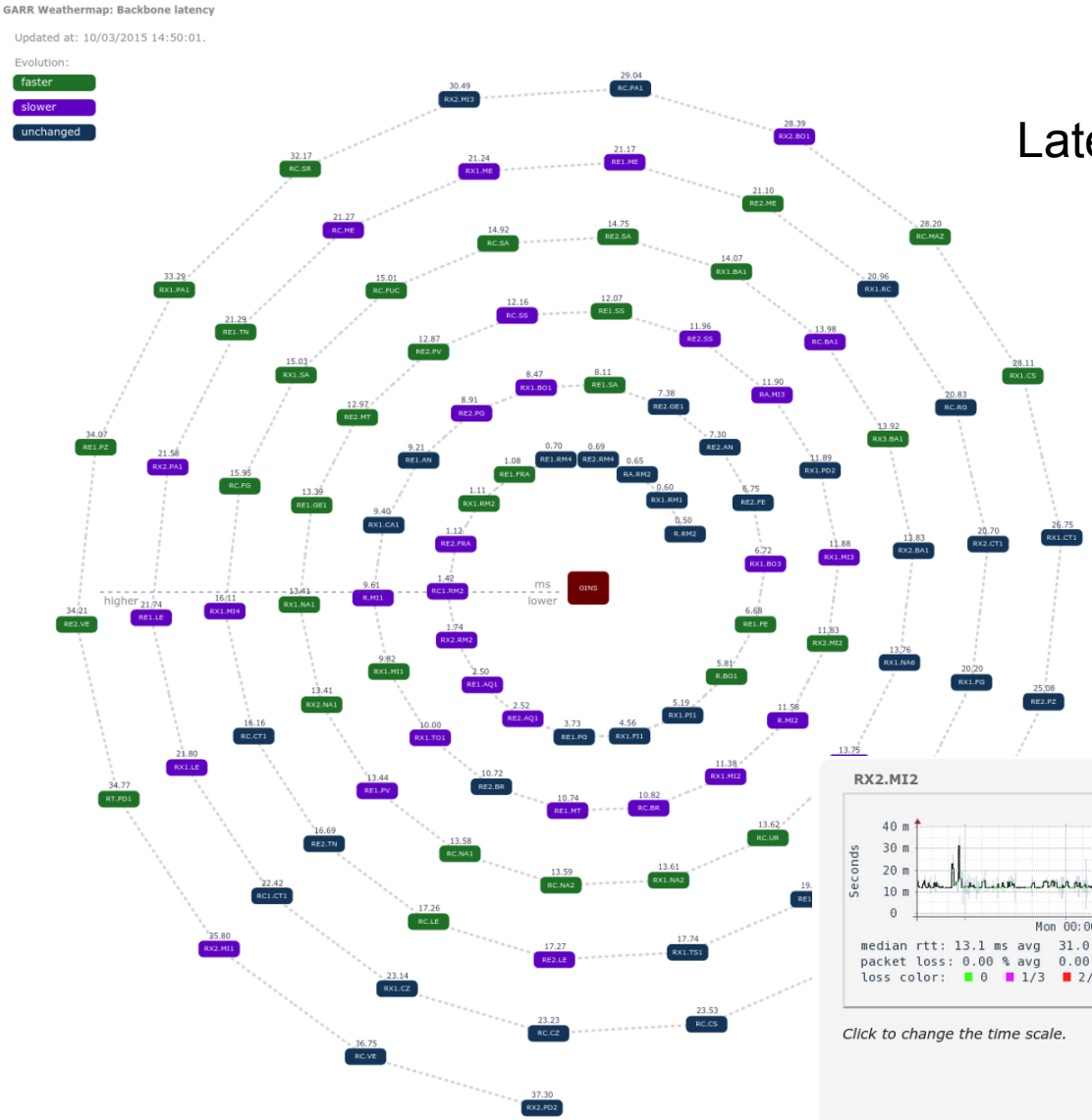
IIS Fermi - Catanzaro -- PoP Catanzaro-Germaneto close

Link Type	Equipment B	Interface B	IPv4 Address	IPv6 Address	Equipment A	Interface A
DF 100Mbps FE	rc.cz.garr.net	Gi0/1	193.204.93.177		rc-cz-ru-isfermi-cz.cz.garr.net	

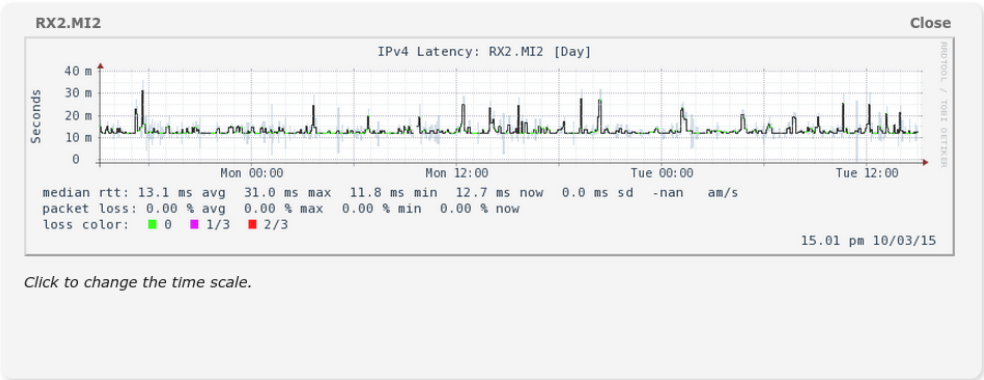




Latency



Latenza della rete vista da GINS

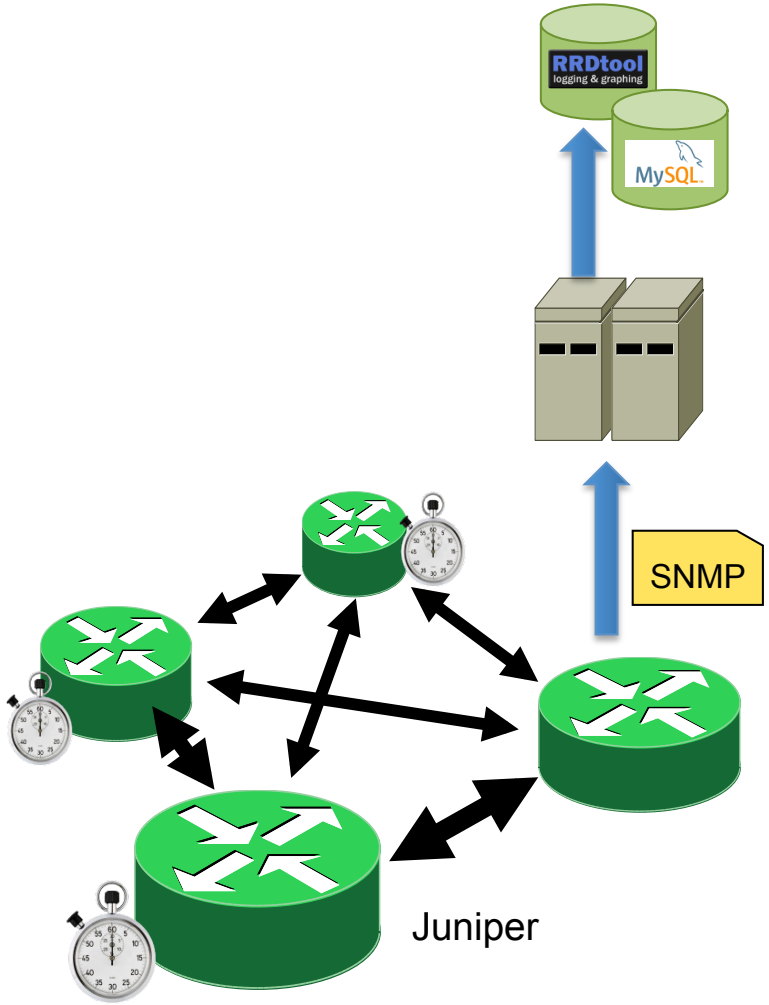


Latency

- Misura nodo-nodo

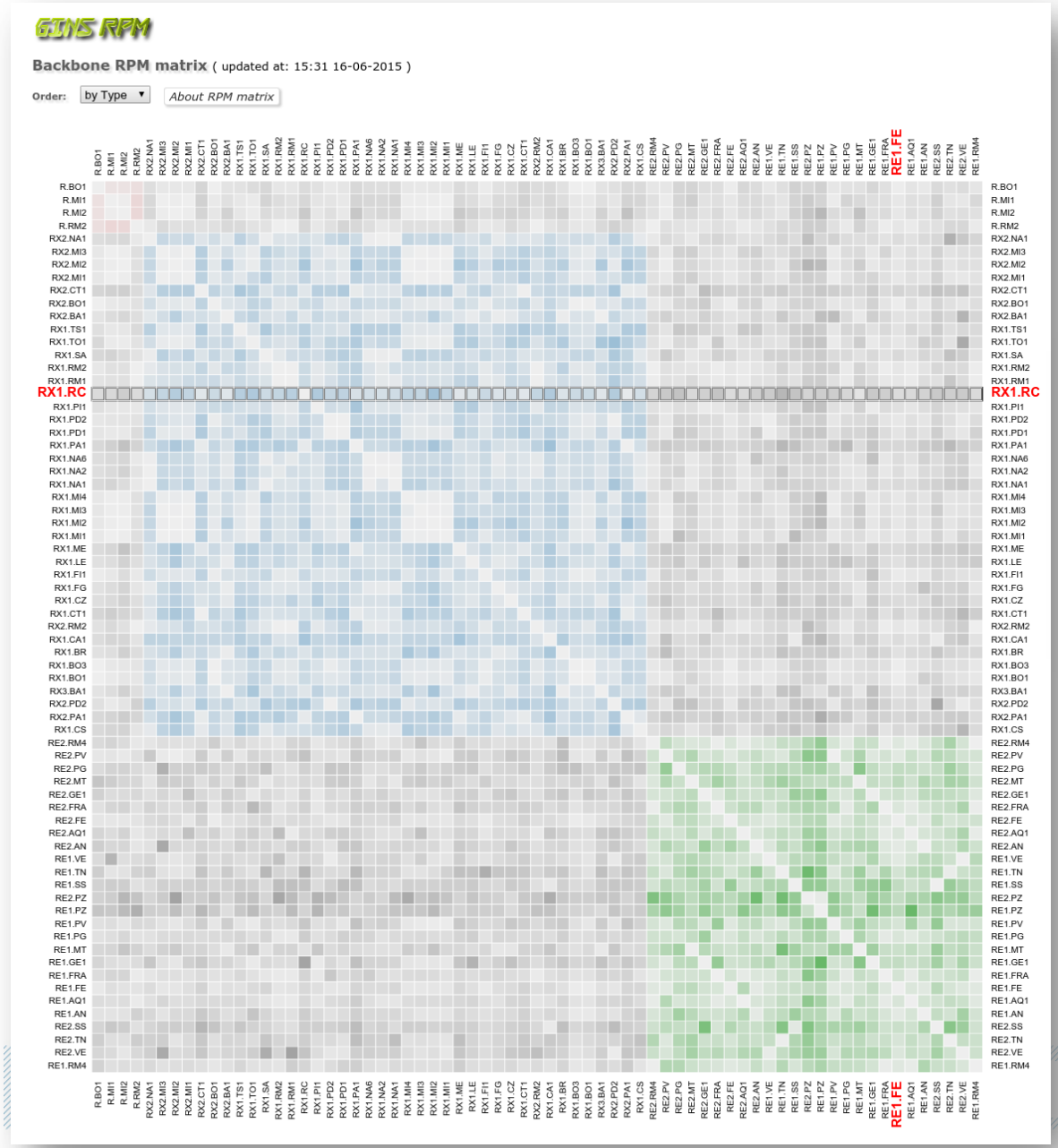
I router Juniper sono dotati di un sistema di misura attivo delle performance distribuito, basato sulla tecnologia RPM (Real-Time Performance Monitoring).

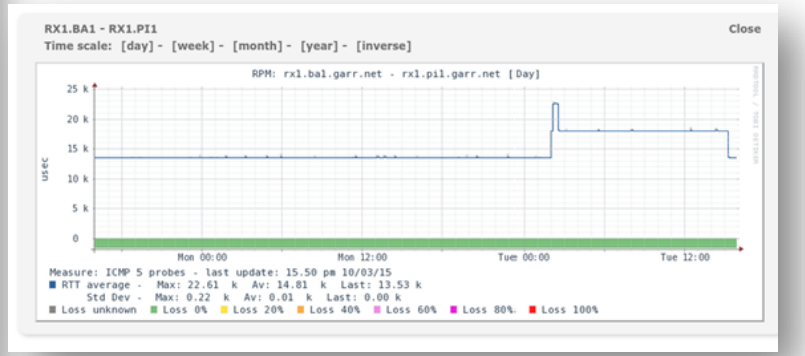
Permette di misurare la latenza della rete tra due nodi qualsiasi anche a livello applicativo.



