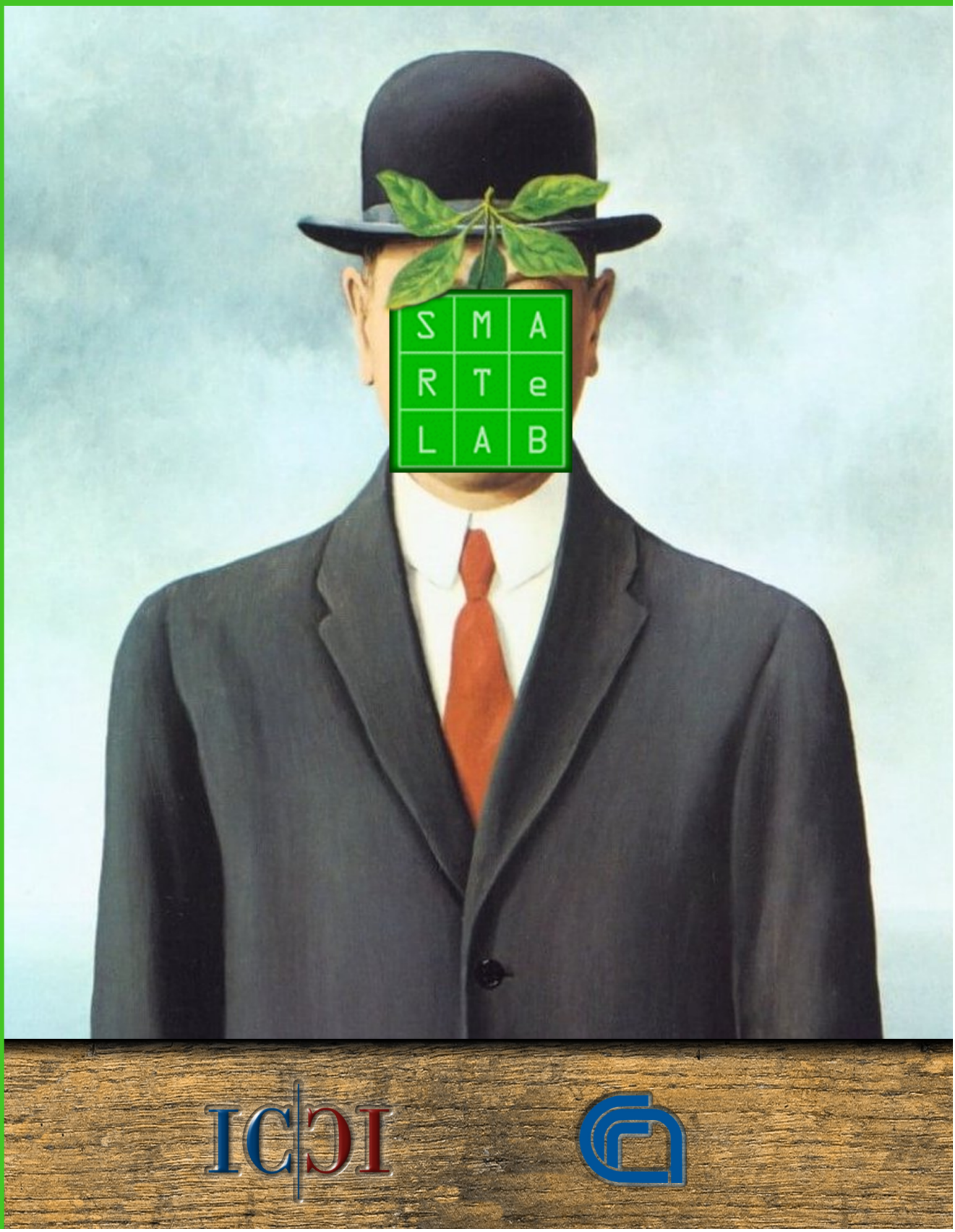
SMART eLAB

VOLUME 2 - ANNO 2013



ISSN 2282 - 2259

SMART eLAB

SOMMARIO
Vol. 2, 2013

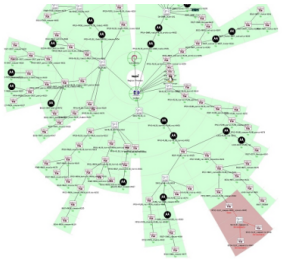
Articoli

Smart e-Lab: http://smart-elab.mlib.ic.cnr.it
A peer-reviewed online resource, published by the Istituto di Cristallografia (CNR-IC)
EDITORS-IN-CHIEF : Michele Saviano, Augusto Pifferi - ASSOCIATED EDITOR : Guido Righini
GRAPHIC DESIGN : Claudio Ricci - EDITORIAL ASSISTANT : Caterina Chiarella
CNR - Istituto di Cristallografia, Strada Provinciale 35/d, I-00015 Monterotondo, Italy

Networking

Analisi e Implementazione di Sistemi per il Monitoraggio della Rete Wireless Relativa al Progetto ADD (Anti Digital Divide) e delle Infrastrutture di Campus AdR RM1.†

Augusto Pifferi,[a] Giuseppe Nantista,[a] Luca Ianniello,[a] Andrea Lora,[a] and Marco Simonetti.[a]



In questo documento verranno valutati 3 sistemi di monitoring Open-Source (Nagios, Cacti e Zabbix) e si mostreranno sia le peculiarità che i differenti pro e contro. Verrà esposto il funzionamento di ogni singolo sistema con le relative operazioni di installazione e configurazione, al fine di fornire un quadro completo delle potenzialità dei mezzi. Infine verrà illustrato l'utilizzo dei tre sistemi di monitoraggio nel caso reale della rete di campus dell'Area della Ricerca Roma 1 e della rete wireless realizzata nel territorio della sabina romana e reatina.

Keywords: Monitoring System, Zabbix, Cacti, Nagios.

1 Introduzione

Gestire un'architettura ICT complessa è un processo che si articola in più fasi, tutte indispensabili al mantenimento in linea dei servizi offerti, dalla progettazione, configurazione e allestimento della rete, atta a offrire il servizio agli utilizzatori, fino alla gestione dei server che ospitano il servizio stesso.

Successivamente alla fase di deployment della struttura e del servizio, inizia una attività fondamentale per mantenere il servizio correttamente funzionante: il monitoraggio dei sistemi, che avrà durata pari a quella del servizio stesso.

Un approccio non automatizzato al monitoring non è pensabile per tre ragioni fondamentali:

- Il monitoring è un'operazione time-consuming;
- Al fine di minimizzare i tempi di ripristino è necessario intervenire tempestivamente;
- In determinati casi il problema è preceduto da una situazione di instabilità di un sistema, non sempre tangibile da un osservatore umano.

La risposta informatica all'esigenza di sollevare l'uomo dal monitoring è stata la creazione di appositi software che permettano di configurare una serie di controlli finalizzati alla raccolta di dati e facciano partire specifiche azioni a seguito del manifestarsi di condizioni prestabilite.

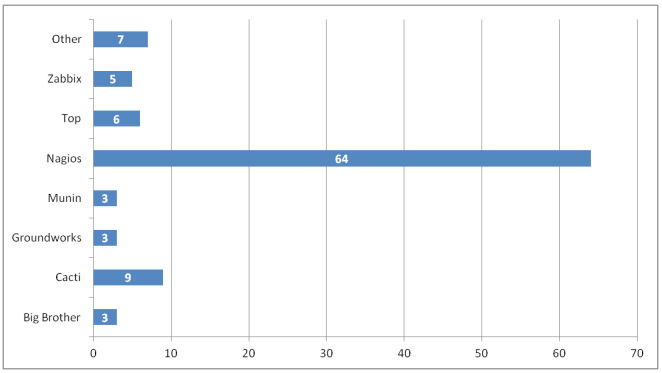


Fig. 1 Diffusioni prodotti OpenSource per il monitoraggio di reti e sistemi ICT.

Nell'ottica quindi di un controllo costante delle infrastrutture ICT all'interno e all'esterno dell'Area della Ricerca Roma 1 del CNR di Montelibretti si è effettuato uno studio dei prodotti Open Source esistenti in rete, quindi sono state realizzate e configurate diverse piattaforme.

2 NAGIOS

2.1 Introduzione

Poiché risultava essere il più diffuso e il più documentato, la prima scelta è ricaduta su Nagios.

Il software è distribuito gratuitamente con licenza GNU – GPL; maggiori informazioni sono disponibili sul sito http://www.nagios.org/

Nel caso specifico il software è stato installato su distribuzione Linux Debian 6.0.3 squeeze su hardware virtuale

[a] *CNR - Istituto di Cristallografia, Strada Provinciale 35/d, Montelibretti, Italia*

† Rapporto tecnico IC-RM/1058 protocollato in data 03/07/2012

VMWare ESXi 5.0

- 1 virtual cpu Xeon®2.0 ghz
- 1 GB ram
- 16 GB hard disk
- 1 GBit ethernet LAN

Nagios possiede un'interfaccia web attraverso la quale è possibile monitorare dispositivi, utilizzando un diverso livello di dettaglio; inoltre è possibile configurare un sistema di invio notifiche riguardante i malfunzionamenti, basato sull'invio di e-mail.

Nagios è in grado di monitorare anche host e servizi, inoltre può essere completato attraverso l'applicazione di scripts e plug-in.

Tale operazione di completamento consente un'ottima flessibilità, tuttavia richiede eccessivo dispendio di tempo perché l'unico modo di configurare il software è da CLI (command line interface).

Una caratteristica interessante è la possibilità di definire, anche graficamente, dipendenze tra apparati monitorati, tramite la costruzione di grafi ad albero, che permettono di evidenziare immediatamente le dipendenza padre-figlio, così da individuare il nodo dell'albero sul quale si è verificato un problema.

