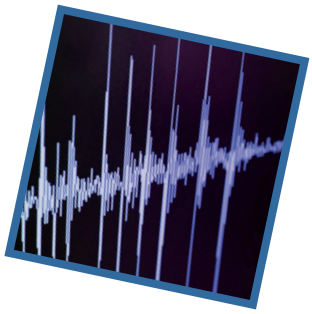
Osservo, misuro, valuto, agisco. Come la gestione consapevole della rete sia benefica per il suo utilizzo



Massimo Carboni

Consortium GARR

Abstract. Attivare un servizio di collegamento e trasmissione dati è solo il primo passo. Il controllo e la gestione di una infrastruttura di rete non servono solo per la risoluzione rapida dei guasti. È necessaria una costante attenzione al comportamento del traffico per comprenderne la qualità, progettare migliorie ed adeguarsi ai cambiamenti prima che vi siano problemi. L'articolo mostra come questa attenzione ed analisi siano svolte costantemente nella rete della ricerca italiana GARR e quale sia il loro effetto benefico.

1. Premessa

L'uso della rete è sempre più pervasivo ed è diventato parte integrante dell'attività lavorativa e di relazione. L'infrastruttura e l'insieme dei servizi di rete, che sottendono alle molteplici e differenti applicazioni che ogni giorno vengono usate attraverso la rete stessa, richiedono un controllo funzionale e operativo costante che ne garantisca la piena disponibilità e qualità. A questo scopo è necessario stabilire una definizione quantitativa del Servizio Rete e delle sue modalità di funzionamento. Questa definizione è indispensabile sia per l'utilizzatore del servizio che per il fornitore. Tale esigenza è sempre più sentita anche nel mondo della ricerca che usa la rete come uno strumento fondamentale per accedere ai dati, alle risorse di calcolo, per organizzare progetti e svolgere il lavoro quotidiano.

Per questi motivi, GARR ha sviluppato ed utilizza strumenti che controllano 24 ore su 24 il funzionamento della rete di trasmissione dati che gestisce e dei servizi che fornisce, avendo particolare attenzione alle funzionalità dei servizi ed alle prestazioni della rete. Tutti i dati sono accessibili, in tempo reale, attraverso il sito web GARR-NOC [1]. Questo breve articolo dettaglia le tecnologie utilizzate e ne indica le ricadute.

2. Che cosa misurare e perché

L'ambito della trasmissione dati a pacchetto su cavi fissi di cui il GARR si occupa, corrisponde al modello classico Internet basato sulla suite di protocolli TCP/IP. Per tale ambito sono stati identificati negli organismi di standardizzazione, come IETF ed ISO/OSI, una serie di parametri che permettono sia di controllare la qualità del servizio e la sua conformità ad un contratto, che di fornire dati sull'evoluzione prevista con un'attenta analisi storica.

I parametri sono (in parentesi i termini inglesi usati comunemente):

- banda passante o capacità (*bandwidth*) espressa in bit al secondo;
- perdita di pacchetti (*packet loss*);
- ritardo (*delay*);
- variazione del ritardo (*IP delay variation* (IPDV), o *delay variation* oppure *jitter*).

La misura di queste grandezze permette di definire e controllare i parametri di funzionamento di un servizio di rete. La definizione di un servizio di rete si riconduce infatti alla definizione delle metriche di funzionamento del servizio stesso che ne consentono la classificazione in macro aree (per es. traffico dati o Voce su IP).

Nella tabella 1 vengono riassunte a titolo

Conferenza GARR_11 Selected Papers. Da 20 anni nel futuro. Bologna 8-10 novembre 2011
ISBN: 978-88-905077-3-1 © 2012 Associazione Consortium GARR

Richieste	Traffico (non real time)	Voce su IP	Streaming video	Service Level Agreement	Disponibilità
Requisiti di funziona-mento	• Adeguata banda passante • Riduzione di: – *ritardo* – *perdita di pacchetti* – *verifica della Qualità del Servizio*	• Riduzione di: – *ritardo* – *perdita di pacchetti* – *variazione del ritardo*	• Riduzione di: – *ritardo* – *perdita di pacchetti*	• Quantificazione di: – *ritardo* – *perdita di pacchetti* – *variazione del ritardo* – *ritardo unidirezionale*	• Verifica della connettività
Grandezze misurabili	• Banda erogata • Variazione del ritardo • Perdita dei pacchetti • Ritardo	• Variazione del ritardo • Perdita dei pacchetti • Ritardo • Qualità del Servizio Applicativo *(codec voce)*	• Variazione del ritardo • Perdita dei pacchetti • Ritardo	• Variazione del ritardo • Perdita dei pacchetti • Ritardo • Ritardo unidirezionale	• Verifica del funzionamento IP dei dispositivi di rete utente

Tab. 1 Classificazione dei servizi di rete in termini di requisiti di funzionamento e grandezze misurabili

di esempio alcune tipologie di uso della rete e come queste siano esprimibili in termini di requisiti di funzionamento, grandezze misurabili e di livelli di servizio erogabili (Disponibilità e SLA).