Latency

https://gins.garr.it/RPM/rpm_matrix.php





Latency

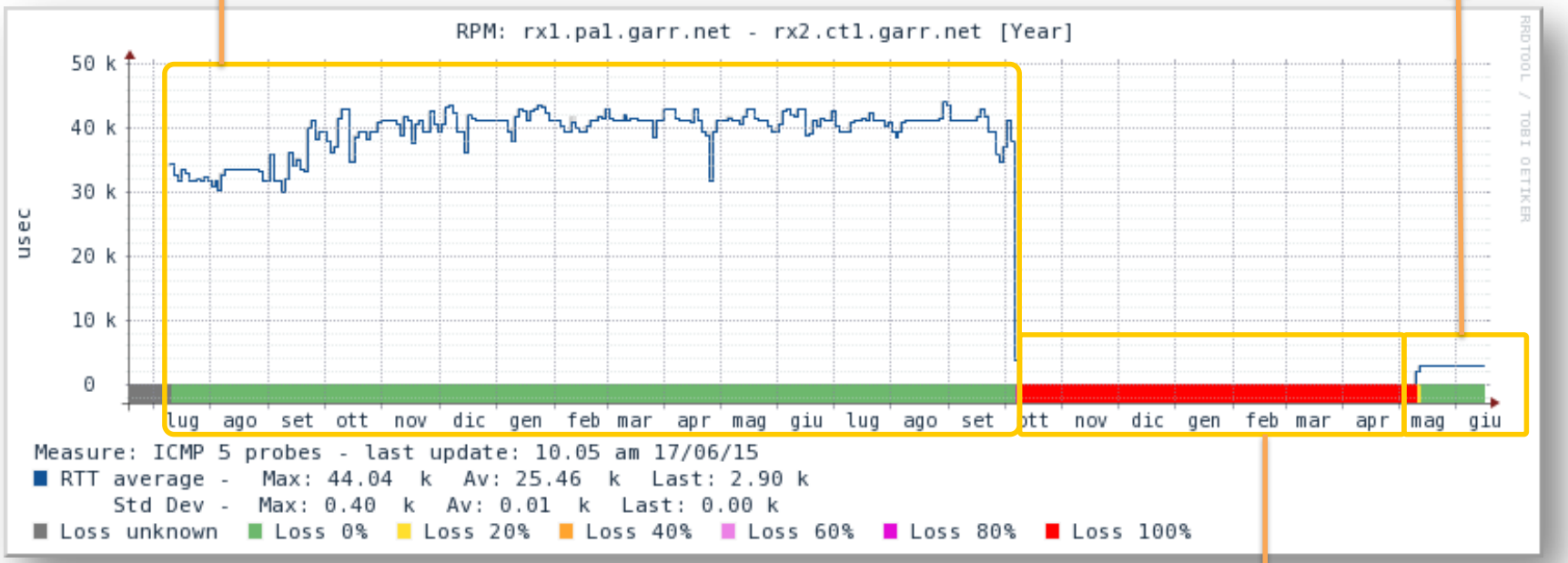
Latenza Palermo - Catania

Prima di GARRX-Progress

~40ms

Ora

~3ms

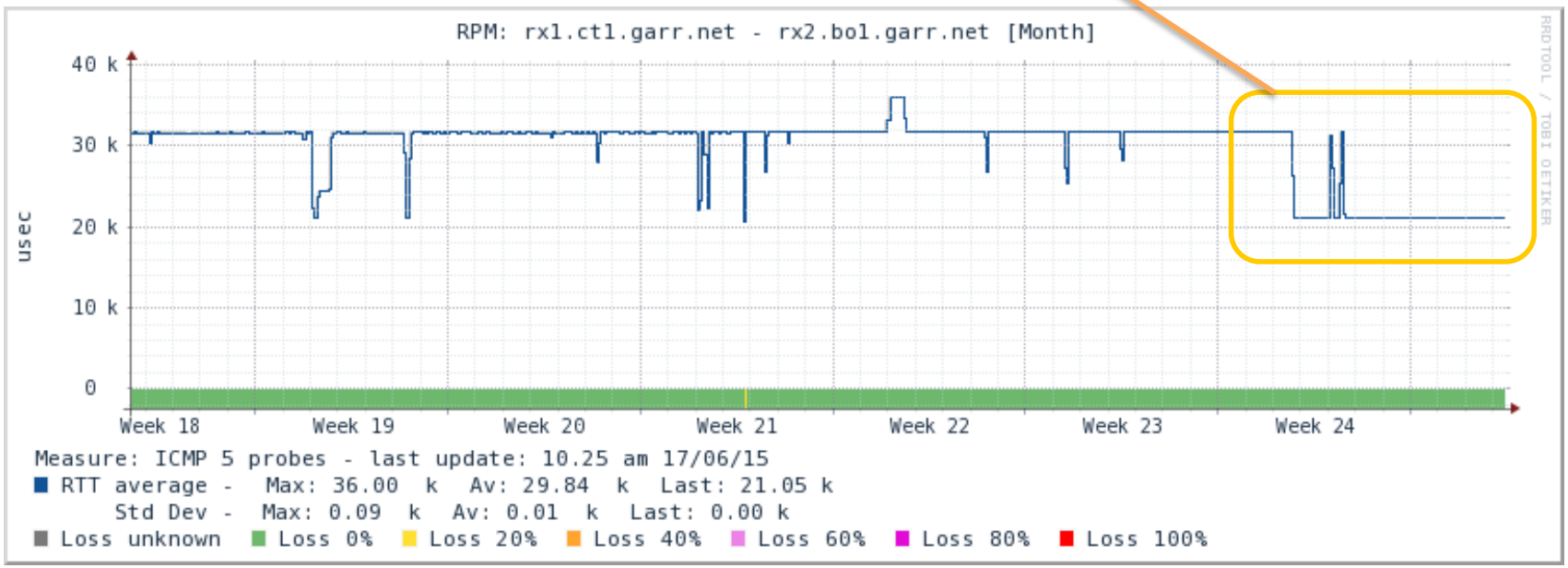


altro circuito

Latency

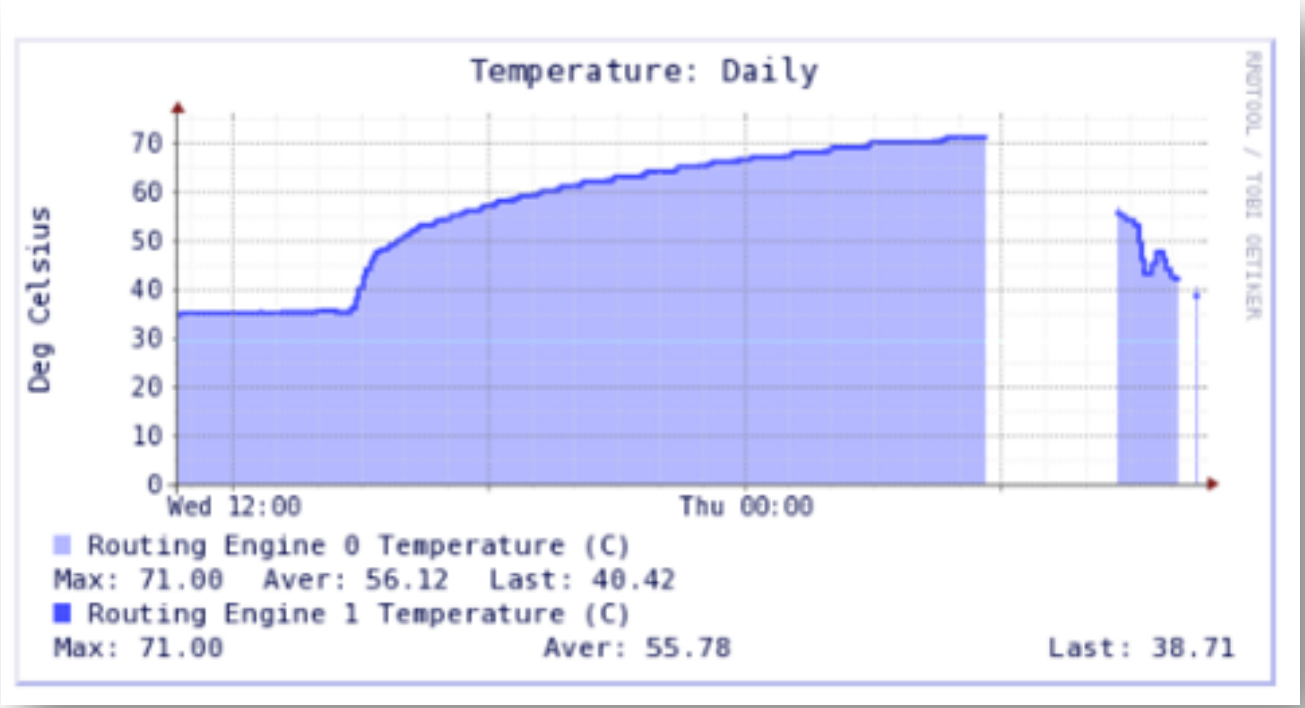
Latenza Catania

Ottimizzazione del trasporto sulla rete ottica



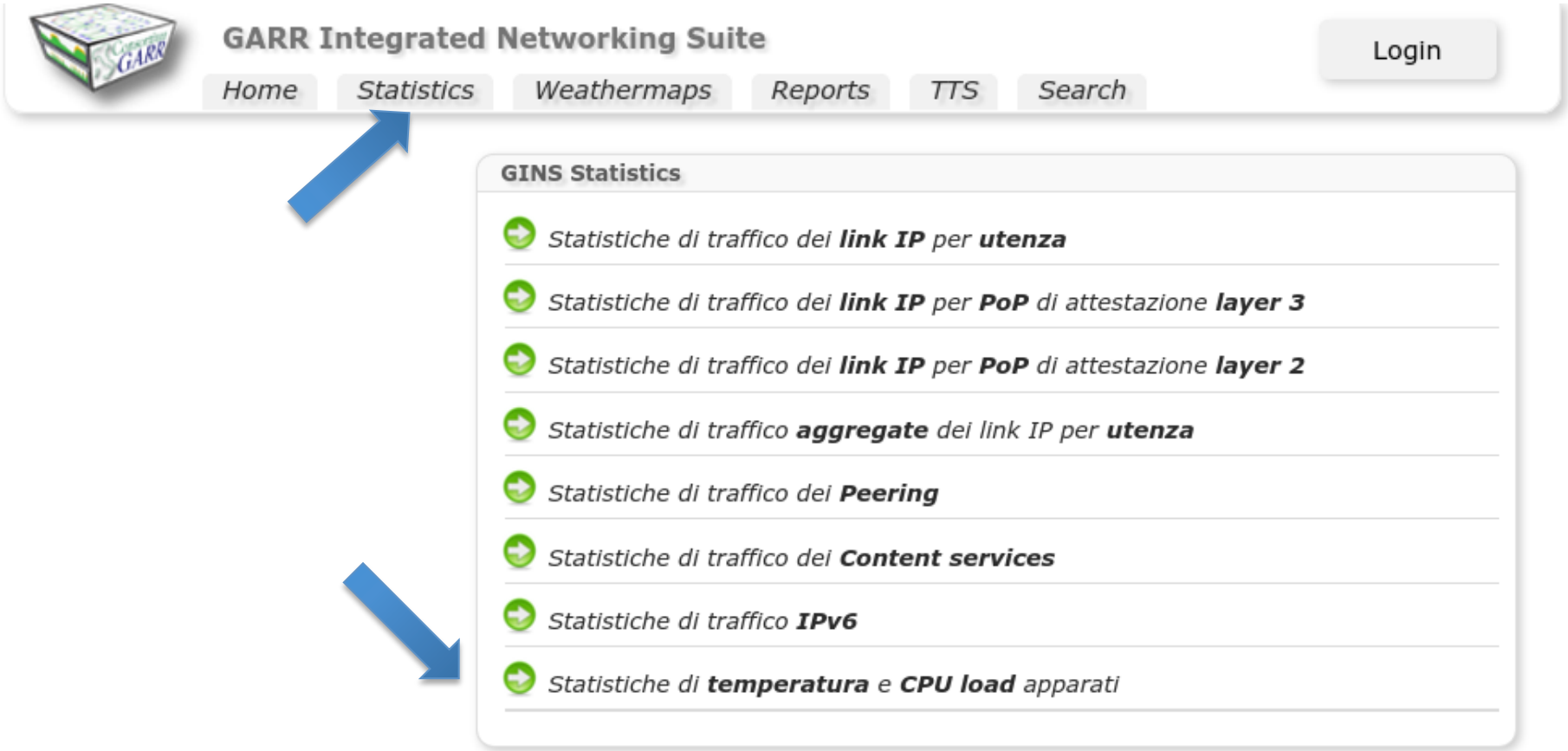
Temperature

Da evitare:



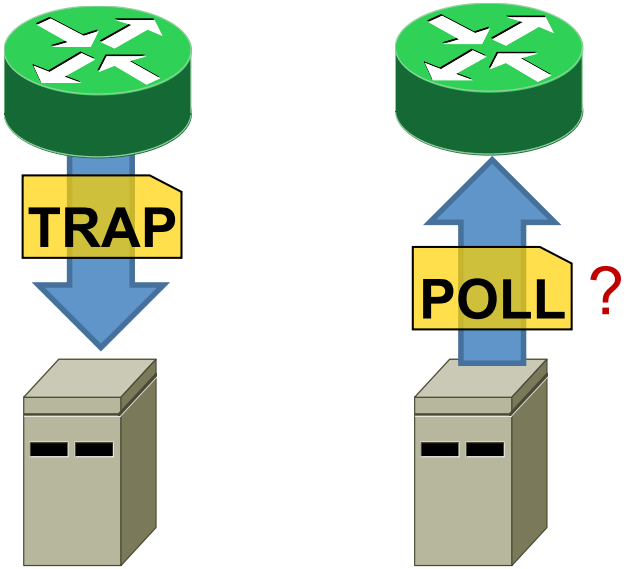
Temperature

Dove trovarle?