2.2 Configurazione

Avendo usato come distribuzione Debian, l'installazione è stata immediata, il gestore di pacchetti ha risolto automaticamente tutte le dipendenze.

```
root@nagios:/# apt-get install nagios3
```

A questo punto la configurazione vera e propria ha riguardato i file relativi agli host da monitorare. Per semplicità ci siamo basati sul template "generic-host"

```
root@nagios:/# more /etc/nagios3/conf.d/generic-host_nagios2.cfg

8< ----------------------

define host{
name            generic-host    ; The name of this host template
notifications_enabled       1 ; Host notifications are enabled
event_handler_enabled       1 ; Host event handler is enabled
flap_detection_enabled      1 ; Flap detection is enabled
failure_prediction_enabled  1 ; Failure prediction is enabled
process_perf_data           1 ; Process performance data
retain_status_information   1 ; Retain status information across
     program restarts
retain_nonstatus_information 1 ; Retain non-status information
     across program
check_command                   check-host-alive
max_check_attempts              10
notification_interval           0
notification_period             24x7
notification_options            d,u,r
contact_groups                  admins
register                        0
}

---------------------- >8
```

Nella configurazione dei singoli host sono state aggiunte solo le informazioni specifiche, come l'indirizzo IP, il nome di sistema e il parent, ossia l'apparato che, in una struttura ad albero, risulta essere il padre dell'host in questione. La totalità delle dipendenze padre-figlio vengono automaticamente gestite da Nagios, che costruisce la site-map (Figura 2).

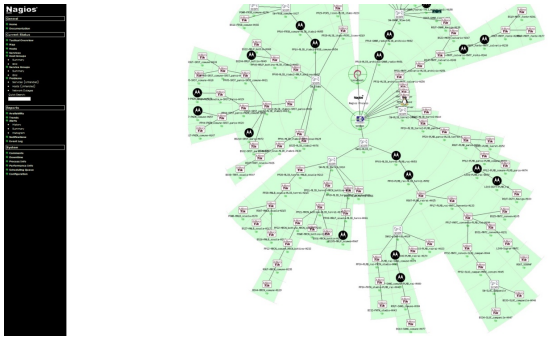


Fig. 2 Mappa di Nagios.

```
root@nagios:/# more /etc/nagios3/objects/host_totali.cfg

8< ----------------------

define host {

use                     generic-host
host_name               BS01-MRCN_bottin-H173
alias                   alias
address                 10.10.235.173
parents                 PP21-MRCN_bottino-MLIB_torre1-H172
contact_groups          admins

}

---------------------- >8
```

Anche gli host sono stati separati in categorie nell'ottica di raggrupparli per tipologie di controlli differenti.

Infine, per distinguere a colpo d'occhio il manufacturer dell'apparato, è stata associata un'icona ed esplicitato il tutto nel file hostextinfo che estende le informazioni appartenenti a un determinato gruppo.

```
root@nagios:/# more /etc/nagios3/objects/hostgroup_totali.cfg

8< ----------------------

define hostgroup {
hostgroup_name   Mikrotik
alias            alias
members         BS01-MRCN_bottin-H173, BS02-SRST_parco-
                                              H014, BS03-PLMB_
}

---------------------- >8
```

Tali configurazioni sono state effettuate seguendo scelte personali e non sono un dictat di Nagios stesso, che invece permette diverse varianti di configurazione a seconda dei gusti o delle specifiche finalità dell'amministratore.

2.3 Visualizzazione

Nelle successive due immagini è visualizzata la classica MAP di Nagios, costruita automaticamente dall'engine prendendo spunto esclusivamente dalle relazioni di parentela specificate in fase di definizione degli host. Si noti come, in caso di down di un ramo (Figura 3) l'attenzione va subito al nodo in cui si è interrotta la comunicazione, facilitando la comprensione del guasto e mettendo in moto rapidamente le procedure di ripristino.

2.4 Valutazioni

L'utilizzo di questa piattaforma ha evidenziato, almeno dal nostro punto di vista, alcuni limiti:

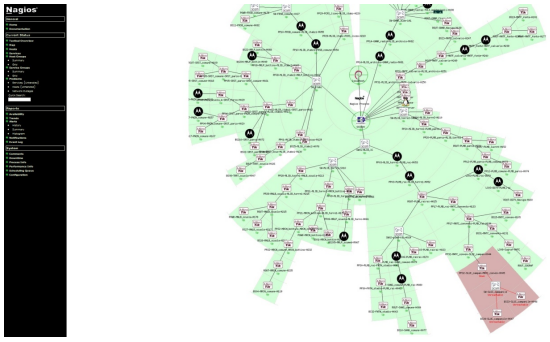


Fig. 3 Mappa di Nagios con evidenziato malfunzionamento host.

- L'installazione, nella sua versione di base, non include uno strumento per la raccolta, memorizzazione e visualizzazione grafica di semplici dati, quali l'utilizzo di CPU, il traffico sulle interfacce di rete, ecc.
- Come già detto, tutta la configurazione, compresa la definizione di allarmi, avvisi e relative soglie di attivazione, si effettua esclusivamente via CLI, rendendo l'operazione poco intuitiva.

3 CACTI

3.1 Introduzione

Il secondo software valutato è stato Cacti, anch'esso distribuito con licenza gratuita GNU – GPL e scaricabile all'indirizzo http://www.cacti.net/

Data la quantità ridotta di risorse richieste e l'assenza di conflitti, è stato installato sulla stessa macchina virtuale utilizzata per Nagios.

Immediatamente si evidenziano due vantaggi:

- La semplice e rapida gestione degli host e dei servizi da monitorare, completamente configurabili via web interface
- La presenza, già nella configurazione di base, dei tool relativi a raccolta, immagazzinamento e visualizzazione grafica dei dati

Merita una nota il sistema utilizzato da Cacti per la memorizzazione dei dati raccolti, il database RRD (Round Robin Database). Questo tiene sotto controllo l'espansione del database, infatti i dati vengono immagazzinati con una densità variabile nel tempo. I dati sono raccolti con una cadenza frequente, ma vengono compressi, tramite media matematica, man mano che diventano più "vecchi", fino ad essere completamente sovrascritti una volta superato il tempo massimo di memorizzazione, che di default è fissato a un anno.

Risulta evidente quindi che, per ogni check effettuato dal software, è fissa la dimensione massima del database su cui i dati sono memorizzati. Questo sgrava l'amministratore di sistema da tutti i problemi relativi alla crescita incontrollata del database.

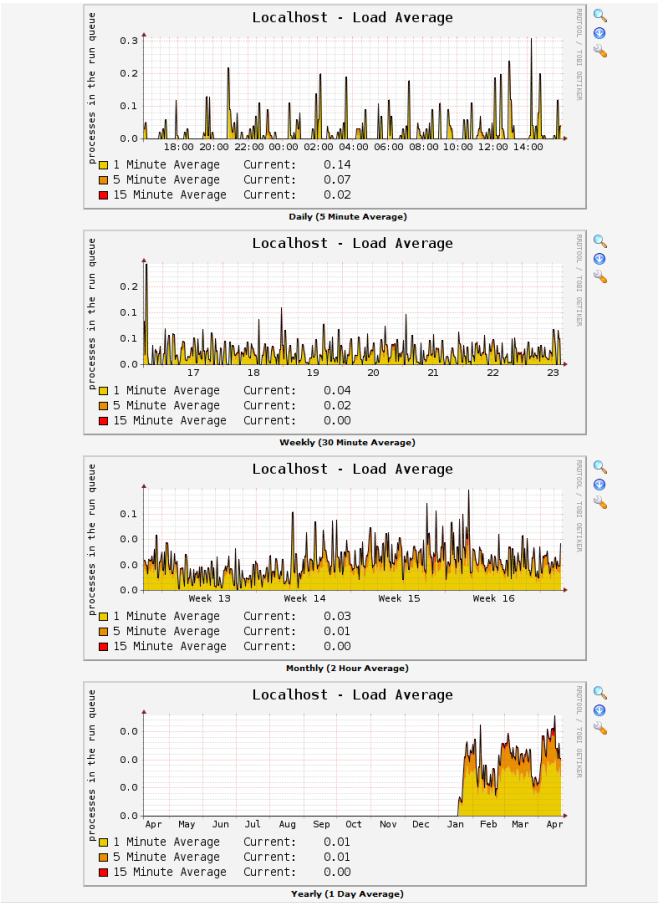


Fig. 4 Grafici e gestione database

3.2 Configurazione

Anche in questo caso la distribuzione Debian ha semplificato enormemente la fase di installazione, installando i componenti aggiuntivi in maniera automatica.

```
root@cacti:/# apt-get install cacti
```

Un aspetto che facilita molto l'inserimento nel database di un gran numero di host è la possibilità di definire dei template, ossia un elenco di controlli da associare a un gruppo di apparati. In questa maniera non appena un host viene creato e associato a un template, immediatamente sono disponibili tutti i relativi check. I template predefiniti sono relativamente pochi, ma è disponibile su internet una grande varietà di personalizzazioni. Nel nostro caso avendo nella rete alcuni host Mikrotik abbiamo aggiunto un template per questi apparati. Tutti i controlli effettuati da Cacti sono query SNMP, pertanto gli apparati devono essere compliant almeno con la versione v1 di tale protocollo.

Creare e visualizzare un grafico è semplice e immediato, questo è il motivo per cui questo strumento è stato preferito ad altri per avere una visione globale di quello che accade nella rete.