Il normale traffico dati (non real-time) presenta una ridotta sensibilità ad alcuni dei parametri tipici di rete, il requisito più forte è di una banda passante minima disponibile così come di una ridotta perdita di pacchetti (<1%). Per le applicazioni di tipo quasi-sincrono (real-time) sono invece importanti non solo gli aspetti connessi alla banda garantita, al ritardo, alla variazione del ritardo, alla perdita di pacchetti, ma è fondamentale considerare anche il ritardo unidirezionale. Le diverse grandezze rientrano quindi all'interno del contratto di servizio fornendo un dato oggettivo di valutazione.

Da un punto di vista tecnico la difficoltà di "gestione della misura" non è data dall'assenza di servizio (indisponibilità), quanto piuttosto dalle condizioni di degrado ovvero di erogazione del servizio richiesto con caratteristiche differenti da quelle attese o concordate, e della relativa misura del degrado.

Nel corso degli anni il GARR ha sviluppato una propria piattaforma di controllo e gestione dei servizi di rete (GINS, GARR Integrated Networking Suite [1]) con l'obiettivo di garantire sia la funzionalità dei servizi erogati che la reportistica verso la propria utenza. Dalla fine del 2004, sono disponibili i dati riguardanti il funzionamento della rete e sulla base di queste informazioni l'utenza è in grado di conoscere sia l'andamento istantaneo della rete che quello di tipo storico. Attraverso tali informazioni, GARR è in grado di valutare in anticipo eventuali limitazioni future e riesce a gestire al meglio la propria infrastruttura di rete.

3. Come misurare

Le tecnologie per misurare i parametri fondamentali sono fornite dagli apparati stessi che smistano i pacchetti nella rete (router, switch).

Le metodologie di misura si possono dividere in due grandi categorie:

- *Active Monitoring*: che agisce immettendo in rete traffico di controllo, di tipologia nota, che si comporti come il traffico utente. La finalità è quella di valutare le prestazioni "reali" del servizio di rete, simulando il comportamento del traffico utente. Questo tipo di approccio è molto efficace nelle misure che partono dall'utente finale e coprono l'intero tragitto fino al suo destinatario. Tali

misure sono parzialmente intrusive e potendo quindi perturbare il traffico in esame sono usate con particolari cautele.
- *Passive Monitoring*: in questo caso si effettua esclusivamente l'osservazione del traffico in transito, in modo non perturbativo in uno o più punti della rete.

La principale distinzione tra i due approcci consiste nella differente capacità di analisi del servizio erogato. Infatti, mentre nel primo caso abbiamo una dettagliata e specifica capacità di analisi del servizio offerto (traffico utente simulato), nel secondo possiamo osservare di norma solo i valori mediati su molti utenti e dall'analisi passiva del traffico è più complesso identificare o prevedere un possibile malfunzionamento del servizio.

Le due metodologie di misura sono complementari ed hanno pari importanza. La modalità Active supporta la gestione "real-time" del servizio consentendo al gestore dello stesso di agire con rapidità per prendere eventuali decisioni di re-instradamento o modulazione del traffico stesso sulla rete. La modalità Passive consente invece di gestire l'allarmistica e tenere sotto controllo la funzionalità della rete, ma soprattutto permette di fare un'analisi "a posteriori" a supporto della progettazione attraverso analisi "storiche" dell'evoluzione dei vari servizi così come dell'infrastruttura di rete a supporto degli stessi.

Ai fini della gestione della rete nota come GARR-G (2003-2011), basata su IP (Internet Protocol), l'approccio di misura ha riguardato principalmente l'uso di misure di tipo Passive, mediante l'acquisizione dei contatori disponibili negli apparati di rete propri di GARR-G. Le misure di tipo Active hanno riguardato esclusivamente aspetti connessi con la disponibilità di connettività IP mediante ICMP testing (*ping*).

Con la nuova rete GARR-X [2], ovvero la multi-service network, diventa necessario modificare la modalità di misura ponendo sempre di più l'attenzione sulla reale capacità di erogare un servizio nel tempo.

Nei prossimi paragrafi vedremo cosa si sta facendo in GARR e come questo si stia trasformando al fine di supportare al meglio l'attività di gestione della rete GARR-X.