Temperature

- Un apparato di rete ha tante temperature
- Le MIBs sono proprietarie
- Le soglie di allarme non sono sempre di facile intrpretazione



OK, se arriva

> show chassis temperature-thresholds

	Fan speed		Yellow alarm		Red alarm	
Item	Normal	High	Normal	Bad fan	Normal	Bad fan
Chassis default	48	54	65	55	75	65
Routing Engine 0	70	80	95	95	110	110
Routing Engine 1	70	80	95	95	110	110
FPC 0	55	60	75	65	90	80
FPC 1	55	60	75	65	90	80
FPC 2	48	54	70	60	80	70
FPC 3	48	54	70	60	80	70
FPC 4	48	54	70	60	80	70
FPC 5	48	54	70	60	80	70
FEB 0	48	54	70	60	80	72
FEB 1	48	54	70	60	80	72
FEB 2	48	54	70	60	80	72
FEB 3	48	54	70	60	80	72
FEB 4	48	54	70	60	80	72
FEB 5	48	54	70	60	80	72

Temperature

```
> show chassis temperature-thresholds
                     Fan speed      Yellow alarm          Red alarm
Item                 Normal  High   Normal  Bad fan       Normal  Bad fan
Chassis default      48      54     65      55            75      65
Routing Engine 0     70      80     95      95            110     110
Routing Engine 1     70      80     95      95            110     110
FPC 0                55      60     75      65            90      80
FPC 1                55      60     75      65            90      80
FPC 2                48      54     70      60            80      70
FPC 3                48      54     70      60            80      70
FPC 4                48      54     70      60            80      70
FPC 5                48      54     70      60            80      70
FEB 0                48      54     70      60            80      72
FEB 1                48      54     70      60            80      72
FEB 2                48      54     70      60            80      72
FEB 3                48      54     70      60            80      72
FEB 4                48      54     70      60            80      72
FEB 5                48      54     70      60            80      72
```

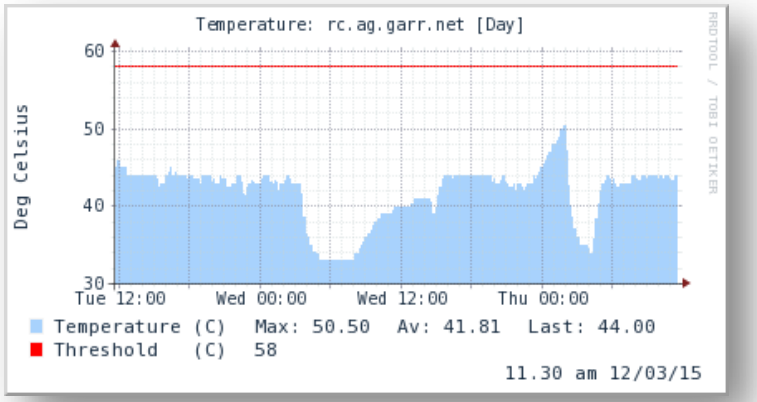
Raffreddamento OK

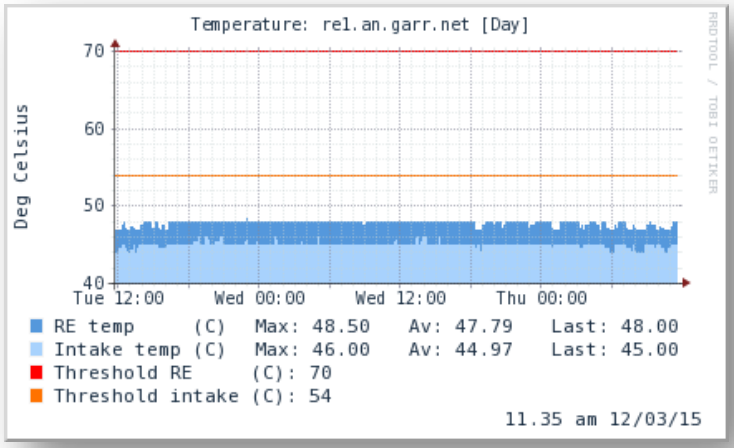
Raffreddamento ridotto

La soglia di temperatura a cui viene generato un allarme e' funzione della capacita' di raffreddamento dell'apparato

Temperature

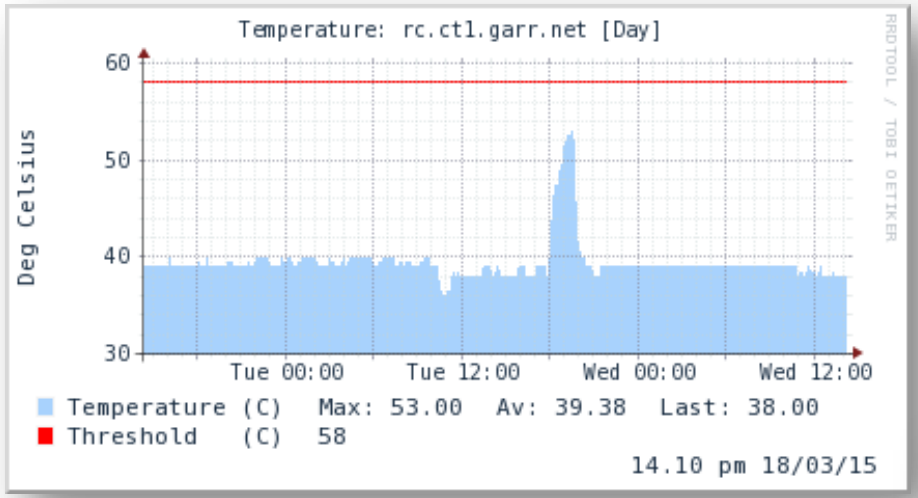
- Cisco
  - temperatura (1.3.6.1.4.1.9.9.13.1.3.1.3.<index>)
    CISCO-ENVMON-MIB::ciscoEnvMonTemperatureStatusValue
  - soglia (1.3.6.1.4.1.9.9.13.1.3.1.4.<index>)
    CISCO-ENVMON-MIB::ciscoEnvMonTemperatureThreshold
- Juniper
  - temperatura (1.3.6.1.4.1.2636.3.1.13.1.7.<index>)
    JUNIPER-MIB::jnxOperatingTemp
    - Allarmi
      - intake > 54
      - RE > 70

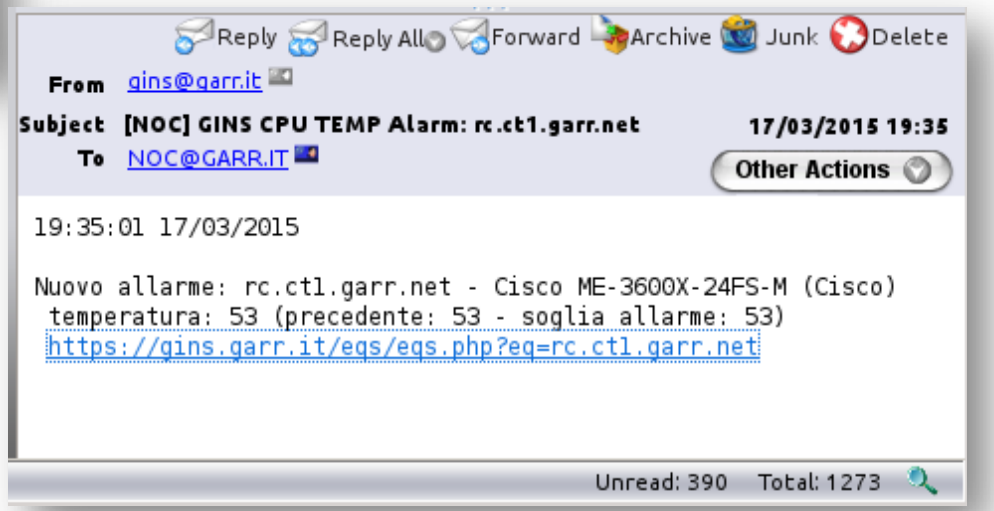




Temperature

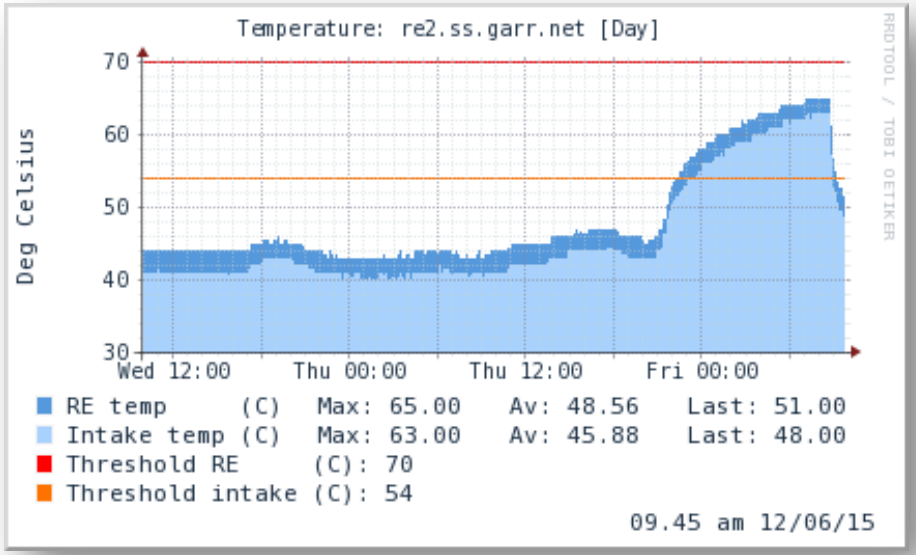
Notifica prima del superamento soglia

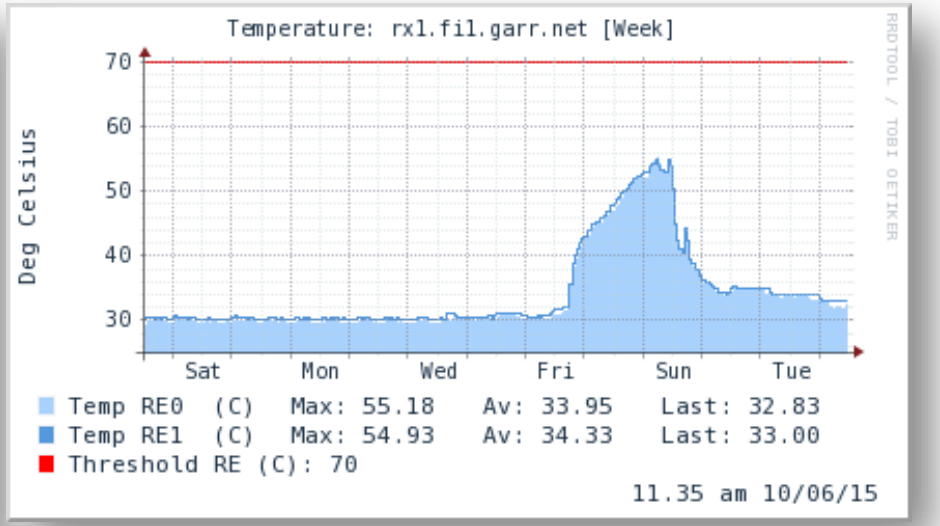


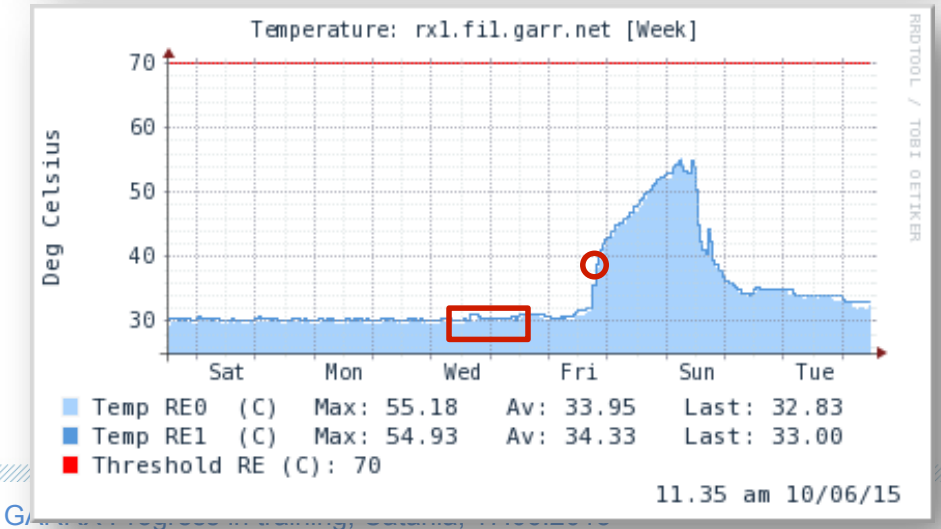


Temperature

Quando il condizionamento ha problemi







Allarme e notifica se:

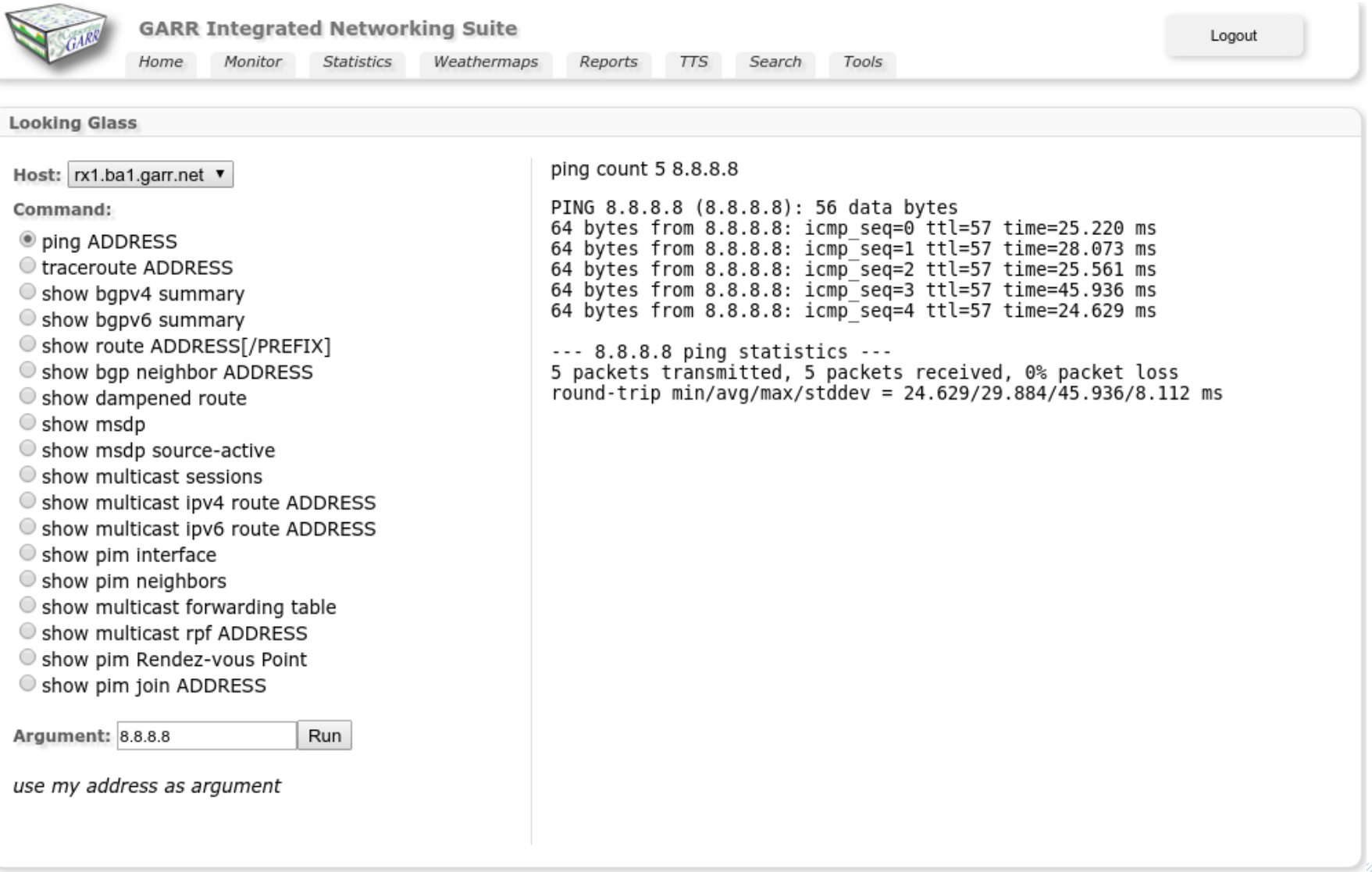
la temperatura attuale

>

temperatura media su 24h delle 24h precedenti al momento attuale + 8 C

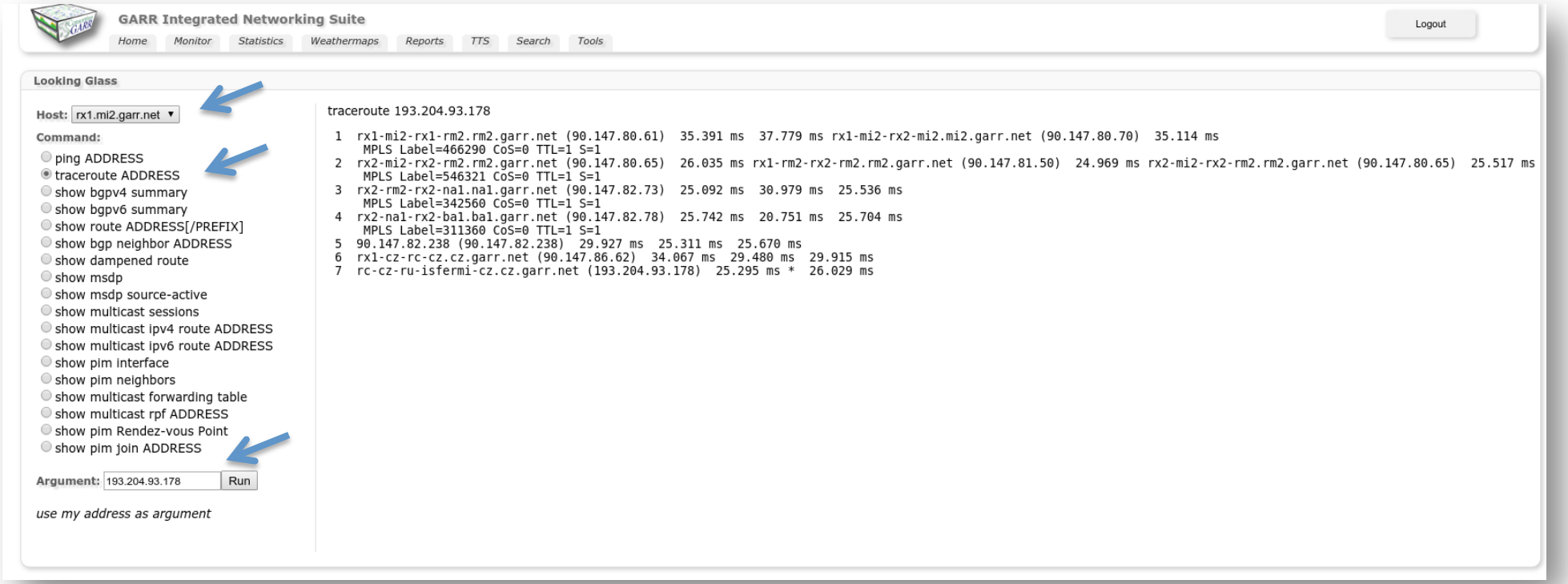
Looking glass

https://gins.garr.it/LG/



Looking glass

https://gins.garr.it/LG/



LLDP protocollo amico

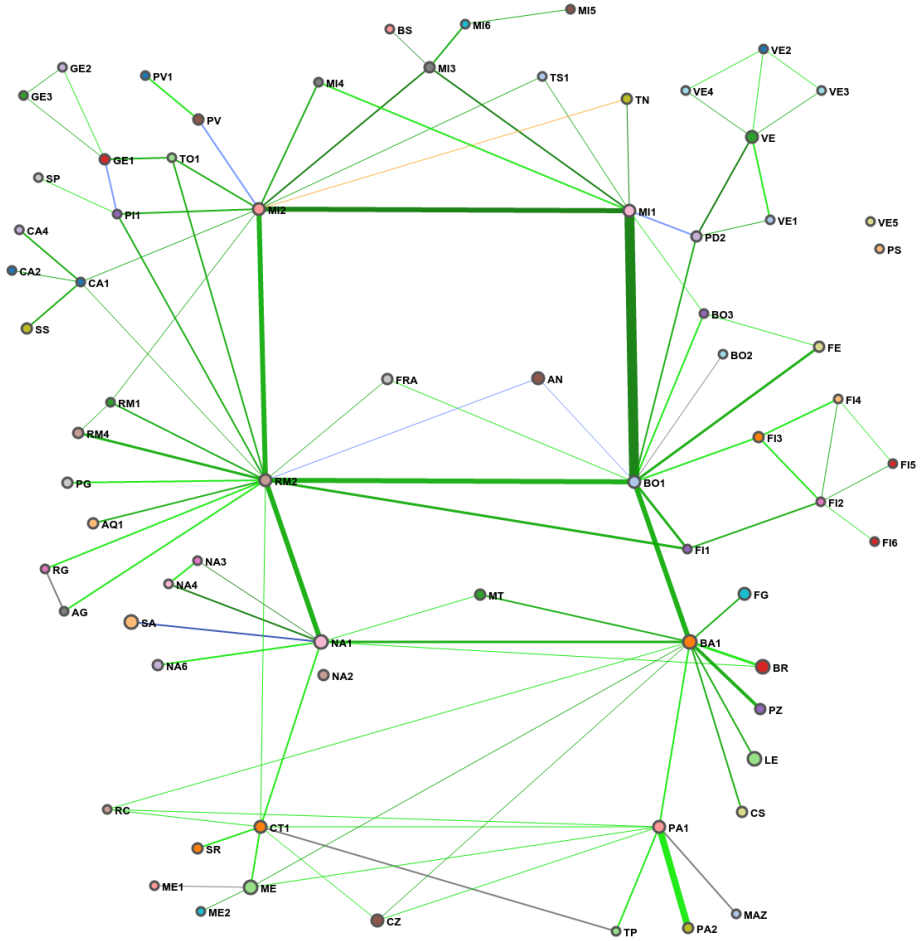
The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.

```
> show lldp neighbors
Local Interface Chassis Id       Port info     System Name
ge-0/3/9        00:1e:bd:97:7e:00  GigabitEthernet1/0/25 SWE-LAN.garr.net
ge-2/3/9        00:1e:bd:97:7e:00  GigabitEthernet1/0/27 SWE-LAN.garr.net
ge-0/2/2        1c:aa:07:cb:6e:00  GigabitEthernet0/13 SWE.FG.garr.net
ge-11/2/2       1c:aa:07:cb:6e:00  GigabitEthernet0/15 SWE.FG.garr.net
xe-2/1/1        1c:de:a7:9b:da:9c  TenGigabitEthernet0/1 swu1-cnr-adr-ba.ba1.garr.net
ge-0/2/1        8c:b6:4f:ae:d8:80  GigabitEthernet1/0/25 swg.ba1.garr.net
ge-11/3/1       f0:9e:63:8c:80:00  GigabitEthernet0/16 swu-uniba-biotec.ba1.garr.net
ge-11/3/3       f0:9e:63:8c:9a:80  GigabitEthernet0/16 swu-uniba-valenzano.garr.net
ge-11/3/0       f8:c0:01:1b:dd:68  ge-1/0/0      RE1.MT
ge-11/2/6       f8:c0:01:1b:dd:68  ge-1/0/1      RE1.MT
ge-11/3/7       f8:c0:01:1c:05:68  ge-1/0/3      RE1.PZ
ge-0/2/3        f8:c0:01:1c:05:68  ge-1/0/4      RE1.PZ
xe-11/1/1       f8:c0:01:1c:2c:68  xe-0/0/1      RE2.LE
ge-11/3/9       f8:c0:01:1c:32:68  ge-1/0/3      RE2.PZ
```

LLDP protocollo amico

Permette di scoprire la topologia layer 2

HOST (info) PORT (info) – PORT (info) HOST (info)