Nonostante non abbia, nel pacchetto base, strumenti per la definizione di una soglia di malfunzionamento, lo strumento dà la possibilità, previa osservazione diretta da parte di un osservatore umano, di accorgersi se un

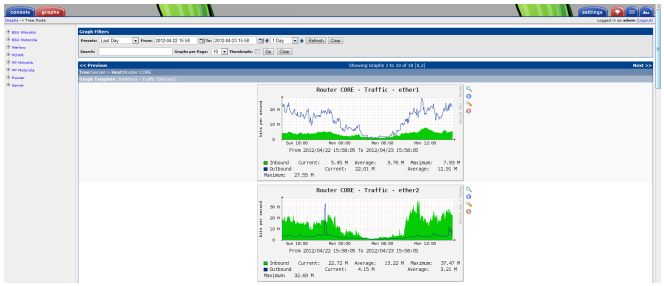


Fig. 5 Traffico in/out sulle interfacce di un router.

apparato funziona male, ad esempio se l'utilizzo medio della CPU è elevato, o se il traffico sulle interfacce arriva a saturazione, oppure se la latenza (icmp ping) sale eccessivamente.

3.3 Valutazioni

Cacti fornisce in definitiva uno strumento facilmente configurabile e particolarmente indicato per il monitoraggio di apparati di rete, non può prescindere dalla presenza di un operatore, ma grazie al database RRD può immagazzinare grandi moli di dati relativi alle osservazioni compiute e fornire un ottimo strumento per verificare le variazioni temporali nell'utilizzo di apparati di rete, prevenendo situazioni di collasso di apparati, ad esempio, per eccessivo utilizzo.

4 ZABBIX

4.1 Introduzione

Il terzo software valutato è stato Zabbix (http://www.zabbix.com). Rilasciato con licenza GNU GPL 2, Zabbix si propone come una soluzione integrata di Nagios e Cacti. Vengono infatti offerte all'interno dello stesso software sia la gestione degli allarmi che la possibilità di visualizzare gli storici dei dati raccolti dal sistema.

4.2 Configurazione Server

Dovendo decidere come approntare il server Zabbix abbiamo constatato che gli sviluppatori offrono una virtual appliance pronta da utilizzare, basata su openSUSE. Abbiamo optato per questa possibilità.

Le risorse assegnate tramite VMWare sono state di 1GB di memoria RAM fisica e 1 Virtual CPU del server VMWare, che nel nostro caso monta degli Intel(R) Xeon(R) CPU E5504@2.00GHz. Il link di rete è ad 1GBps. Per quanto concerne la scelta del sistema disco, essa dipenderà dalla localizzazione del database MySQL.

Nel caso di storage su server esterno, il traffico I/O di Zabbix su disco si limita a 3/5 kbit al secondo durante le fasi di monitoring, e lo spazio necessario è quello dell'installazione della distribuzione. Nel caso invece di server MySQL sulla stessa macchina Zabbix, lo storage locale deve essere aumentato, e le prestazioni del sistema dovranno essere monitorate per evitare che il traffico I/O disco saturi la macchina (I/O waiting).

Poiché le operazioni di I/O disco di Zabbix si limitano alla lettura/scrittura di dati sul server MySQL, a seconda del numero di host e del numero e della frequenza dei check, le query verso il database possono diventare numerose a tal punto da degradare le performances del sistema. Può dunque diventare conveniente delocalizzare il database MySQL fuori dalla macchina Zabbix. Questo è proprio il nostro caso, infatti Zabbix monitora 160 apparati, eseguendo circa 10 scritture su DB al secondo, per un totale di circa 650 check totali.

Una volta installato tutta la configurazione e consultazione avviene tramite interfaccia web, scritta in php, che si appoggia anch'essa su database MySQL. Rimandiamo alla pagina web di Zabbix http://www.zabbix.com/ per una lista esaustiva delle sue capacità, qui ci limiteremo ad elencarne le principali, comunque sufficienti ai nostri scopi.

4.3 Schema di funzionamento

Le modalità con cui funziona Zabbix sono mostrate nel seguente grafico. (fig. 6)

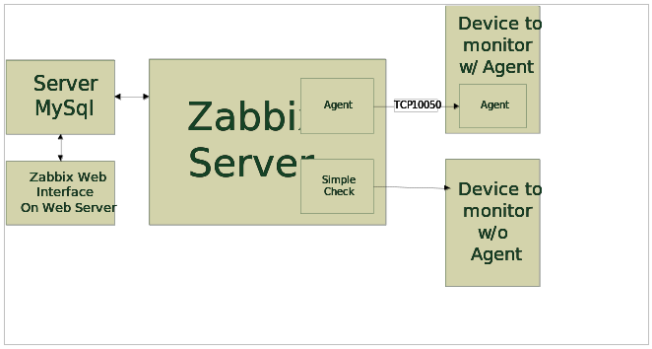


Fig. 6 Schema di funzionamento di Zabbix.

Il processo Zabbix server è il cuore del sistema, si occupa di eseguire tutti check e lanciare le eventuali azioni condizionali. Tutti i dati che il server raccoglie durante il suo funzionamento sono memorizzati su un database SQL. MySQL come già ribadito è il DBMS in questo momento supportato da Zabbix.

La Zabbix web interface è lo strumento con cui gli utenti si interfacciano al sistema. Essa non è legata al processo Zabbix server, e può essere ospitata fuori dalla macchina stessa. L'interfaccia infatti instaura una connessione con il server SQL direttamente, e non opera con il processo server se non tramite questo scambio dati.

L'interfaccia web permette sia la consultazione dei dati, sia l'inserimento/modifica/cancellazione di host e azioni di monitoraggio. Offre anche la possibilità di cambiare i meccanismi di controllo, e permette infine di inserire i classici Acknowledge sugli alert o lo scheduling di manutenzioni. Sempre dall'interfaccia andremo anche a

configurare le eventuali azioni che Zabbix dovrà eseguire in caso di una condizione determinata.

4.4 Zabbix Check

I controlli possono essere di diversi tipi, il sistema è stato infatti concepito per essere il più flessibile possibile. Se quindi vengono offerti di default controlli come quello della risposta al ping, della raggiungibilità di una ben precisa porta TCP o altri controlli basati su SNMP, nulla impedisce di costruirsi check propri, concepiti magari tramite un comando esterno.

I check esterni, chiamati in Zabbix simple checks, non riguardano una singola macchina, ma esprimono piuttosto un'azione che lo Zabbix server esegue. Tali check vengono eseguiti direttamente dalla macchina che ospita il processo Zabbix server, tramite i noti protocolli UDP/TCP. Le macchine da controllare dovranno solo rispondere alle richieste standard. Questo tipo di controlli non prevede particolari configurazioni sulle macchine da monitorare.

4.5 Zabbix Agent

Lo Zabbix agent, di contro, è un'ulteriore opzione che viene data per monitorare i sistemi. Si installa come servizio sulla macchina da monitorare e ha dunque accesso a tutte le informazioni di sistema della macchina stessa. Esso è disponibile per la maggior parte dei sistemi operativi correntemente in uso. L'agent mette a disposizione due tipi di check: attivi e passivi. Per check passivo viene inteso il meccanismo con cui Zabbix Server interroga lo Zabbix Agent (instaurando una connessione TCP tra i due). I check attivi invece vengono configurati direttamente nell'Agent, che si occupa di instaurare una connessione verso il server.

L'agent di Zabbix viene rilasciato come sorgente e come pacchetto precompilato. Nel caso di sistemi Linux esso è disponibili nei repository delle varie distribuzioni. L'installazione su Debian si limita a

```
root@debian:/# apt-get install zabbix-agent
```

Il file di configurazione /etc/zabbix/zabbix_agentd.conf andrà modificato per inserire a quale server Zabbix rispondere. Di base la riga da modificare è solo quella che riguarda l'hostname

```
Server=my.zabbix.server.fqdn
```

Eventualmente è possibile attivare l'esecuzione di comandi remoti aggiungendo questa riga al file

```
EnableRemoteCommands=1
```

Nel caso di sistemi Windows, dopo aver scaricato dal sito di Zabbix il pacchetto precompilato andremo ad estrarre in una directory a nostra scelta il file agent, scegliendolo in base al tipo di architettura che andremo a monitorare (32 o 64 bit). Nella stessa directory dovrà essere creato ex novo un file di configurazione. La

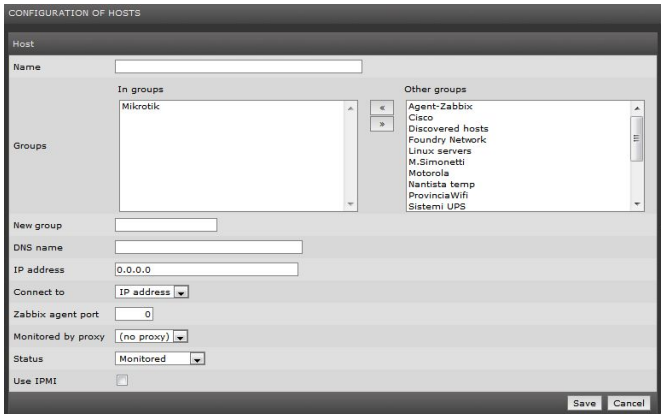


Fig. 7 Configurazione di un host.

configurazione base consiste in poche righe in cui vengono definiti il server a cui l'agent dovrà rispondere, il nome mnemonico del server e i parametri di fork. Per esempio memorizzeremo nel file agentd.conf il seguente contenuto

```
Server=my.zabbix.server.fqdn
Hostname=Windows Test
StartAgents=5
```

L'installazione viene eseguita a riga di commando, tramite un accesso a console Administrator (in caso contrario verrà visualizzato l'errore di accesso negato)

```
Zabbix_Agentd.exe -c agentd.conf -i
```

Il servizio verrà installato con parametri di esecuzione automatica, per eseguire il servizio la prima volta, se si vuole evitare il riavvio della macchina è sufficiente eseguire

```
Zabbix_Agentd.exe -c agentd.conf -s
```

5 ACL

Zabbix usa internamente un meccanismo di ACL (Access Control List) basato su utenti. Gli utenti possono essere raccolti eventualmente in gruppi, ai quali possono essere assegnati permessi per operare sul sistema. La dichiarazione di ruoli non è essenziale ai fini del funzionamento del sistema, ma diventa molto utile sia nella fase di reportistica (qualunque azione del sistema eseguita viene infatti loggata assieme all'utente), sia nella fase di escalation.