2.1 Passive Monitoring

Ogni apparato di rete IP, dispone di contatori in grado di fornire lo stato di funzionamento, che possono essere acquisiti utilizzando il protocollo SNMP [3]. Tra i possibili contatori, previsti dal costruttore allo scopo di fornire informazioni sullo stato di funzionamento di un apparato, vi sono ad esempio i contatori di traffico su base interfaccia fisica (*ifInOctets*, *ifOutOctets*) mediante i quali è possibile avere la percentuale di traffico rispetto alla sua capacità (*ifSpeed*) in un determinato intervallo di tempo Δ*tempo*.

$$\%\,utilizzo\ della\ larghezza\ di\ banda = \frac{(\Delta ifInOctets + \Delta ifOutOctets)\times 8}{(\Delta tempo)\times ifSpeed}\times 100$$

Separando i due contatori si possono avere le informazioni relative al traffico in ingresso (In) ed in uscita (Out). Accanto alle informazioni connesse alla banda si possono avere informazioni riguardanti i pacchetti persi (Packet Loss) cosi come i pacchetti scartati (Drops) che danno una misura del degrado della linea di rete oggetto dell'osservazione.

Le informazioni di questo tipo vengono acquisite con MRTG (Multi Router Traffic Grapher) [4] il quale consente d'immagazzinare le informazioni in una base dati ad accesso diretto RRD (Round Robin Database) [5]. Così facendo è possibile mantenere i parametri di funzionamento di ogni singolo nodo di rete. Mediante questi contatori si può avere l'andamento storico d'uso della rete di ogni singolo accesso utente della rete, così come dei servizi IP che il GARR acquista da fornitori esterni, come ad esempio il transito IP verso il Global Internet.

Nelle figure seguenti si vede quale è stato il traffico dati di due sedi dell'INFN, quella del Tier1 presso INFN-CNAF a Bologna e quella del Tier2 presso INFN-Napoli in un in-

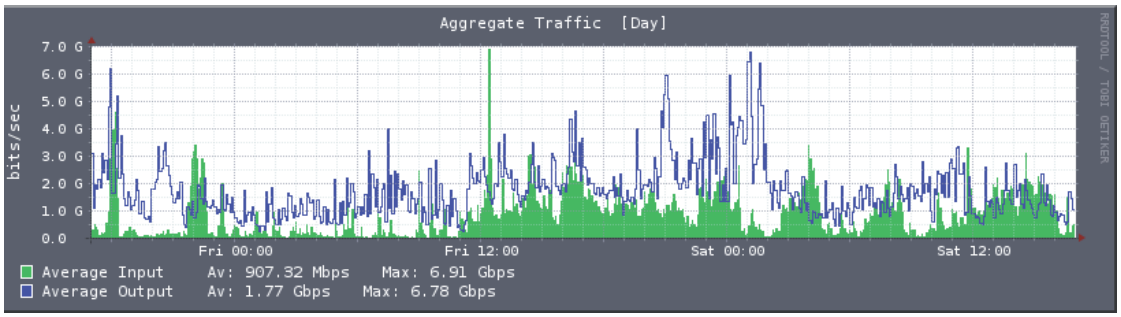


Fig. 1 Due giorni di traffico nella sede italiana del Tier1 presso INFN-CNAF (dal 6 novembre 2011, ore 18)

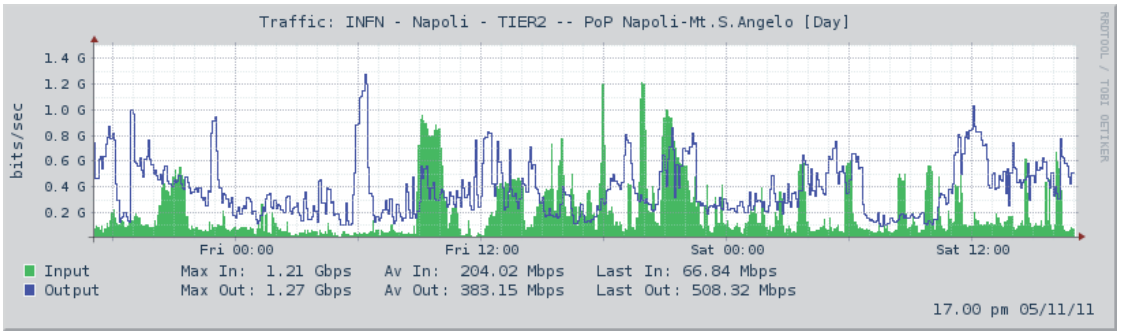


Fig. 2 Due giorni di traffico nella sede italiana del Tier2 presso INFN-Sezione di Napoli (dal 6 novembre 2011, ore 18)

tervallo di 48 ore di servizio.