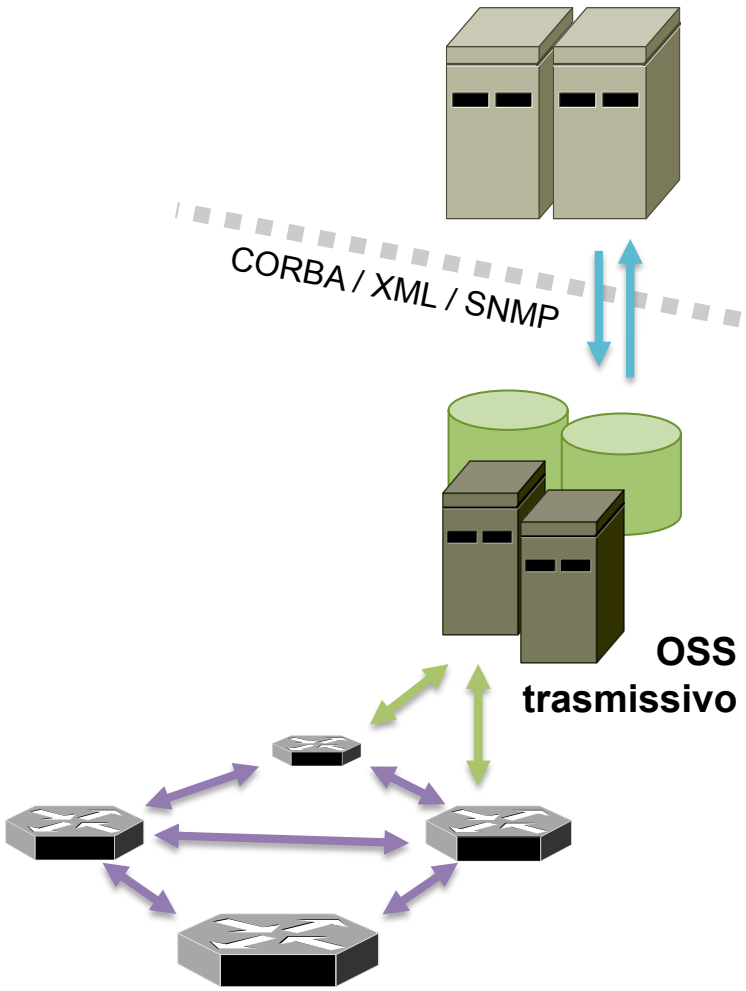


Rete trasmissiva

La gestione e il controllo della rete ottica avviene tramite un sistema hardware e software dedicato, chiamato **OSS** (Operating Support System).

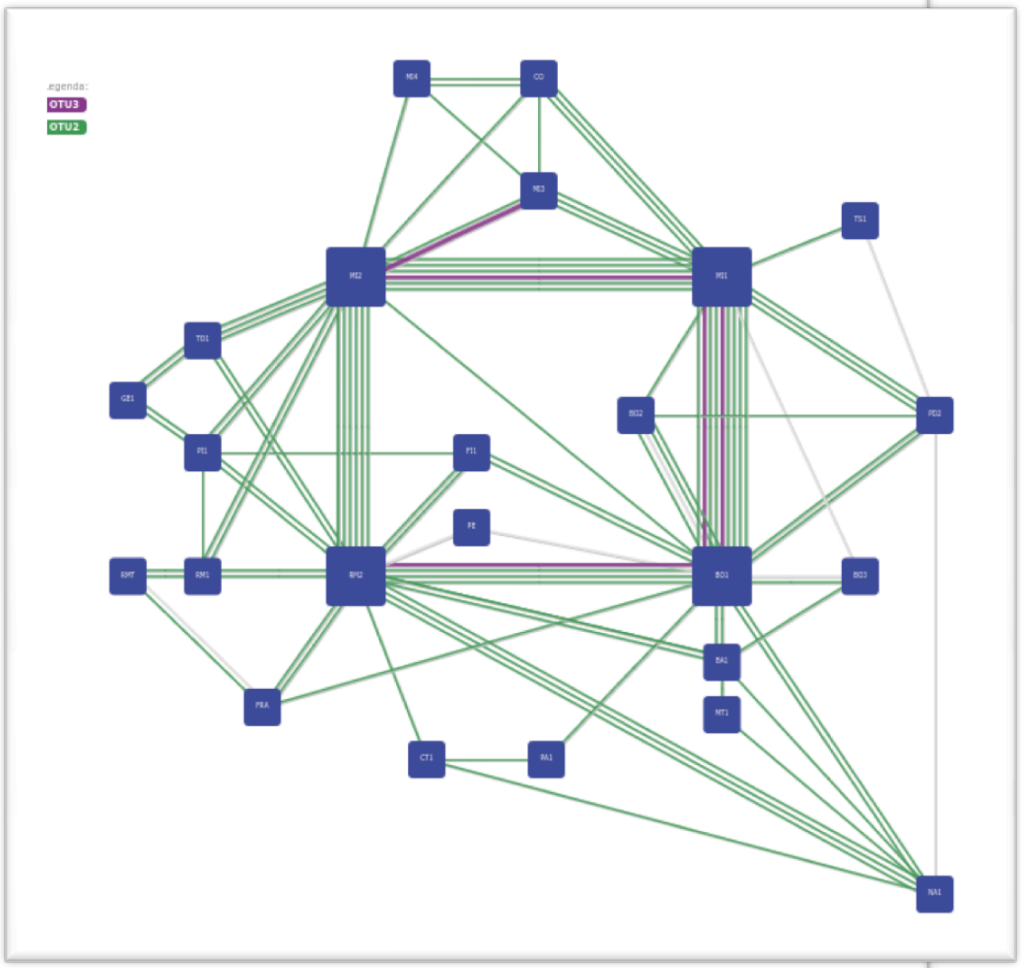
Questo sistema e' parte integrante dell'infrastruttura della rete trasmissiva.

I dati raccolti dall'OSS vengono esportati mediante molteplici interfacce, che permettono l'analisi e la correlazione delle informazioni della rete ottica con i dati relativi agli altri livelli di rete.



Rete Trasmissiva

Lambda

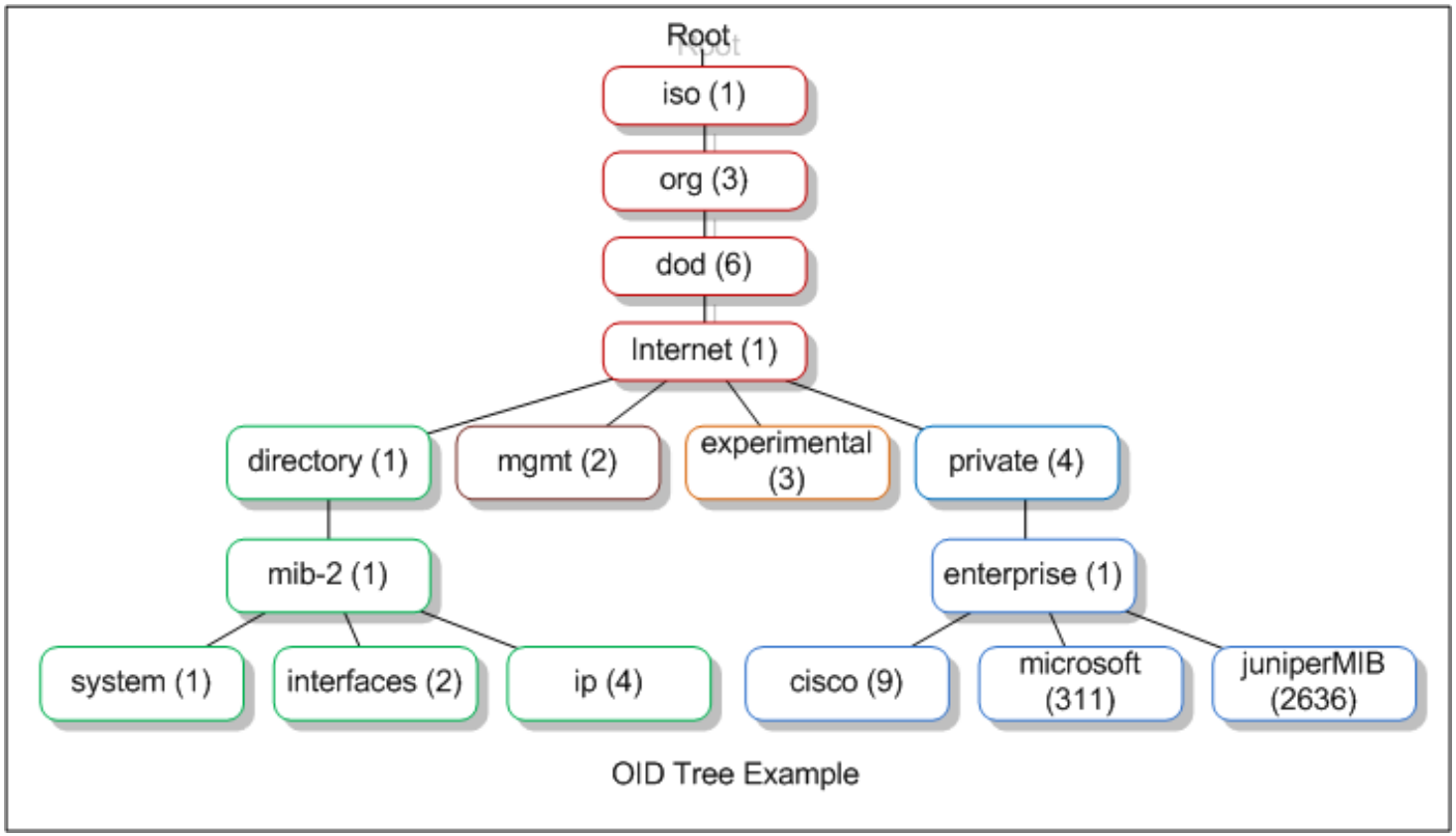


Fibra

Agenda

- MIBs
- SNMP Trap
- SNMP Trap con snmptrapd
- SNMP Trap con nodejs
- SNMP Poll esempi
- RRD

MIB OID



OID Tree Example

MIB translate

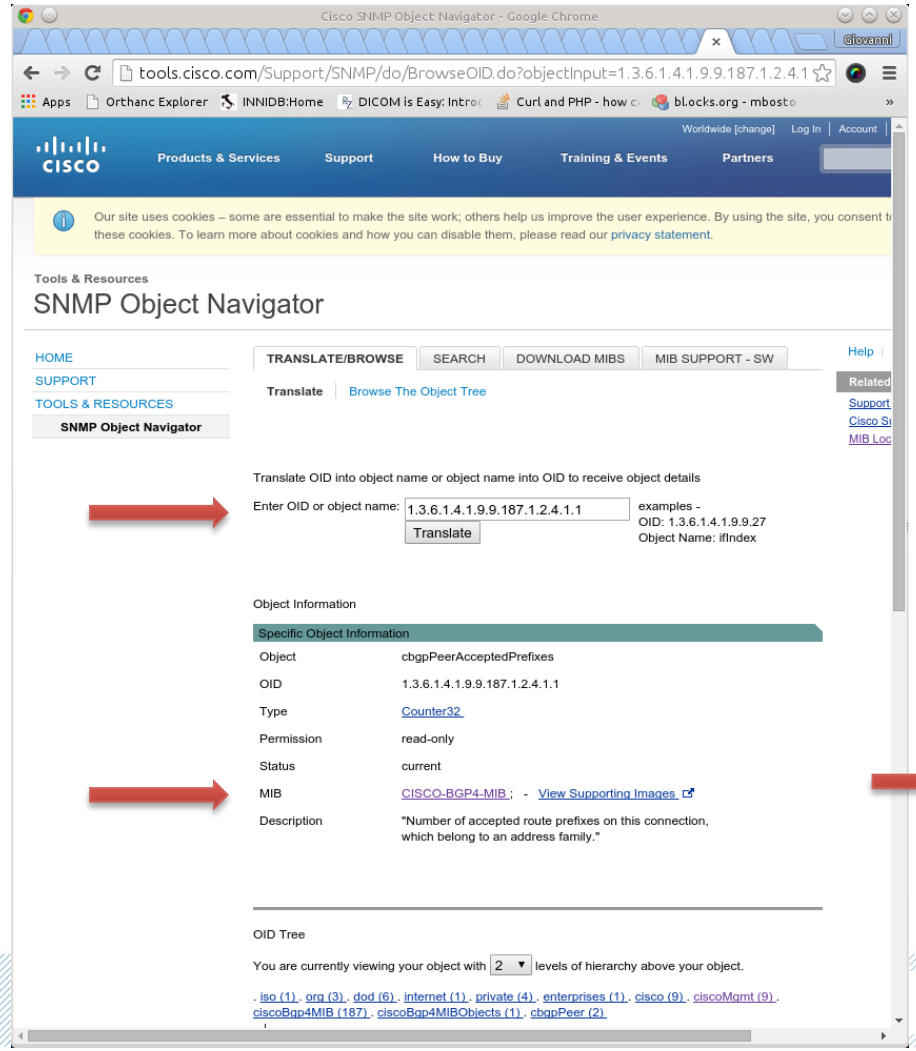
OID: 1.3.6.1.4.1.9.9.187.1.2.4.1.1 ?