6 Hosts e Groups

L'inserimento degli host da controllare sarà sicuramente una delle prime attività con cui si avrà a che fare se si vuole utilizzare Zabbix. Un host è identificato da Zabbix con due parametri obbligatori: un'etichetta e un IP o un FQDN. Gli host possono essere raggruppati, al fine di applicare policy di controllo su interi gruppi piuttosto che su singoli hosts.

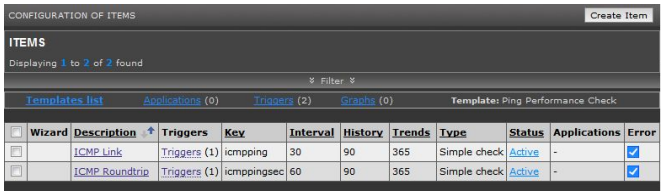


Fig. 8 Lista degli items attivi.

7 Items / Triggers / Actions

La distinzione tra items, triggers e actions è alla base per la comprensione del funzionamento di Zabbix nel suo processo di monitoring.

Gli items sono i dati grezzi raccolti dal sistema: tutte le caratteristiche che vogliamo controllare sono degli items. Questi possono essere frutto di misurazioni, come per esempio il tempo di roundtrip da un host all'altro, o la quantità di carico della macchina, oppure calcolati a partire da altri dati grezzi; per esempio si può calcolare la percentuale di spazio libero su disco a partire da dati quali la capacità totale e la capacità occupata.

I triggers descrivono una serie di condizioni, soddisfatte le quali Zabbix provvede ad entrare in uno stato di allerta. Nei trigger vengono inseriti dunque quei parametri che identificano eventuali problemi; ad esempio uno dei modi convenzionalmente utilizzati per dichiarare un host down è controllare il suo roundtrip dal server Zabbix. Se il valore massimo delle misurazioni negli ultimi 3 minuti è uguale a zero si suppone che l'host non sia raggiungibile. Al verificarsi di questa condizione nell'interfaccia di controllo Zabbix verrà visualizzato un nuovo problema. In questa fase non vengono inviate comunicazioni all'esterno, questo perché i triggers (come il loro nome fa intendere) non si occupano di eseguire una certa azione, ma fungono semplicemente da meccanismi di attivazione. I triggers hanno un campo descrittivo particolare, chiamato Severity, che descrive l'importanza del trigger stesso, consentendo azioni diverse a seconda di questo parametro.

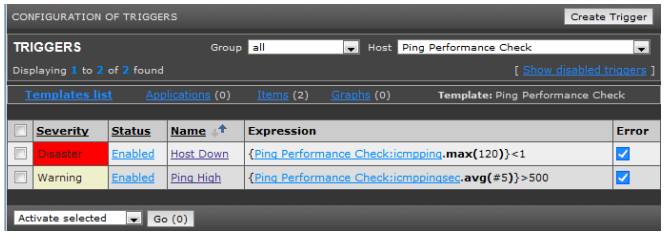


Fig. 9 Lista triggers attivi sul sistema.

Di base una action è semplicemente un'azione generica, che viene eseguita ogni volta che un trigger viene attivato. Una serie di parametri di configurazione permette di limitare l'esecuzione della action ai soli casi di interesse. Per esempio si possono configurare action che vengono eseguite soltanto nel caso in cui la gravità del

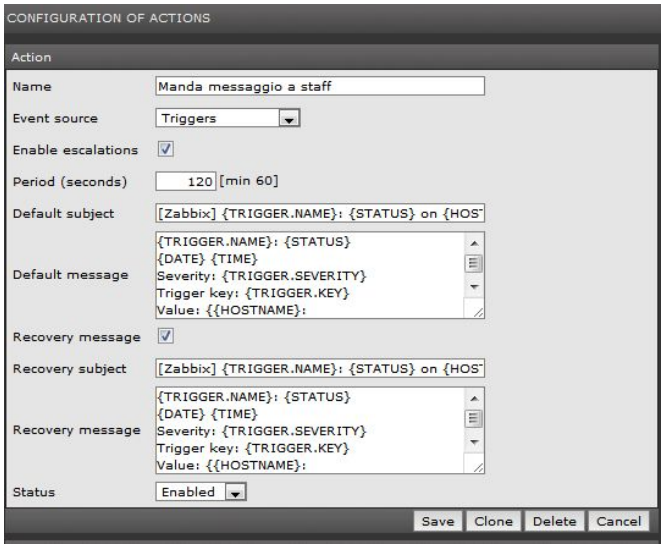


Fig. 10 Creazione di una action.

trigger sia di tipo "Disaster", o si può evitare che venga mandata in esecuzione nel caso il sistema sia posto in "Maintanence" mode, o ancora che venga ignorata nel caso in cui qualcuno abbia già eseguito l'operazione di Acknowledge del trigger.

Le actions sono in grado di eseguire due compiti: mandare un messaggio (attraverso i media configurati in Zabbix) o eseguire un comando (Zabbix server può eseguire un comando a nostra scelta). Il primo compito è quello che ci aspettiamo da un sistema di monitoring: a seguito di un trigger attivato un messaggio email viene inviato ad un gruppo di utenti Zabbix. Nel corpo del messaggio è possibile inserire tutti i dettagli riguardanti l'evento ricorrendo ad una serie di variabili che il sistema mette a disposizione. Il secondo caso fa sì che, a seguito dell'attivazione del trigger, Zabbix risponda con un comando lanciato sul server stesso, o, nel caso sia stato installato l'agent, direttamente sul server monitorato. Sul server "XYZ" il processo "QWE" non risponde da troppo tempo? Zabbix può tentare di riavviare il servizio, garantendo che il downtime sia minimo.

8 Escalations

Le escalations sono delle specializzazioni delle actions, estendono il loro comportamento introducendo il concetto di evoluzione temporale. Col passare del tempo l'azione esegue operazioni differenti. Supponiamo che un server sia down. Dopo 2 minuti viene inviata una mail allo staff IT che segnala il malfunzionamento. Questa mail verrà ripetuta ogni 60 minuti, o finché verrà dato l'Acknowledge dell'evento.

L'invio delle mail non è l'unica azione che Zabbix può eseguire, sebbene sia la più utilizzata. In casi particolari può essere più utile eseguire un comando. Zabbix mette a disposizione questa funzionalità tramite un nuovo tipo di operazione: "Remote Command".

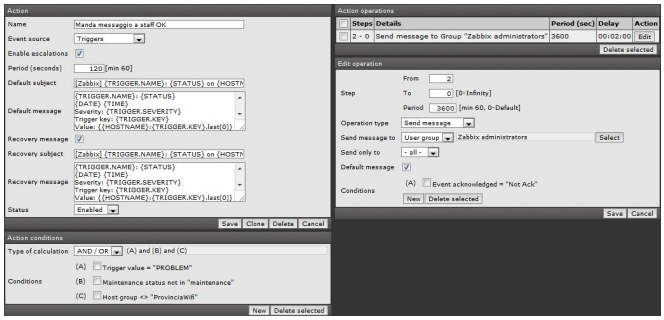


Fig. 11 Una action che prevede escalation.

Un esempio di questo tipo è visualizzabile nella prossima figura. Dopo 30 minuti dal rilevamento di un problema di severità “Disaster” (precedentemente definito nella configurazione degli host) sull’host “Zabbix Server” viene eseguito lo script /bin/send_sms.sh con parametri definiti a riga di comando come visto nello screenshot. Lo script si occupa di inviare ad un gateway mail-to-sms i contenuti dell’alert.

```
#!/bin/bash
echo $@ > /tmp/zabbix.txt
mail m2s@gatewaysms -s numerotelefono < /tmp/zabbix.txt
```

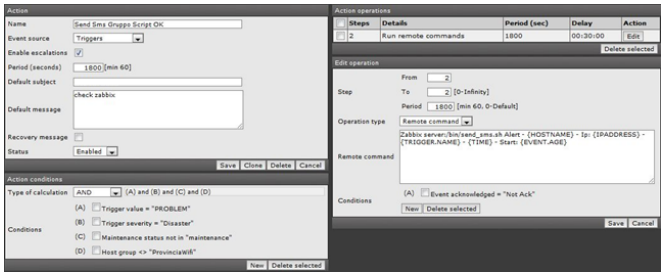


Fig. 12 Esecuzione di un comando remoto tramite Zabbix.

9 External Check

La presenza dell’agent su una macchina permette di monitorarne praticamente qualunque aspetto, attraverso le descrizioni che vengono inserite nel file zabbix_agentd.conf. Supponiamo di aver necessità di monitorare lo stato della replication master-slave tra due server MySQL. Abbiamo provveduto ad individuare i parametri che sarebbero stati necessari controllare. Una possibilità è quella di confrontare lo stato dei binary log files e verificare che il server slave non stia rimanendo indietro nell’applicazione degli stessi.

Sullo slave nello zabbix_agentd.conf aggiungeremo le righe

```
UserParameter=mysql.slaveposition,mysql -e “show slave status” -E
-uroot| grep Exec | cut -d ":" -f 2 | cut -d " " -f 2
```

Sul master nello zabbix_agentd.conf aggiungeremo le righe

```
UserParameter=mysql.masterposition,mysql   -e   “show   master   status”
-E -uroot | grep mysql-bin | cut -f 2
```

Gli items da monitorare in Zabbix a questo punto saranno mysql.slaveposition e mysql.masterposition, che sono le rispettive posizioni dei file bin log. Questi parametri, ad ogni controllo richiesto da Zabbix, assumeranno il valore dell’output dello script che viene descritto nei file di configurazione. Nel nostro caso un semplice intero.