Questo tipo di approccio di misura, che osserva lo stato di funzionamento in un punto di accesso della rete, non permette da solo di valutare il funzionamento complessivo del servizio di trasmissione dei dati da e verso queste sedi, a tal fine è necessario condurre un'analisi di correlazione delle informazioni che consenta di determinare la Matrice di Traffico.

2.1.1 Matrice di traffico

Al fine di analizzare nel dettaglio quali siano i flussi di traffico (IP) sulla rete viene utilizzato il protocollo Netflow [6] mediante il quale, sempre mantenendo un approccio "puntuale" proprio della misura di tipo Passive, è possibile conoscere le sorgenti e le destinazioni del traffico utente. Mediante l'acquisizione delle informazioni relative ai flussi di traffico è possibile per esempio conoscere quale frazione di traffico riguarda esclusivamente le due sedi sopra citate (*fig. 3*).

Questa informazione fornisce una misura estremamente utile ai fini progettuali e di gestione della rete, in quanto consente di valutare soluzioni tecniche mirate, in grado di veicolare il traffico in modo efficiente. Un esempio di matrice di traffico su di una scala più ampia è quello in uso per il monitoring dell'ENEA così come riportato in figura 4.

Alcuni anni fa, dall'analisi periodica sulle

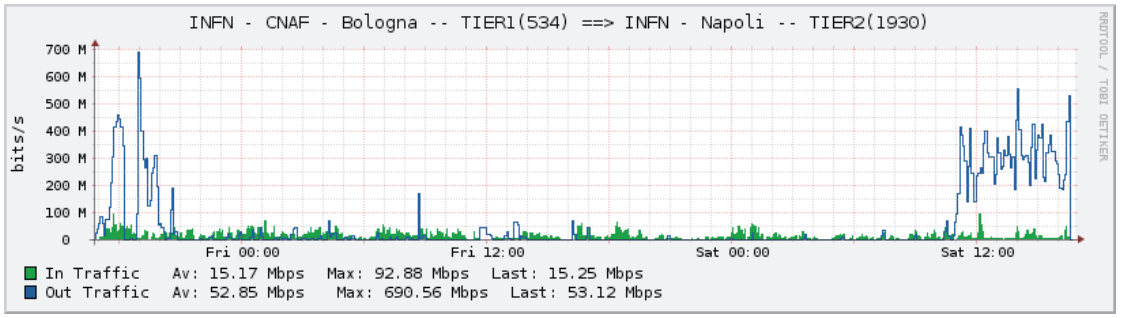


Fig. 3 Traffico tra le sedi Tier1 al CNAF e Tier2 a Napoli misurato utilizzando Netflow

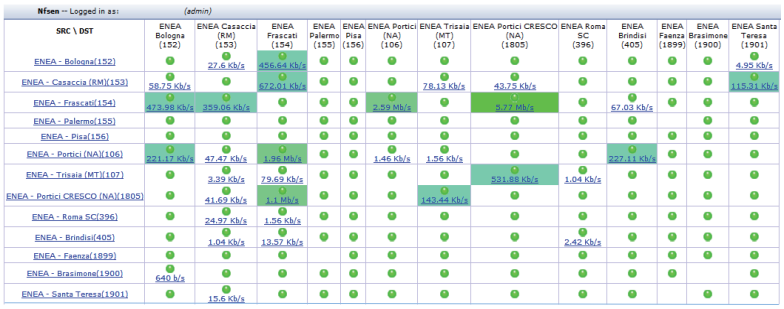


Fig. 4 Matrice di traffico IP tra le sedi ENEA

principali sorgenti di traffico sulla rete GARR, si è visto come Google stesse crescendo ad un ritmo annuo (>3) superiore al valore medio di crescita del traffico di rete (~1,3) e come questo avrebbe presto potuto rappresentare un problema di crescita dei costi del servizio di transito verso il General Internet. Dall'osservazione di tale fattore di crescita si è deciso di attivare un collegamento "diretto" tra GARR e Google al fine di ridurre il volume di traffico scambiato attraverso i normali canali di accesso al General Internet.

Per ogni sede GARR o collegamento di peering esterno (*fig. 5*) è possibile conoscere quali siano le sorgenti e le destinazioni di traffico aggregato in dato intervallo di tempo semplicemente attraverso la selezione di una regione grafica ottenuta a partire dal grafico d'uso della rete. Questo strumento di analisi del traffico agevola in modo straordinario il lavoro dei progettisti di rete.