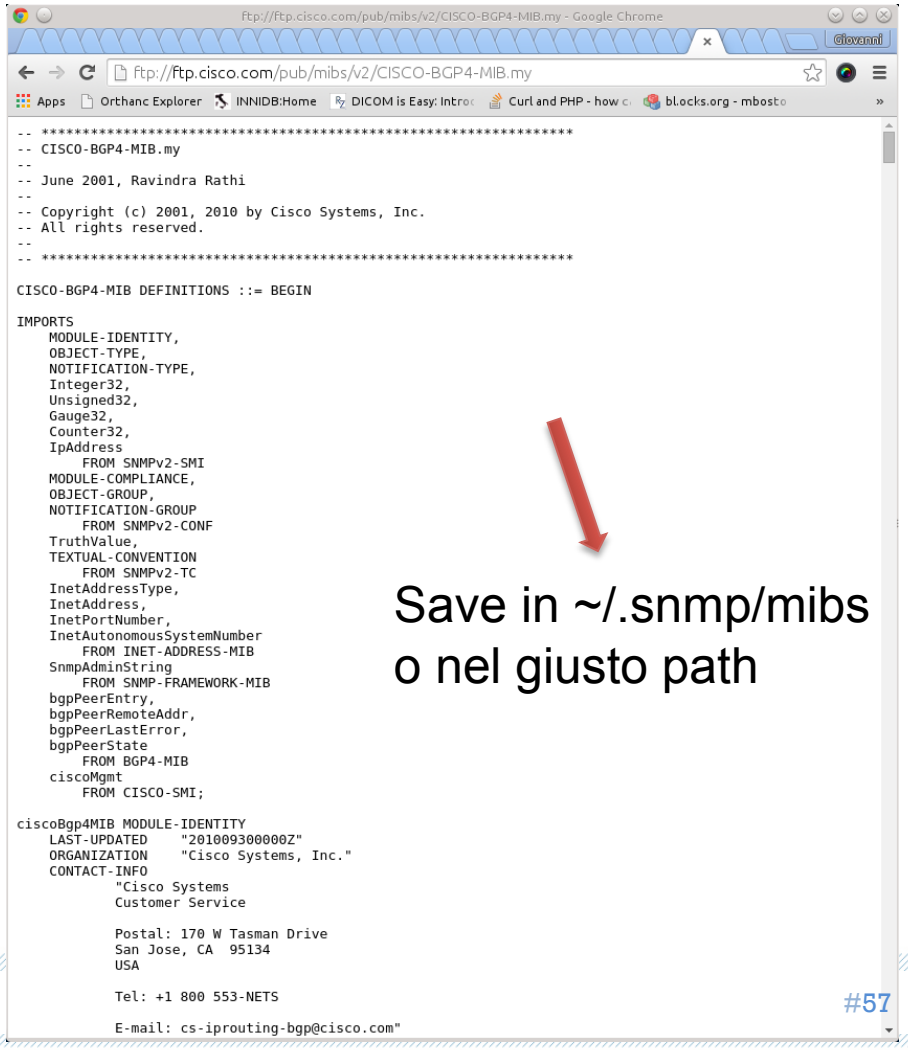
```
$ snmptranslate -m ALL -Pu -Ts 1.3.6.1.4.1.9.9.187.1.2.4.1.1

SNMPv2-SMI::enterprises.9.9.187.1.2.4.1.1
```

mancano i MIB file

MIB dowload

1.3.6.1.4.1.9.9.187.1.2.4.1.1 ?





Save in ~/.snmp/mibs o nel giusto path

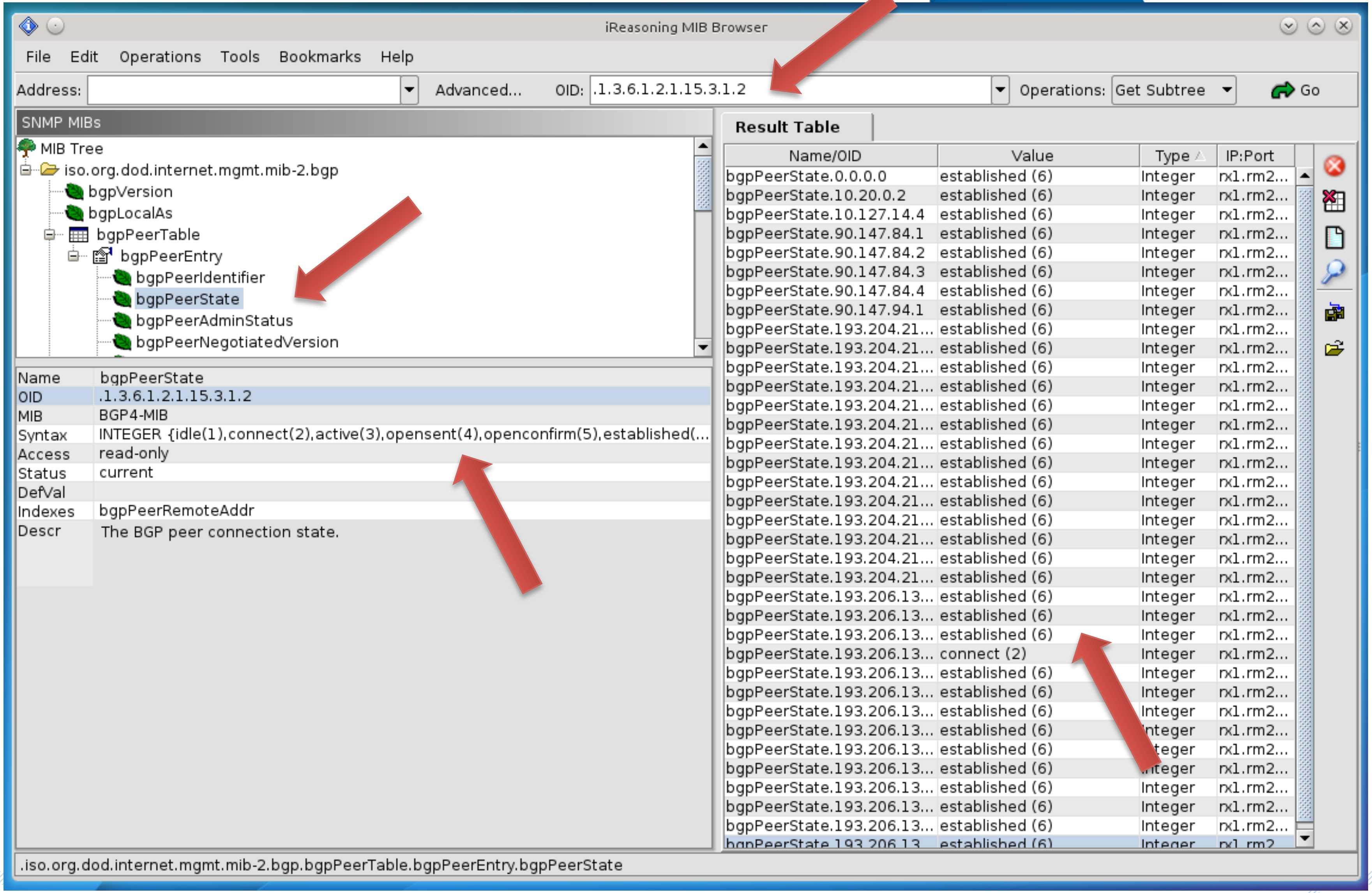
MIB translate

1.3.6.1.4.1.9.9.187.1.2.4.1.1 ?

```
$ snmptranslate -m ALL -Pu -Ts 1.3.6.1.4.1.9.9.187.1.2.4.1.1

CISCO-BGP4-MIB::cbgpPeerAcceptedPrefixes
```

MIB browser

MIB Browser



Ascoltare la rete: SNMP Trap

Struttura della trap:

<host> UDP: [<IP src>]:<port>->[<IP dst>]:162 <OID> <value> <OID> <value> …

Trap tradotta:

```
{src: '<ip>',
 date: Wed May 20 2015 19:19:11 GMT+0200 (CEST),
 type: 'SNMPv2_Trap(7)',
 oid: '1.3.6.1.4.1.9.9.91.2.0.1',
 name: 'CISCO-ENTITY-SENSOR-MIB::entSensorThresholdNotification',
 vb:
  [ 'DISMAN-EVENT-MIB::sysUpTimeInstance': '615516684',
    'SNMPv2-MIB::snmpTrapOID.0': '1.3.6.1.4.1.9.9.91.2.0.1',
    'CISCO-ENTITY-SENSOR-MIB::entSensorThresholdValue.1058.2': '-70',
    'CISCO-ENTITY-SENSOR-MIB::entSensorValue.1058': '-63' ] }
```

Tipo di evento

informazioni

```
{ src: '<ip>',
  date: Wed May 20 2015 19:25:32 GMT+0200 (CEST),
  type: 'Trap(4)',
  oid: '1.3.6.1.4.1.318',
  name: 'SNMPv2-SMI::enterprises.318',
  vb: [ 'SNMPv2-SMI::enterprises.318.2.3.3.0': 'UPS: Batteries need immediate replacement.' ] }
```

Ascoltare la rete: SNMP Trap

Struttura della trap:

<host> UDP: [<IP src>]:<port>->[<IP dst>]:162 <OID> <value> <OID> <value> …

Trap tradotta:

{ src: '<ip>',
  date: Wed May 20 2015 19:29:13 GMT+0200 (CEST),
  type: 'SNMPv2_Trap(7)',
  oid: '1.3.6.1.6.3.1.1.5.3',
  name: 'IF-MIB::**linkDown**',
  vb:
   ['DISMAN-EVENT-MIB::sysUpTimeInstance': '112224290',
    'SNMPv2-MIB::snmpTrapOID.0': '1.3.6.1.6.3.1.1.5.3',
    'IF-MIB::ifIndex.2': '2',
    'IF-MIB::ifDescr.2': '**GigabitEthernet0/0**',
    'IF-MIB::ifType.2': '6',
    'CISCO-SMI::local.2.1.1.20.2': 'Link down'] }

Ascoltare la rete: SNMP Trap

Struttura della trap:

<host> UDP: [<IP src>]:<port>->[<IP dst>]:162 <OID> <value> <OID> <value> …

Trap tradotta:

{ src: '<ip>',
  date: Wed May 20 2015 19:29:13 GMT+0200 (CEST),
  type: 'SNMPv2_Trap(7)',
  oid: '1.3.6.1.6.3.1.1.5.3',
  name: 'IF-MIB::**linkDown**',
  vb:
   ['DISMAN-EVENT-MIB::sysUpTimeInstance': '112224290',
     'SNMPv2-MIB::snmpTrapOID.0': '1.3.6.1.6.3.1.1.5.3',
     'IF-MIB::ifIndex.2': '2',
     'IF-MIB::ifDescr.2': '**GigabitEthernet0/0**',
     'IF-MIB::ifType.2': '6',
     'CISCO-SMI::local.2.1.1.20.2': 'Link down'] }

Ascoltare la rete: SNMP Trap

Trap tradotta:

Trap from host: <ip> -
Event: CISCO-ENTITY-SENSOR-MIB::***entSensorThresholdNotification*** –
Date:Fri Jun 12 2015 10:26:43 GMT+0200 (CEST)
DISMAN-EVENT-MIB::sysUpTimeInstance: 844717312
SNMPv2-MIB::snmpTrapOID.0: 1.3.6.1.4.1.9.9.91.2.0.1
CISCO-ENTITY-SENSOR-MIB::***entSensorThresholdValue.1135***.4: **-30**
CISCO-ENTITY-SENSOR-MIB::***entSensorValue.1135***: **-56**

Chi e' l'entita' 1135?

$ snmpwalk -c public -v2c <ip> .1.3.6.1.2.1.47.1.1.1.1.7.***1135***
SNMPv2-SMI::mib-2.47.1.1.1.1.7.1135 = STRING: "**Gi0/3 Transmit Power Sensor**"

(I valori -30 e -56 sono in realta' -3.0 e -5.6)

SNMP TRAP ascoltare con snmptrapd

1- /etc/snmp/snmptrapd.conf

```
disableAuthorization yes
traphandle default /home/cesaroni/test/my_trap_handler.sh
```

2- /home/cesaroni/test/my_trap_handler.sh

```
#!/bin/bash
A=`cat /dev/stdin`
echo $A >> /home/cesaroni/test/trap_log.txt
```

3- lancio snmptrapd

```
$ sudo snmptrapd -d
```

```
$ tail -f trap_log.txt
<host> UDP: [<IP src>]:<port>->[<my IP>]:162 OID value OID value OID value
….
```

SNMP TRAP ascoltare con nodejs

Node.js is a platform built on Chrome's JavaScript runtime for easily building fast, scalable network applications.
Node.js uses an event-driven, non-blocking I/O model that makes it lightweight and efficient, perfect for data-intensive real-time applications that run across distributed devices.