Per poter capire se la replication sta avvenendo in maniera corretta andiamo a creare un terzo item di tipo Calculated che chiameremo BinlogDiff. I Calculated sono tipi astratti che derivano da operazioni eseguite su uno o più item reali, non necessariamente legati ad una singola macchina. In questo caso quello che ci servirà è la differenza tra la posizione del master e la posizione dello slave.

Un esempio di formula Calculated può essere il seguente

```
last(SQL Master:mysql.masterposition) - last(SQL
Slave:mysql.slaveposition)
```

Un valore pari a 0 indicherà che la replica sta funzionando a dovere. Un valore troppo alto indicherà dei problemi nella replication.

Il trigger dunque verrà lanciato a seguito del superamento di una soglia prestabilita proprio di BinlogDiff

10 Case study

10.1 Servizi Area

Nella nostra esperienza lavorativa i software descritti hanno un’importanza cruciale per il corretto svolgimento delle attività gestionali della rete. Sono utilizzati per tenere sotto controllo 71 switch e 21 access point, che sono presenti nei vari edifici e istituti attraverso dei semplici ICMP check, e quindi controllare basilarmente il loro corretto funzionamento. Abbiamo organizzato la struttura a gruppi, per capire dove fisicamente intervenire in caso di guasto. A seguito di malfunzionamento rilevato dal sistema esso invia una mail dopo 3 minuti dall’evento, nel caso esso non fosse stato nel frattempo risolto, e si occupa di inviarne un’altra ogni 15 minuti, fino alla risoluzione del problema o all’acknowledge dello stesso.

Discorso particolare invece è quello legato al monitoraggio delle macchine server presenti all’interno del CED; esse infatti hanno la possibilità di eseguire al proprio interno lo Zabbix Agent che, come precedentemente descritto, permette di tenere sotto monitoraggio non soltanto le risposte al ping (ICMP) ma anche lo stato generale del sistema mediante un gran numero di parametri, come la quantità di memoria o spazio disco disponibile, il carico della CPU, l’attività delle schede di rete fino al tipo e numero di processi in esecuzione. Ad esempio sul server web dell’Area della Ricerca viene tenuto sotto controllo lo stato del processo Apache, così da essere avvisati tempestivamente nel caso non dovesse rispondere

correttamente a seguito di qualche malfunzionamento o attacco informatico esterno.

10.2 Rete wireless geografica a 5Ghz

La rete 5ghz comprende più di 140 apparati da monitorare. Essi sono dispositivi eterogenei, e anche quelli che svolgono le stesse funzioni possono appartenere a costruttori differenti. Abbiamo dunque deciso dividere in gruppi i vari apparati sia secondo il costruttore che secondo il funzionamento. In tal modo ci siamo garantiti la possibilità di applicare template agli apparati secondo le nostre necessità. Abbiamo ovviamente mantenuto una template comune che si occupava di verificare i link, tramite un controllo icmp in cui si considerava solo il packetloss, e un altro che invece analizzava il round-trip, informazione utile per capire se i link radio erano soggetti a qualche tipo di deterioramento. Per tutti gli apparati che lo permettevano abbiamo monitorato via SNMP i parametri di utilizzo degli stessi, verificando che i valori di utilizzo cpu, memoria e spazio disco non oltrepassassero una soglia di allarme che non avrebbe garantito il corretto funzionamento. Altri dati vengono stockati senza che vi siano allarmi specifici per essi, ma se ne mantiene uno storico nel caso fosse necessario analizzarli a posteriori.

10.3 Tipologie di allarme

Per quanto concerne le action che vengono eseguite da Zabbix a seguito di evento, esse sono diverse a seconda della gravità del problema e della sfera di competenza. E' possibile infatti configurare gli invii di alert solo a specifici gruppi utente Zabbix. Nel caso più grave possibile, ovvero la perdita di link verso un determinato apparato, il sistema provvede ad inoltrare ai destinatari preimpostati una email dopo 2 minuti. Ne invierà un'altra ogni ora nel caso in cui il problema non dovesse essere risolto o riconosciuto tramite acknowledge. Oltre a questa azione, dopo 15 minuti dall'inizio del malfunzionamento viene eseguito uno script da Zabbix che tramite un gateway mailto-sms invia ai destinatari preimpostati un sms contenente le informazioni necessarie per identificare l'apparato che ha smesso di essere raggiungibile.

Nel caso di problemi meno seri, come un roundtrip time troppo elevato tra Zabbix e un apparato, il problema viene memorizzato e viene inviata una singola mail di segnalazione ai destinatari preimpostati. Il sistema provvede ad avvertire i destinatari che avevano ricevuto l'alert non appena riconosce l'avvenuta risoluzione del problema.

10.4 SLA

Un altro utilizzo che abbiamo fatto della piattaforma Zabbix è stato quello di conservare le statistiche relative al livello di servizio offerto dalla rete. Per ogni apparato posto sotto monitoraggio, infatti, è disponibile una rappresentazione statistica ad istogramma che evidenzia la disponibilità, espressa in percentuale sul tempo totale, di un singolo apparato. Tali numeri sono indispensabili per comprendere a fondo quanto sta funzionando una rete. Le maggiori aziende che offrono servizi ICT usano questi dati con molteplici finalità, promozionali ma anche legali, per avere una controprova della qualità dei servizi offerti alla clientela. Analogamente anche il servizio reti si è voluto dotare di uno strumento di valutazione statistica della bontà dei servizi offerti. Un down di un apparato di trasmissione radio comporta delle procedure più o meno onerose per il suo ripristino ed è impossibile annullare qualunque possibilità di fault sulla rete, tuttavia è possibile, tenendo traccia dei tempi di down e di ripristino, capire dove è più conveniente investire in rinnovo del parco hardware.

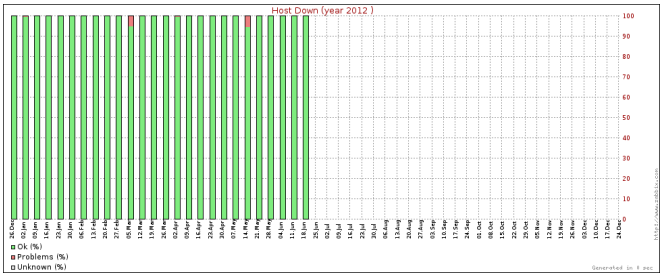


Fig. 13 Availability report.

10.5 Valutazioni

In definitiva Zabbix ha rappresentato, nel caso specifico dell'utilizzo che ne abbiamo fatto, uno strumento prezioso per il monitoraggio attivo e passivo di apparati di rete così come di servizi IT erogati all'interno dell'Area della Ricerca Roma 1 del CNR, offrendo ai sistemisti la possibilità di intervenire tempestivamente in caso di malfunzionamento di apparati o servizi grazie a un efficace sistema di alerting via SMS verso il reparto tecnico. La motivazione principale che ha portato Zabbix ad essere scelto è da imputare alla facilità di configurazione. L'appliance offre un sistema turn key già pronto, senza però impedire customizzazioni anche profonde.

Il sistema sarà di facile utilizzo anche al sistemista che si affaccia per la prima volta ad un sistema di monitoring. Un altro vantaggio è sicuramente la capacità di Zabbix di stockare i dati raccolti su MySQL e di renderli immediatamente consultabili. Considerando che essi sono memorizzati su una base di dati è possibile interfacciare al database un qualsiasi altro applicativo per un'analisi approfondita. A differenza di Cacti Zabbix non utilizza un database RRD. Questo comporta da un lato la necessità di archiviare i dati per evitare che il database cresca senza limiti, un'operazione chiamata house-keeping che può svolgere autonomamente, e dall'altro la persistenza di informazioni non aggregate, che mantengono quindi l'originalità dei dati. Sebbene Zabbix sia inferiore a Na-

gios per quel che concerne il sistema mappa, le sue capacità di alert basati su trigger consentono una gestione granulare e la configurazione di scenari complessi.

11 Considerazioni finali

Scegliere quale tipo di piattaforma monitoring utilizzare come strumento finale è stato oggetto di confronto all'interno del gruppo SRA dell'AdR Roma 1. Sebbene le funzionalità messe a disposizione da Zabbix fossero indubbie, alcune feature tipiche degli altri sistemi risultavano troppo peculiari per poter essere abbandonate.

Considerando che le risorse richieste da Nagios e Cacti sono molto inferiori a quelle richieste da Zabbix (che fa pesante uso di MySql), e che tutti e tre gli ambienti convivono in un ambiente virtualizzato la scelta finale è ricaduta sul mantenere attivi tutti e tre i sistemi. Di Nagios non ci si è voluti privare per via della potente mappa integrata. Considerando che la rete monitorata è di tipo gerarchico la mappa di Nagios svolge un lavoro eccellente nel mostrare dove è il problema e quanto è profondo. Un tale tipo di approccio consente anche a personale non tecnico di poter consultare la mappa e capire subito l'entità del problema.

Cacti da parte sua, avvalendosi di un database RRD garantisce la persistenza di informazioni per quanto concerne il traffico generato dai diversi apparati di rete, senza limite di tempo, al contrario di Zabbix che necessita di operazioni di house-keeping al fine di cancellare i dati più vecchi di una certa soglia. Seppure si perde in Cacti risoluzione nell'andare indietro nel tempo, i dati stockati saranno comunque consistenti, e permetteranno di capire come alcuni parametri si siano evoluti in un arco temporale anche lungo. A tutti gli effetti Cacti offre uno strumento eccellente per verificare lo stato di salute di una rete e l'analisi delle sue performance in un periodo temporale.