2.2 Active Monitoring

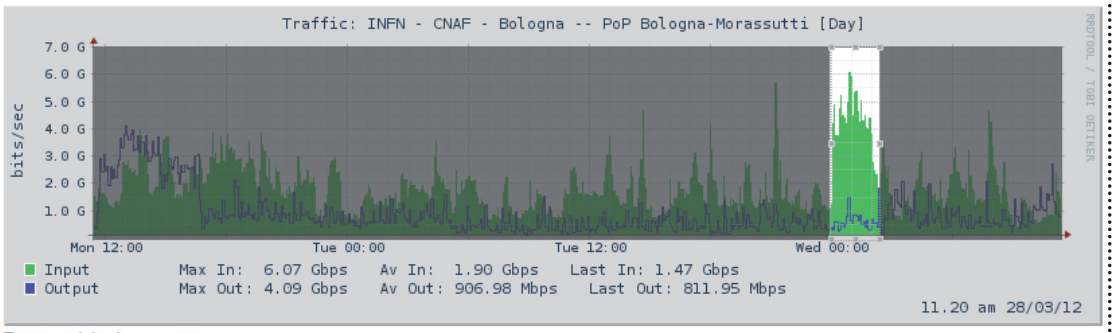
La misura di monitoring tipo Active è per sua natura intrusiva, in quanto mescola al traffico di produzione il traffico di monitoraggio. Poiché è perturbativa, la sua implementazione deve essere adottata con cautela al fine di non rappresentare motivo di malfunzionamento.

Ciò premesso, le misure di monitoring di tipo Active sono estremamente efficaci per avere informazioni reali su Delay, Jitter e Drop. In linea di principio si possono ottenere anche informazioni relative alla banda disponibile, tuttavia non è stata in alcun modo codificata una modalità di analisi della banda disponibile in un determinato istante. Alcuni metodi utilizzati, come per esempio iperf (Internet Performance), valutano la disponibilità di banda tra due punti della rete in termini della possibilità di saturare la capacità dell'intero percorso di rete. Questa modalità presenta due distinte controindicazioni, la prima riguarda il fatto che nell'intervallo di tempo in cui viene eseguita la misura, ovvero iniettando un flusso di dati alla massima capacità, un eventuale utente che volesse utilizzare la stessa porzione di rete la troverebbe già impegnata, la seconda e più importante è che, nonostante l'esito della misura, non si avrebbe comunque la garanzia di reale disponibilità della banda in un tempo successivo alla misura.

Strumenti di questo tipo sono utilizzati all'interno della rete GARR dal 2005 e fanno parte di un'infrastruttura di controllo internazionale atta ad analizzare eventuali malfunzionamenti di rete [7] ed hanno il solo scopo di supportare la gestione dei malfunzionamenti nel caso in cui si presentino limitazioni prolungate nell'uso della rete alle sue massime prestazioni.

3. Cosa sta facendo GARR

Il GARR ha sviluppato una propria piattaforma di controllo [1], mediante la quale riesce a valutare e rendere disponibile ai propri utenti lo stato di funzionamento dei servizi di rete erogati. La rete è un sistema complesso all'interno del quale coesistono diversi meccanismi che partecipano al funzionamento globale, è solo attraverso il controllo di questi meccanismi che è possibile fornire un servizio affidabile nel tempo. Ogni utente può controllare lo stato del proprio accesso alla rete (*fig. 1*) così come l'intero funzionamento della rete nella sua globalità (*fig. 6*). Nel caso in cui ven-



Router:rt1.bo1.garr.net
IP:193.206.128.17
Ifindex:229
Class_Type: access
Select an area on the graph:
Start Date: Tue Mar 27 2012 23:50:24 GMT+0200
End Date: Wed Mar 28 2012 02:06:24 GMT+0200
get flow details | get sites details

Posizione	Sorgente	Destinazione	Traffico	% sul totale: 4.49 TB
1	INFN - CNAF - Bologna -- TIER1	INFN - Roma1 -- TIER2	1.25 TB	27.94%
2	INFN - CNAF - Bologna -- TIER1	INFN - LNF - Frascati	739.51 GB	16.08%
3	INFN - CNAF - Bologna -- TIER1	INFN - Milano -- TIER2	442.96 GB	9.63%
4	INFN - CNAF - Bologna -- TIER1	INFN - Torino	418.48 GB	9.1%
5	INFN - CNAF - Bologna -- TIER1	INFN - Napoli -- TIER2	350.82 GB	7.63%
6	INFN - CNAF - Bologna -- TIER1	INFN - Catania -- TIER2	135.44 GB	2.95%
7	INFN - CNAF - Bologna -- TIER1	INFN - Padova	104.96 GB	2.28%
8	INFN - CNAF - Bologna -- TIER1	INFN - Bari -- TIER2	75.25 GB	1.64%
9	INFN - LNF - Frascati	INFN - CNAF - Bologna -- TIER1	72.65 GB	1.58%
10	DFN-IP(AS680)	INFN - CNAF - Bologna -- TIER1	61.8 GB	1.34%
11	INFN - CNAF - Bologna -- TIER1	INFN - LNF - Frascati -- KLOE	43.42 GB	0.94%
12	CERN CERN(AS513)	INFN - CNAF - Bologna -- TIER1	41.8 GB	0.91%
13	INFN - CNAF - Bologna -- TIER1	BCNET-AS(AS271)	40.49 GB	0.88%
14	INFN - CNAF - Bologna -- TIER1	POZMAN-EDU(AS9112)	32.7 GB	0.71%