SNMP TRAP + nodejs

Invio Trap:

```
$ snmptrap  -v 2c -c public localhost  ""  .1.3.6.1.4.1.5000.5000.1 .
1.3.6.1.4.1.5000.5000.1.1 s "pippo" .1.3.6.1.4.1.5000.5000.1.2 s "pluto"
```

Ricevo Trap:

```
$ sudo nodejs test.js
{"name":"snmpjs","hostname":"pcgarr9","pid":26416,"level":30,"msg":"Bound to
0.0.0.0:162","time":"2015-03-11T15:52:40.742Z","v":0}

Trap Received Wed Mar 11 2015 16:53:05 GMT+0100 (CET) n: 1
Trap Sender 127.0.0.1
varbind oid: 1.3.6.1.2.1.1.3.0 value: 60677003
varbind oid: 1.3.6.1.6.3.1.1.4.1.0 value: 1.3.6.1.4.1.5000.5000.1
varbind oid: 1.3.6.1.4.1.5000.5000.1.1 value: pippo
varbind oid: 1.3.6.1.4.1.5000.5000.1.2 value: pluto
```

Hands on: SNMP TRAP + nodejs

Esempio di Trap listener minimale in nodejs

```
var os = require('os');
var snmp = require('snmpjs');
var trapd = snmp.createTrapListener();
var count=0;

trapd.on('trap', function(msg){
   count = count+1;
   var src=msg.src.address;
   var now = new Date();
   console.log("Trap Received " + now + " n: "+ count);
   console.log("Trap Sender "+src);
   var vars = snmp.message.serializer(msg)['pdu'].varbinds;
   for(var i in vars){
        console.log('varbind oid: ' + vars[i].oid + ' value: '+ vars[i].string_value);
   }
});
trapd.bind({family: 'udp4', port: 162});
```

Hands on: SNMP TRAP + nodejs

Ma arriveranno tutte? stressiamolo

```
$ for i in {1..10000}; do snmptrap -v 2c -c public localhost:162 "" .1.3.6.1.2.1.25.3.1.2.0&
done
```

```
Trap Received Wed Mar 11 2015 17:12:10 GMT+0100 (CET) n: 10000
Trap Sender 127.0.0.1
varbind oid: 1.3.6.1.2.1.1.3.0 value: 60791459
varbind oid: 1.3.6.1.6.3.1.1.4.1.0 value: 1.3.6.1.2.1.25.3.1.2.0
```

Hands on: SNMP TRAP + nodejs

In opera

GINS-TrapServer status:
Started at: Tue Jun 16 2015 17:18:47 GMT+0200 (CEST)
Ora sono le 11:58 del Jun 17 2015

Trap counters:
CISCO-ENTITY-SENSOR-MIB::entSensorThresholdNotification: **82502**
IF-MIB::linkDown: **170714**

In circa 20 ore sono state ricevute
82502 trap di sensori fuori soglia
170714 trap di link down

I link down quasi interamente da un singolo Cisco 2900 con una porta malfunzionante

Hands on: SNMP TRAP + nodejs

Quindi?

Cosa fare con l'evento TRAP:

- **Fare poco e veloce**
- **Meccanismi di blacklist pre processing**
- **Selezione eventi specifici**
- **Poco storico (no DB)**
- **No mail**

Hands on: SNMP poll esempi

snmpget -v2c -c <community> <router> <Object Identifier OID>
snmpwalk -v2c -c <community> <router> <Object Identifier OID subtree>

Poll response: <OID> = <data type>: <value>

Esempi:
snmpget -v2c -c <community> <router> IP-MIB::**ipAdEntIfIndex**.192.168.0.1
IP-MIB::**ipAdEntIfIndex**.192.168.0.1 = INTEGER: 82

snmpget -v2c -c <community> <router> IF-MIB::**ifName**.82
IF-MIB::**ifName**.82 = STRING: ge-1/2/0.4

snmpget -v2c -c <community> <router> IF-MIB::**ifHighSpeed**.82
IF-MIB::**ifHighSpeed**.82 = Gauge32: 1000

snmpget -v2c -c <community> <router> IF-MIB::**ifHCInOctets**.82
IF-MIB::**ifHCInOctets**.82 = Counter64: 262925908632166

Hands on: SNMP poll esempi

Stato di un Peer BGP: 1.3.6.1.2.1.15.3.1.2 (RFC 1269)

```
snmpwalk -v2c -c <comunity> <router> 1.3.6.1.2.1.15.3.1.2 |
            awk -F '15.3.1.2.'          '{print $2}‘ |
            awk -F ' = INTEGER: ' '{print $1,$2}'
```

Restituisce la lista di :
<IP address del Peer> <Stato numerico Peer>

```
"1"=>"Idle"
"2"=>"Connect"
"3"=>"Active"
"4"=>"Opensent"
"5"=>"Openconfirm"
"6"=>"Established"
```

AS of the Peer BGP:
1.3.6.1.2.1.15.3.1.9 (RFC 1269)

```
snmpwalk -v2c -c <community> <router> 1.3.6.1.2.1.15.3.1.9 |
            awk -F '15.3.1.9.' '{print $2}' |
            awk -F ' = INTEGER: ' '{print $1,$2;}'
```

Restituisce la lista di :
<IP address del Peer> <AS del Peer>

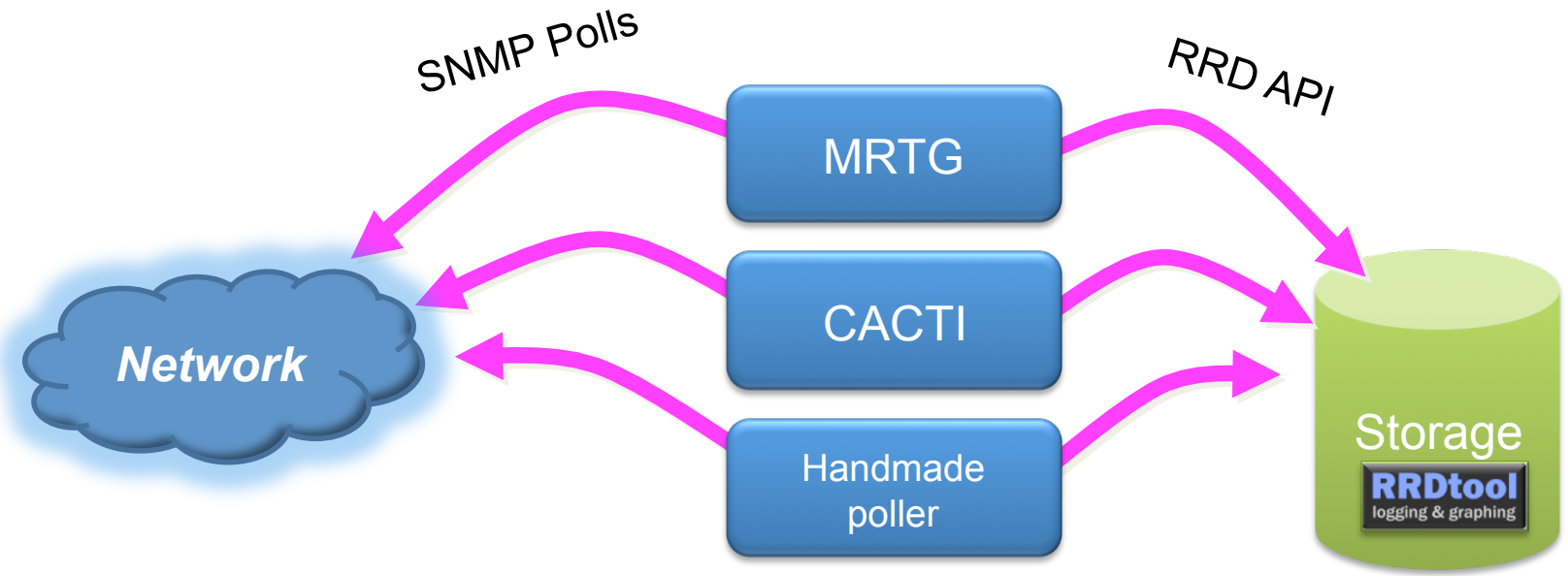
Hands on: SNMP poll esempi

Prefissi BGP, MIB proprietarie

CISCO-BGP4-MIB
Accepted prefixes from Peer
1.3.6.1.4.1.9.9.187.1.2.4.1.1.<IP>.1.1 (.1.1 = IPv4 Unicast)
Advertised prefixes to Peer
1.3.6.1.4.1.9.9.187.1.2.4.1.6.<IP>.1.1

BGP4-V2-MIB-JUNIPER
Received prefixes from Peer
1.3.6.1.4.1.2636.5.1.1.2.6.2.1.7.<Peer Index>.1.1
Advertised prefixes to Peer
1.3.6.1.4.1.2636.5.1.1.2.6.2.1.10.<Peer Index>.1.1
Accepted prefixes from Peer
1.3.6.1.4.1.2636.5.1.1.2.6.2.1.8.<Peer Index>.1.1
Peer Index from:
1.3.6.1.4.1.2636.5.1.1.2.1.1.1.14

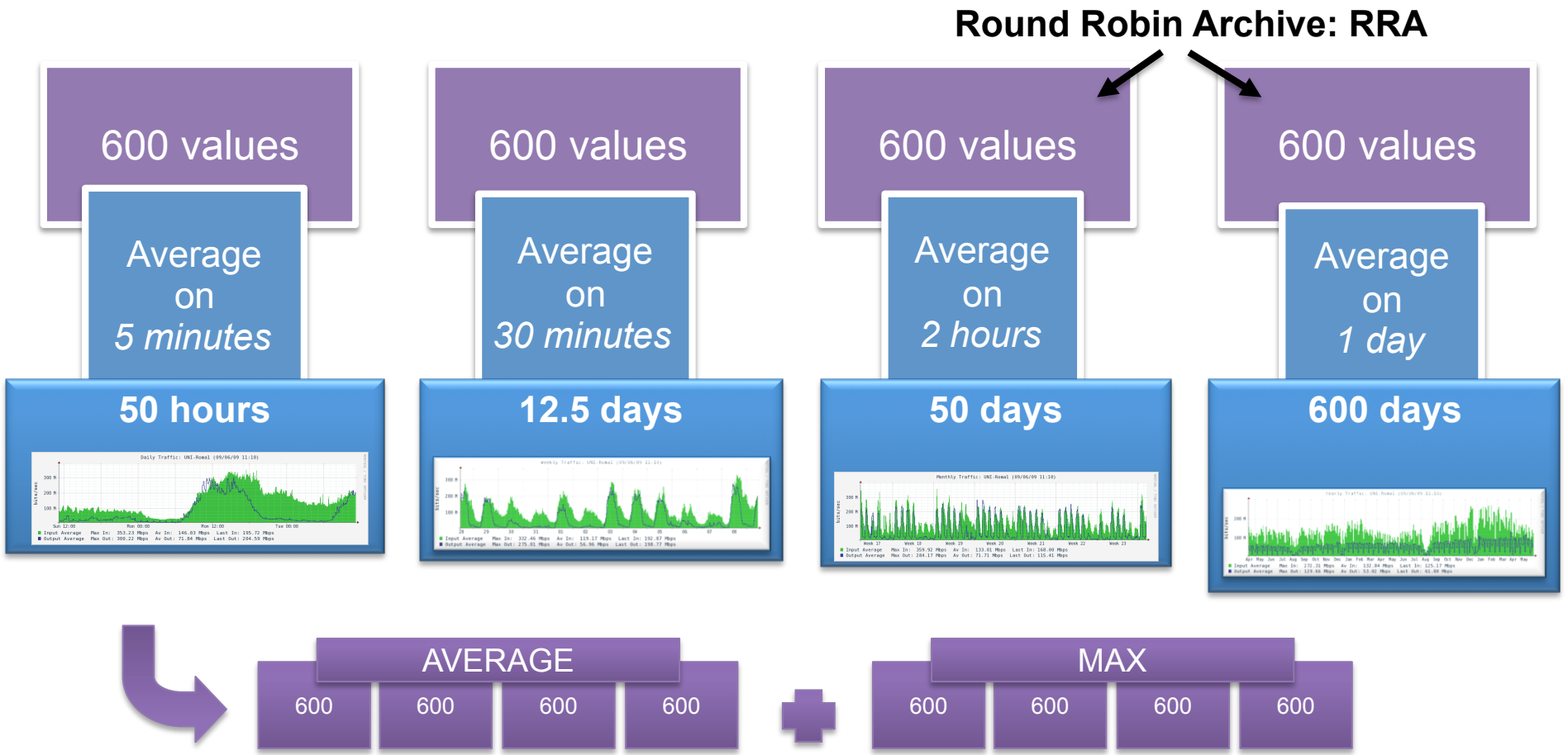
Hands on: RRD


SNMP Polls
RRD API
MRTG
CACTI
Handmade poller
Network
Storage
RRDtool
logging & graphing