Il core del sistema di monitoring è comunque costituito da Zabbix, a lui è delegato il compito della reportistica. Zabbix, da noi provato nella versione 1.8.9, è risultato un prodotto maturo dal punto di vista delle features che offre, anche se pecca ancora per quanto riguarda l'interfaccia utente. La presenza di agent disponibili per una gran quantità di sistemi operativi e la possibilità di creare condizioni anche complesse per quanto riguarda l'invio degli alert fanno di Zabbix uno strumento indispensabile a disposizione degli amministratori di sistema.

Riferimenti

1 Nagios http://www.nagios.org/.

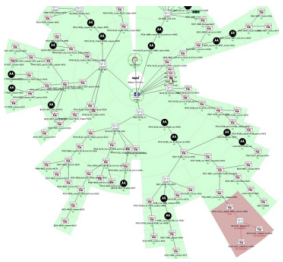
2 Cacti http://www.cacti.net/.

3 Zabbix http://www.zabbix.com/.

Networking

Analisi e Implementazione di Sistemi per il Monitoraggio della Rete Wireless Relativa al Progetto ADD (Anti Digital Divide) e delle Infrastrutture di Campus AdR RM1.†

Augusto Pifferi,[a] Giuseppe Nantista,[a] Luca Ianniello,[a] Andrea Lora,[a] and Marco Simonetti.[a]



In questo documento verranno valutati 3 sistemi di monitoring Open-Source (Nagios, Cacti e Zabbix) e si mostreranno sia le peculiarità che i differenti pro e contro. Verrà esposto il funzionamento di ogni singolo sistema con le relative operazioni di installazione e configurazione, al fine di fornire un quadro completo delle potenzialità dei mezzi. Infine verrà illustrato l'utilizzo dei tre sistemi di monitoraggio nel caso reale della rete di campus dell'Area della Ricerca Roma 1 e della rete wireless realizzata nel territorio della sabina romana e reatina.

Keywords: Monitoring System, Zabbix, Cacti, Nagios.

Documentazione Supplementare

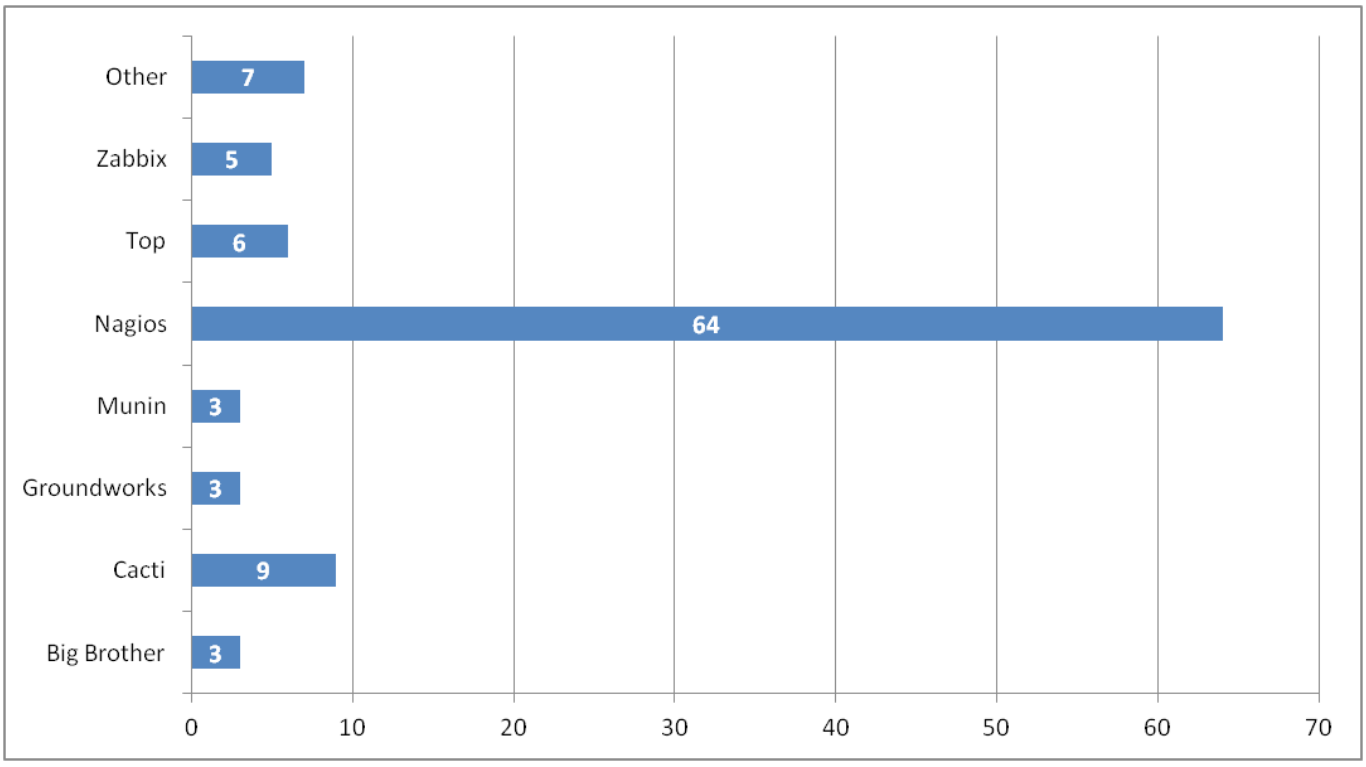


Fig. 1 Diffusioni prodotti OpenSource per il monitoraggio di reti e sistemi ICT.

[a] *CNR - Istituto di Cristallografia, Strada Provinciale 35/d, Montelibretti, Italia*

† Rapporto tecnico IC-RM/1058 protocollato in data 03/07/2012

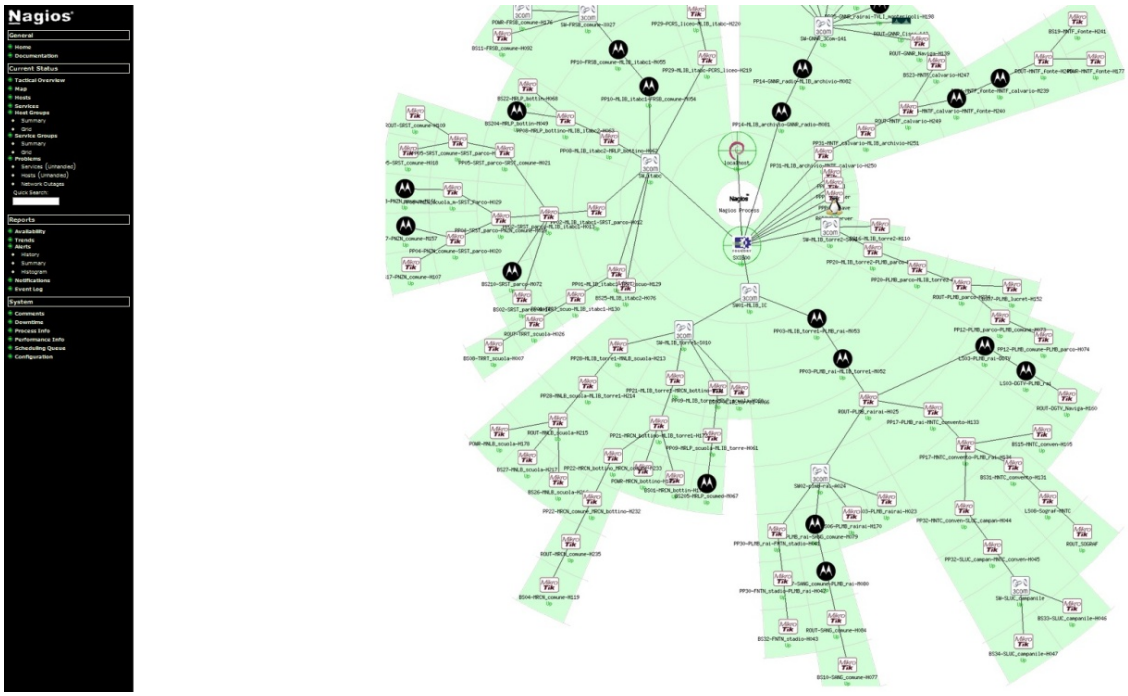


Fig. 2 Mappa di Nagios.

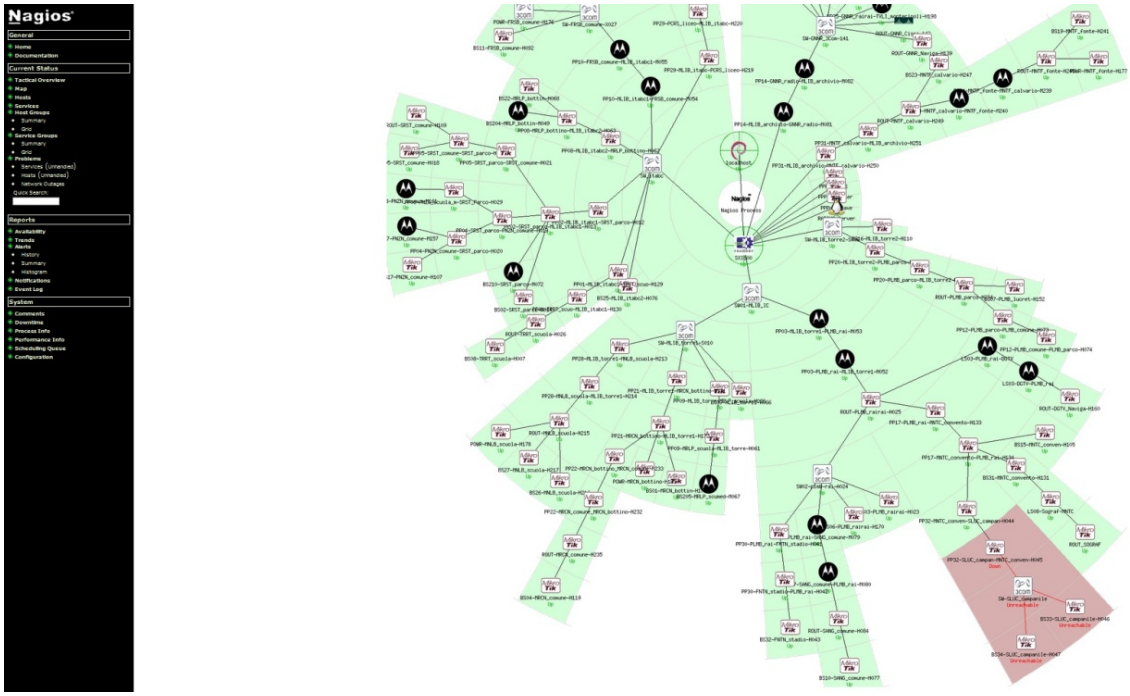


Fig. 3 Mappa di Nagios con evidenziato malfunzionamento host.