Fig. 5 Analisi del traffico in modalità grafica basato su Netflow

gano riscontrate difformità dall'ipotesi iniziale di funzionamento, l'utente ha la possibilità di comunicare con il reparto del GARR-NOC che è in grado di analizzare, congiuntamente con l'utente, le possibili cause di malfunzionamento e di agire di conseguenza.

Indipendentemente da quali e quanti strumenti di controllo si possano mettere in campo, l'effettiva capacità di erogare un servizio si misura nel momento in cui qualcosa non funziona. Come abbiamo detto si hanno due distinte situazioni: l'indisponibilità ed il degrado. Nel primo caso la risoluzione passa attraverso la suddivisione del servizio erogato nelle sue componenti di base e la verifica dello stato di funzionamento di ognuna di esse con il conseguente ripristino del servizio. Se il problema è di natura software, il ripristino può avvenire in modo sufficientemente rapido, mentre nel caso di un guasto su di una componente "unica" il tempo di ripristino può richiedere alcune ore. Nel caso del degrado la situazione è più articolata in quanto coinvolge non solo l'insieme delle componenti che partecipano all'erogazione del servizio, ma anche l'applicazione utente.

In queste circostanze è necessario agire utilizzando strumenti di monitoraggio attivo tali da riprodurre il comportamento dell'applicazione. Al fine d'individuare l'elemento che causa il degrado, si agisce, analogamente al