Hands on: RRD

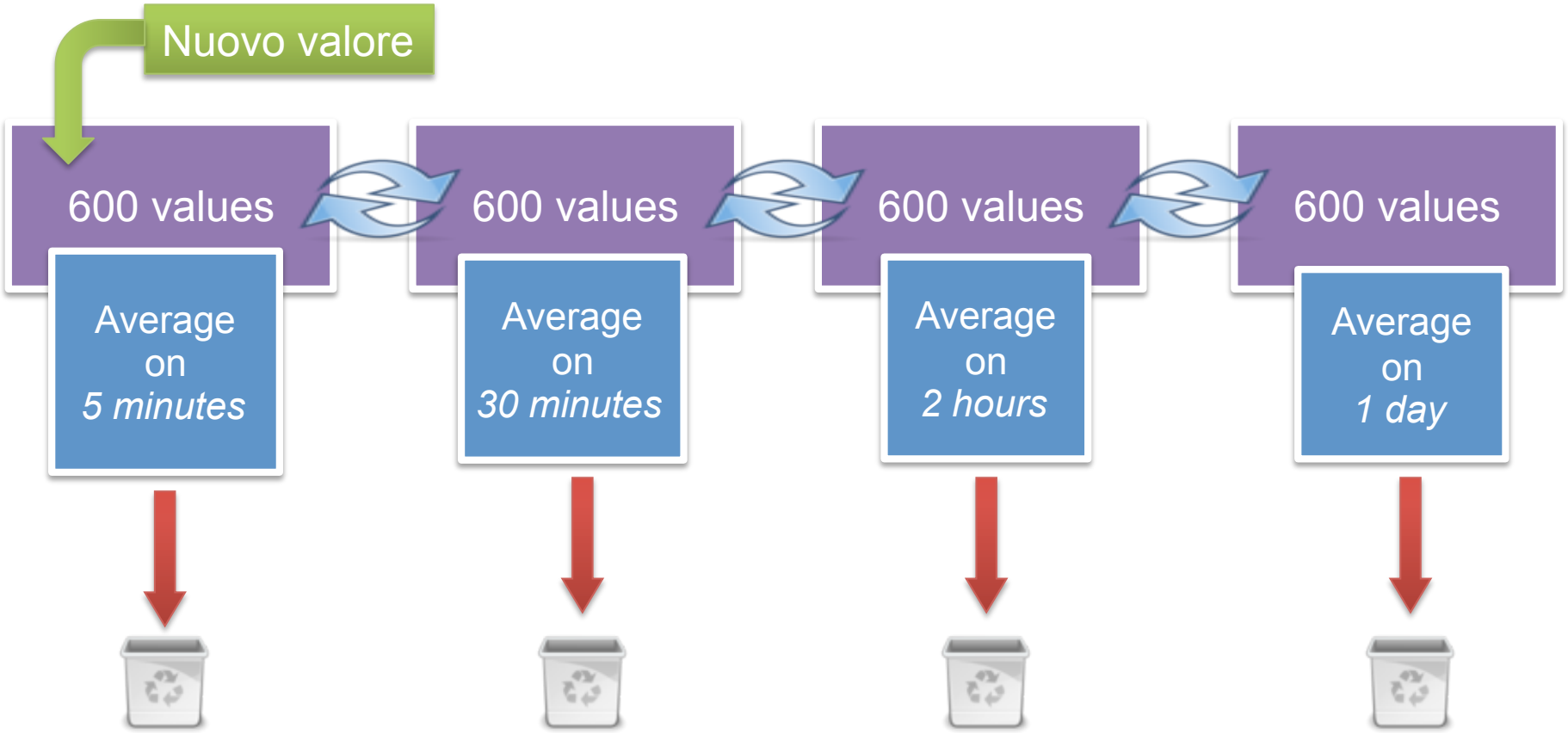
Il file RRD:

Possibile e tipica struttura temporale di un RRD file creato da MRTG:



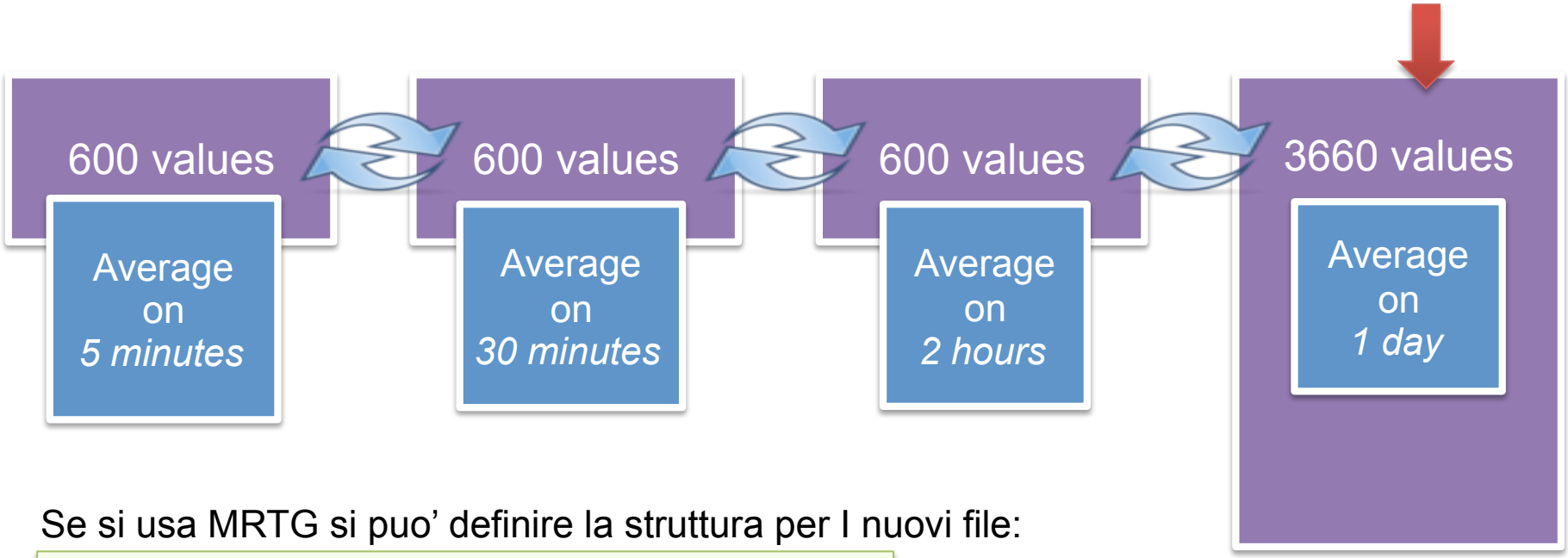
Hands on: RRD

aggiornamento RRD:



Hands on: RRD

Modificare la struttura temporale del RRA a **10** anni



Se si usa MRTG si puo' definire la struttura per I nuovi file:

```
Target[<target>]: /
<IP>:<community>@<host>:::::2
RRDRowCount1d[<target>]: 3660
MaxBytes[<target>]: 4000000
Options[<target>]: bits,growright
YLegend[<target>]: Bits Per Second
ShortLegend[<target>]: b/s
```

Hands on: RRD

RRD API:

Info, create, update, fetch, tune, graph, dump, restore, etc.

rrdtool info <file.rrd>

```
rra[0].cf = "AVERAGE"
rra[0].rows = 600
rra[0].pdp_per_row = 1
rra[1].cf = "AVERAGE"
rra[1].rows = 600
rra[1].pdp_per_row = 6
rra[2].cf = "AVERAGE"
rra[2].rows = 600
rra[2].pdp_per_row = 24
rra[3].cf = "AVERAGE"
rra[3].rows = 600
rra[3].pdp_per_row = 288
```

5 m

30 m

2 h

1 d

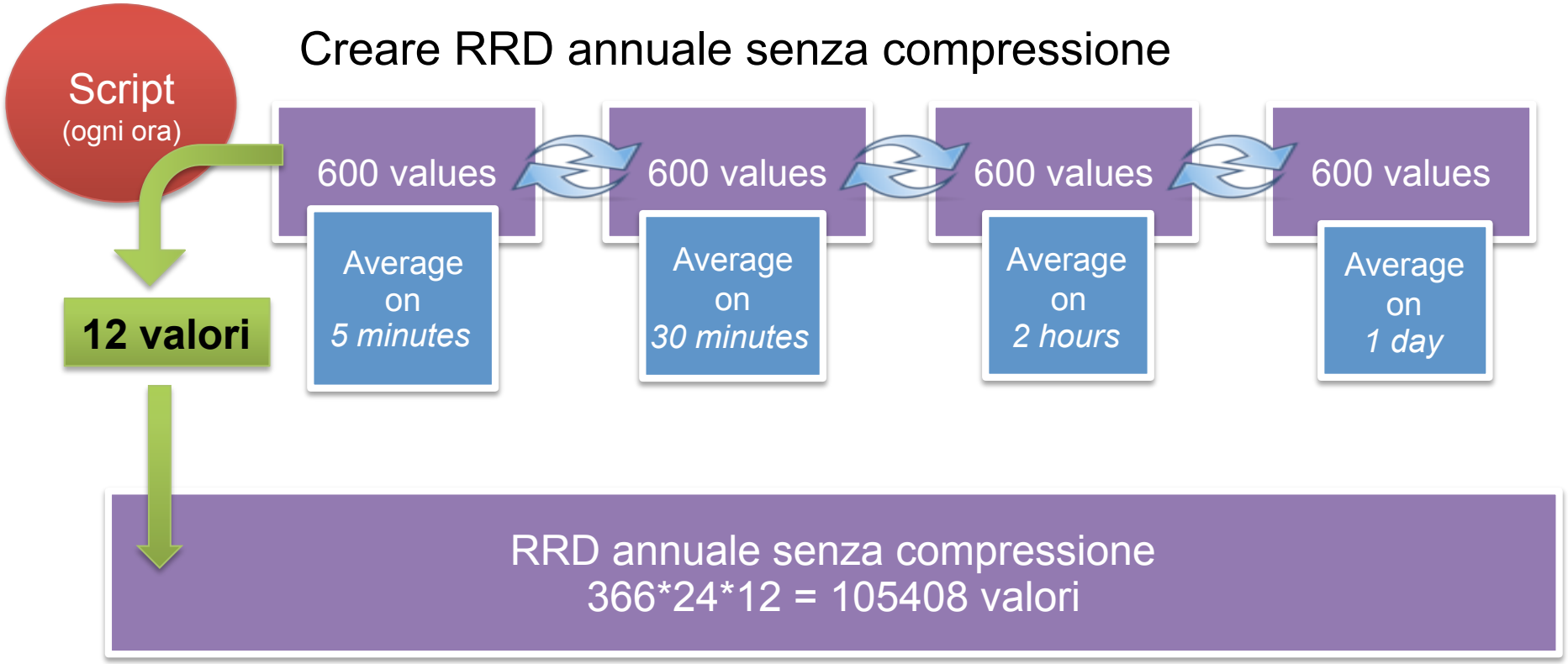
RRA number

rrdtool resize <file.rrd> 3 GROW 3060

```
rra[0].cf = "AVERAGE"
rra[0].rows = 600
rra[0].pdp_per_row = 1
rra[1].cf = "AVERAGE"
rra[1].rows = 600
rra[1].pdp_per_row = 6
rra[2].cf = "AVERAGE"
rra[2].rows = 600
rra[2].pdp_per_row = 24
rra[3].cf = "AVERAGE"
rra[3].rows = 3660
rra[3].pdp_per_row = 288
```

Hands on: RRD

Come evitare di perdere i dati:



Hands on: RRD

Creare RRD annuale senza compressione:

1- creazione RRD un anno :

```
rrdtool create <destinazione.rrd>
>       --start <qualche anno fa> --step 300
>       DS:in:GAUGE:600:U:U DS:out:GAUGE:600:U:U
>       RRA:LAST:0.5:1:105408
```

2- estrazione valori di 1 ora e inserimento:

```
rrdtool fetch <sorgente.rrd> --end now-600s --start now-4200s AVERAGE |
        awk -F ' ' 'BEGIN {x=0;}{x++; if (x>2){ print $1 $2":"$3 } }' |
        xargs rrdtool update <destinazione.rrd>
```

Riferimenti

- https://gins.garr.it
- sw.dev@garr.it
- info@garr.it
- noc@garr.it
- giovanni.cesaroni@garr.it