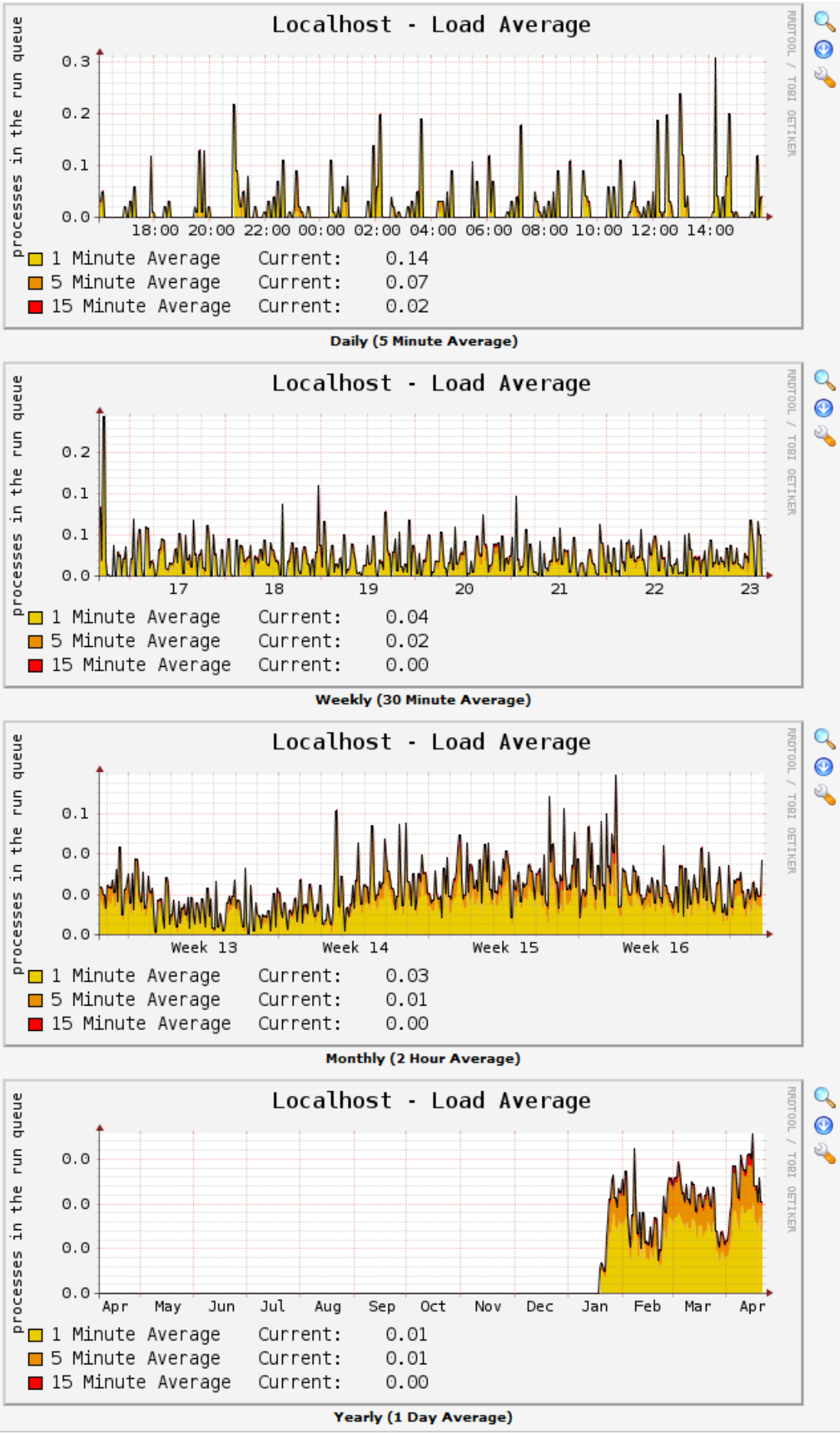


Fig. 4 Grafici e gestione database

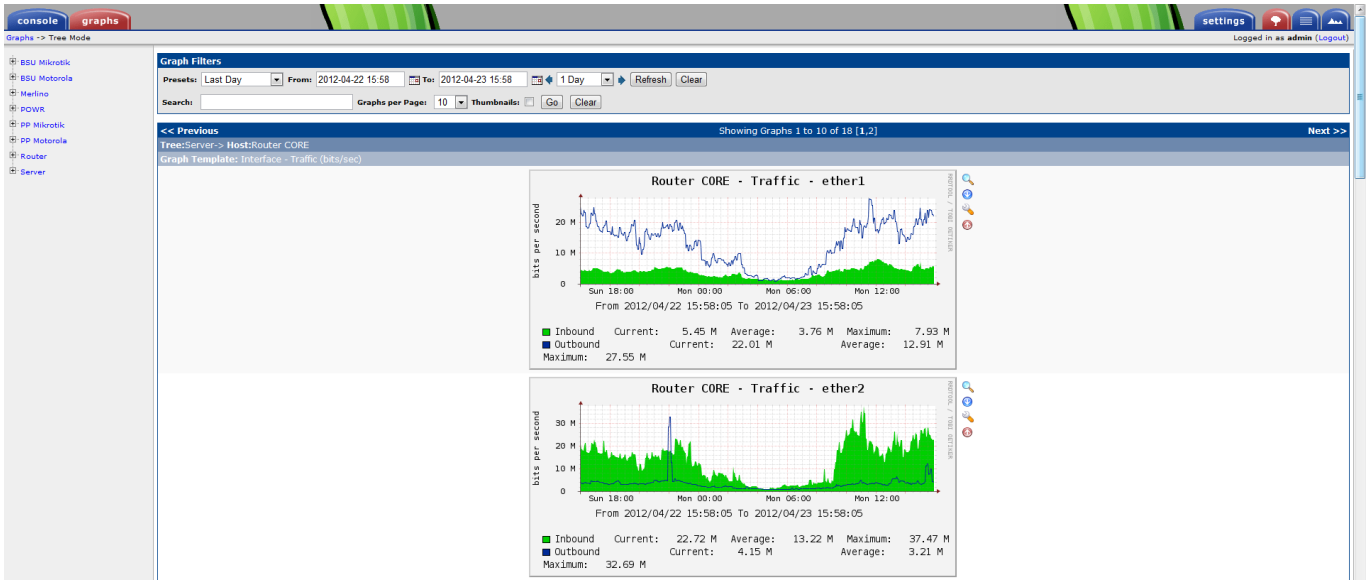


Fig. 5 Traffico in/out sulle interfacce di un router.