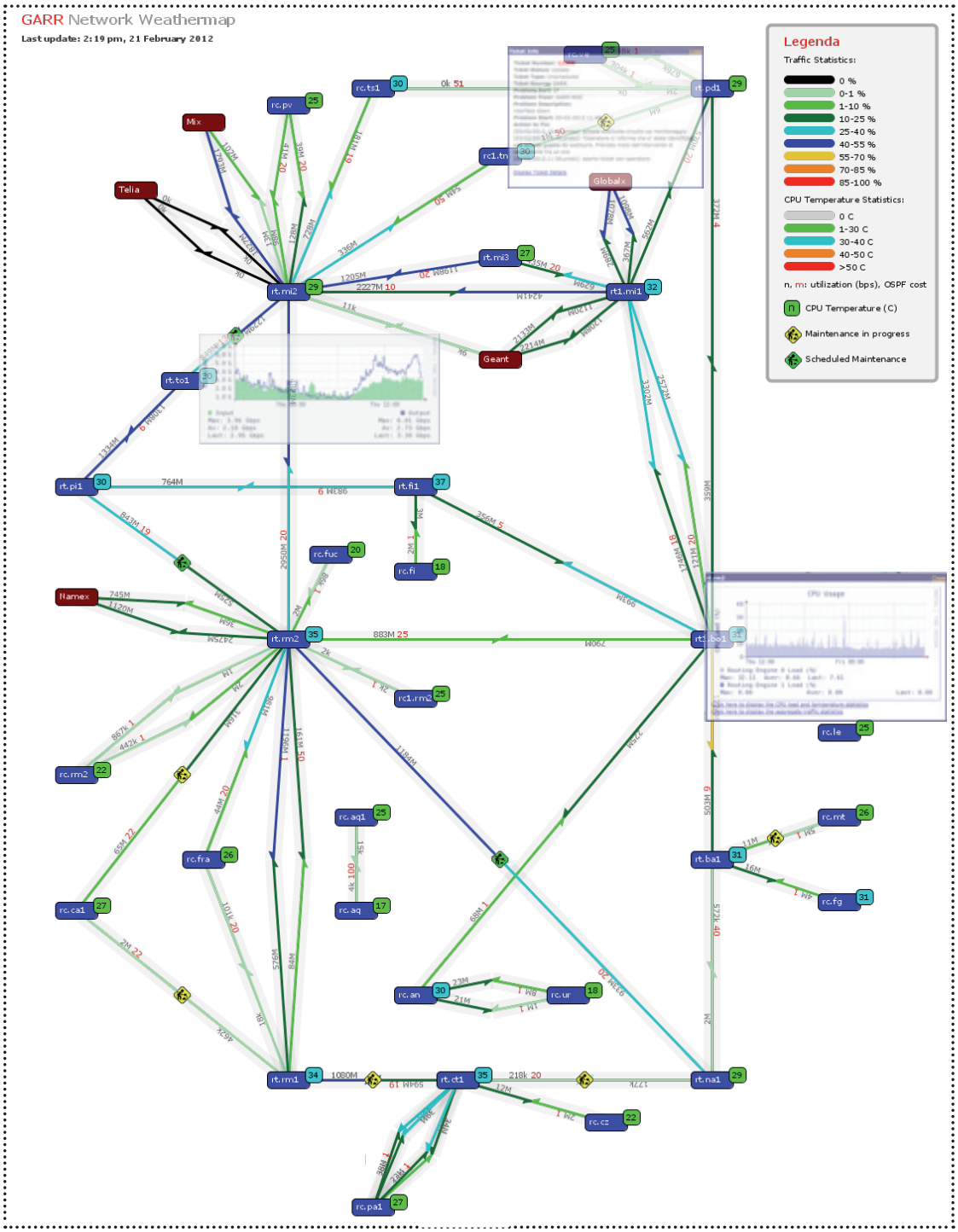


Fig. 6 Wheathermap interattiva della rete GARR

caso dell'assenza o indisponibilità di servizio, simulando il comportamento dell'applicazione nelle sottosezioni di rete. Questo tipo di attività richiede una conoscenza approfondita non solo dei protocolli di rete, ma anche di come questi agiscono all'interno dei sistemi di calcolo, così come del protocollo TCP/IP. Tali competenze costituiscono parte integrante della formazione del personale del GARR-NOC. Questa attività viene svolta in molti casi in accordo con un gruppo molto più ampio che opera a livello europeo ed è coordi-

nato nell'ambito del progetto di rete paneuropea GÉANT [8] nel quale GARR è impegnato attivamente.

3.1 Sicurezza

Data la natura della rete GARR quale rete privata di indirizzi pubblici, è necessario porre l'attenzione anche su aspetti che non riguardano esclusivamente il tradizionale contratto di servizio (che regola la funzionalità della rete), ma anche quelli legati alla gestione della sicurezza così come l'analisi del tipo di utilizzo che l'utenza fa della rete.

L'analisi dei flussi di rete IP condotta costantemente da GARR mediante il protocollo di rete Netflow [6] consente di conoscere la matrice di traffico d'uso della rete GARR (AS-Matrix), sia tra le sedi utente (*fig. 4*) che verso l'esterno della rete. Tali informazioni sono state utilizzate per progettare l'evoluzione della rete GARR (GARR-X) [2] e allo stesso tempo sono di supporto per gli utenti in quanto consente loro di definire meglio i propri requisiti di rete, di prevedere possibili evoluzioni e di adattare le proprie applicazioni in base all'effettivo uso della rete.

Lo strumento di analisi dei flussi di traffico fornisce inoltre un importante supporto alla gestione della sicurezza della rete. Tale aspetto può essere affrontato in maniera:

- *reattiva*: assistendo gli utenti nella gestione degli incidenti di sicurezza, informandoli e supportandoli nella realizzazione di misure preventive atte a ridurre l'impatto degli incidenti;
- *proattiva*: utilizzando l'acquisizione e l'analisi costante dei flussi di traffico sulla rete. Mediante l'analisi dei flussi è infatti possibile individuare le sorgenti (indirizzo IP) che stanno facendo scansioni sulla rete o che sono state oggetto di attacco. Questa azione si svolge sia in modalità online che in modalità offline al fine di stabilire a posteriori quali siano state le cause.

GARR ha da sempre curato con attenzione gli aspetti legati alla sicurezza della rete e dei servizi fornendo un supporto dedicato alla propria utenza. Sin dall'inizio, all'interno del GARR è presente un gruppo di esperti di sicurezza informatica (GARR-CERT) che si occupa della gestione e della prevenzione degli incidenti di sicurezza, in collaborazione con il GARR-NOC che opera sulla rete.

Utilizzando le informazioni relative ai flussi IP, generate dalle informazioni raccolte con il protocollo Netflow, viene offerto un supporto agli operatori di rete per evidenziare eventi malevoli che si verificano nella propria infrastruttura. In figura 7 viene riportato il caso di un Denial of Service (DoS) verificatosi nella rete GARR tra Gennaio e Febbraio 2012, i dati riguardano il traffico presente su uno dei router GARR, nella stessa figura sono rappresentati sia i dati di traffico (in arancio) che il numero di pacchetti relativi al solo protocollo UDP (in azzurro).

È evidente come il volume di traffico non sia adeguato a fornire l'evidenza di alcuna anomalia mentre quello relativo al rate dei pacchetti mostri un grosso "picco" in corrispondenza dell'evento malevolo.

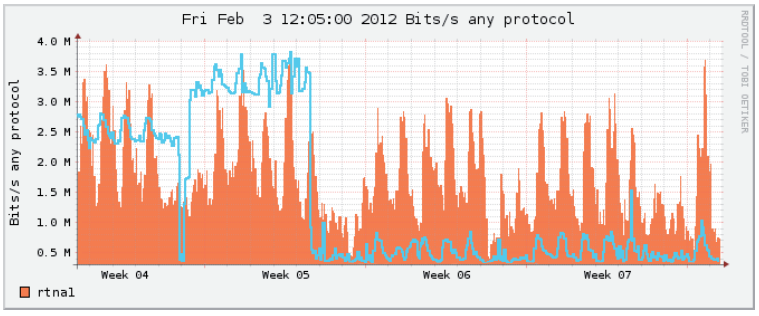


Fig. 7 Esempio di Denial of Service

4. Conclusioni

Gli elementi che riguardano l'evoluzione della rete GARR riguardano da un lato l'implementazione dell'infrastruttura in fibra ottica nota come GARR-X e dall'altra l'integrazione all'interno di essa del paradigma appli-

cativo che può essere sintetizzato con il termine Cloud.

Da una parte la rete in fibra ottica sta favorendo l'evoluzione della capacità di accesso delle sedi utente connesse in fibra ad almeno 1Gbps, con capacità di accesso singolo fino a 100Gbps. Tali accessi potranno far parte di un insieme di reti private virtuali (VPN) sia nel dominio ottico che in quello IP. La modalità di monitoring che può essere attivata nei due casi è diversa, sia in termini di strumenti utilizzati che di metriche di valutazione da mettere a disposizione degli utenti. Nel caso di reti virtuali nel dominio ottico (Optical Private Network) l'informazione che verrà resa disponibile riguarda gli aspetti connessi con la qualità della trasmissione dati (per esempio in termini di BER, Bit Error Rate, del canale trasmissivo o lambda). Nel caso invece di VPN nel dominio IP è possibile operare un monitoraggio attivo mediante l'inserimento di sonde negli apparati di rete. Tali sonde sono in grado di simulare il comportamento dell'applicazione utente e quindi di evidenziare eventuali difformità nell'erogazione del servizio di rete, sia per il traffico IPv4 che IPv6. In questi anni la comunità GARR ha infatti maturato un elevato livello di conoscenze tali da consentire un efficace controllo del funzionamento e delle prestazioni del traffico in IPv6, così come stiamo facendo con IPv4, sia all'interno delle VPN che nell'uso generale di Internet.

Ma non è solo l'infrastruttura di rete che evolve, è infatti in forte crescita la diffusione e lo sviluppo, anche da parte degli stessi utenti finali, di applicazioni accessibili mediante semplici interfacce web (paradigma cloud) e da differenti tipi di device come desktop, laptop, tablet, ecc, la cui funzionalità e qualità dipendono certamente dalle prestazioni dell'infrastruttura di rete sottostante, ma anche dallo strato applicativo intermedio, deputato al controllo dell'accesso alle applicazioni e costituito da sistemi di autenticazione e autorizzazione, sistemi di accesso nomadico alla rete, meccanismi di sicurezza come firewall, ecc. La lista mostrata in tabella 1 dovrà considerare questi servizi applicativi di fatto come nuovi servizi di rete. Ciò comporta necessariamente l'integrazione ancora più stretta che in passato tra la rete e le applicazioni, come parte di un unicum fornito ai propri utenti.

Le attività di controllo, osservazione e misurazione dovranno pertanto tenere conto di questi nuovi elementi al fine di valutare complessivamente la funzionalità e la qualità della rete e dei servizi applicativi.

Riferimenti bibliografici

[1] GINS. GARR Integrated Networking Suite http://www.gins.garr.it

[2] La rete GARR-X, http://www.garr.it/garr-x

[3] RFC 1157 - A Simple Network Management Protocol (SNMP)

[4] MRTG. Multi Router Traffic Grapher. http://www.mrtg.org

[5] Round Robin Database. About RRDtool. http://oss.oetiker.ch/rrdtool

[6] NETFLOW. RFC3954 Specification http://www.ietf.org/rfc/rfc3954.txt

[7] Web100 based Network Diagnostic Tool http://ndt.garr.net; http://ndt1.garr.net

[8] GÉANT Network, http://www.geant.net

[9] GARR-CERT. Gestione Incidenti di Sicurezza, http://www.cert.garr.it

Massimo Carboni
massimo.carboni@garr.it
È un fisico dell'INFN, si occupa di reti e calcolo scientifico dal 1990. Attualmente è il responsabile dell'infrastruttura di rete GARR, ed è il responsabile tecnico del progetto di rete GARR-X.