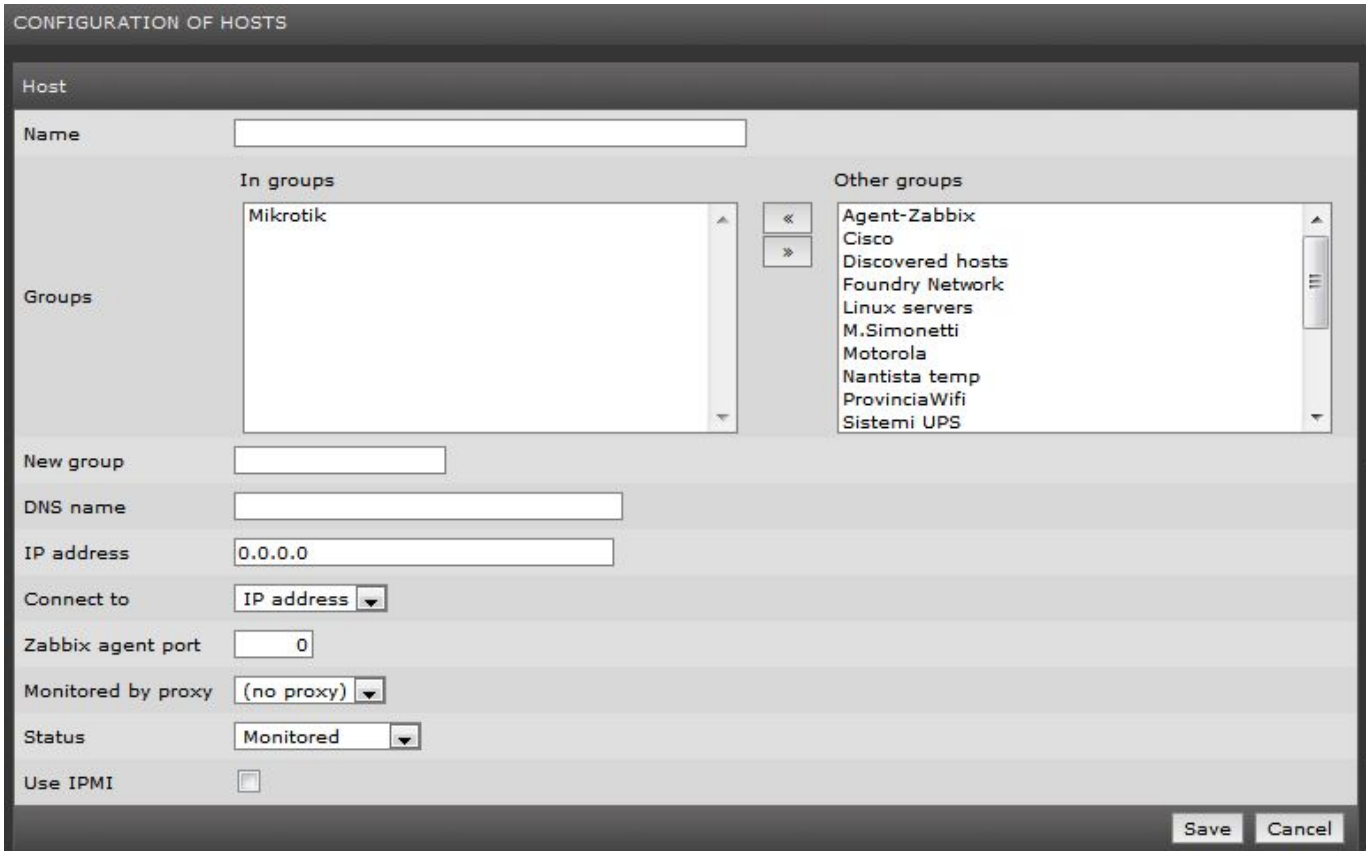


Fig. 7 Configurazione di un host.

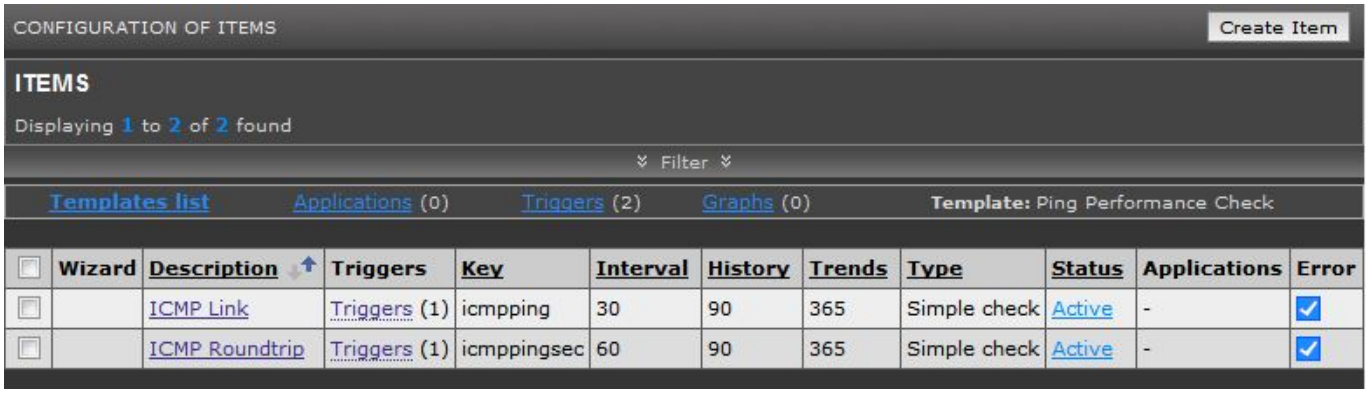


Fig. 8 Lista degli items attivi.

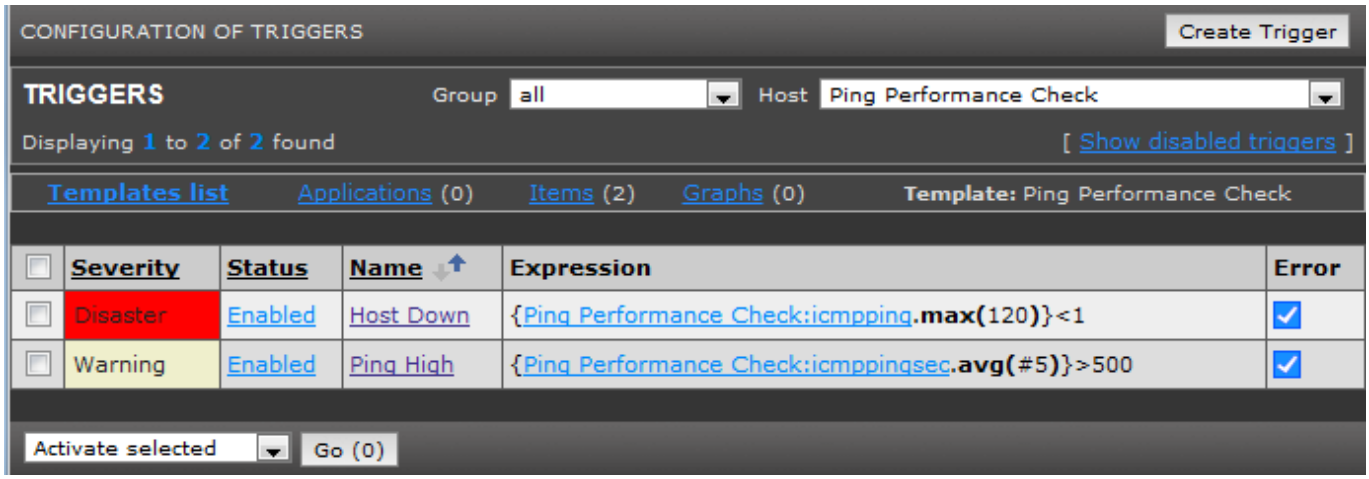


Fig. 9 Lista triggers attivi sul sistema.

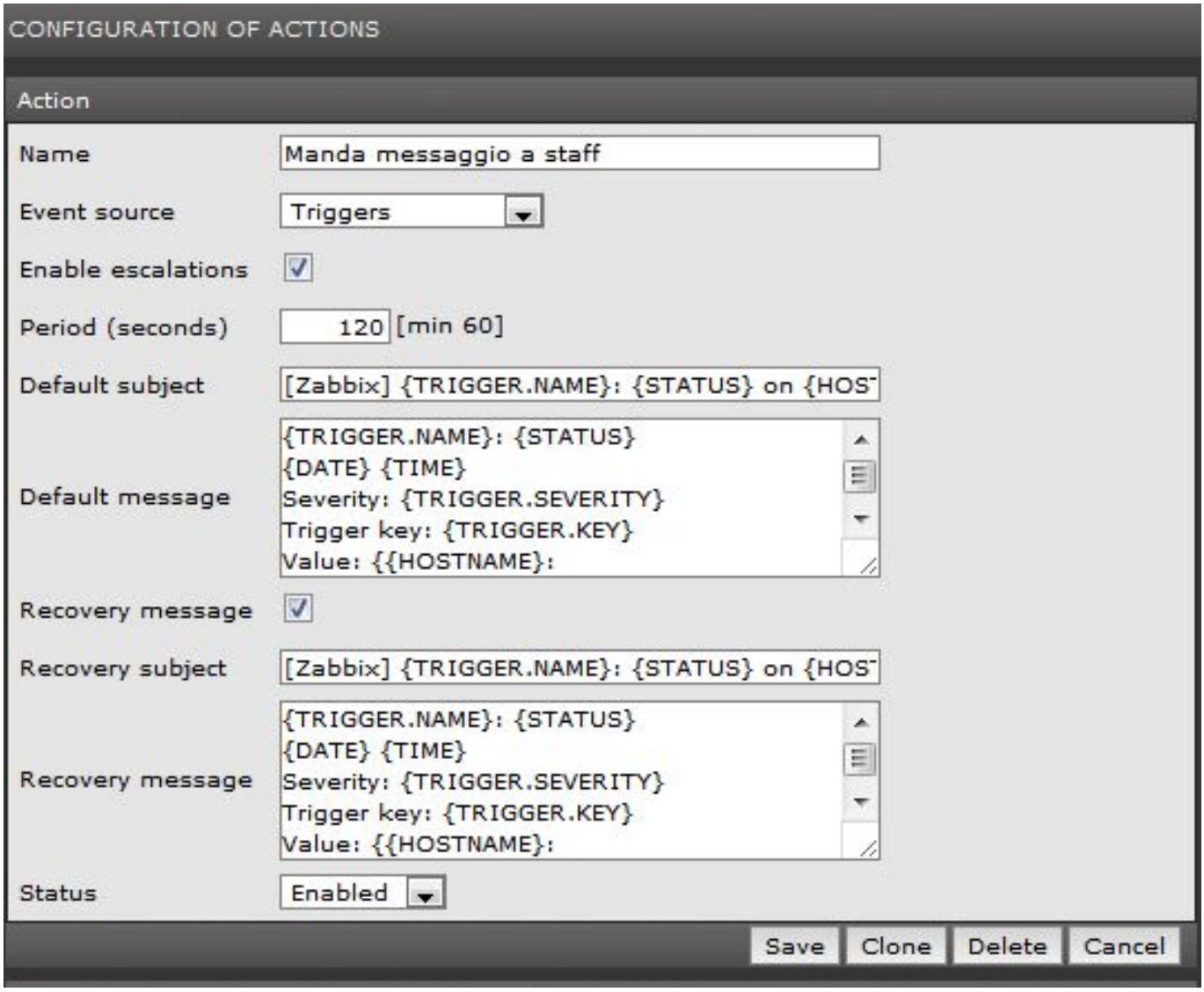


Fig. 10 Creazione di una action.

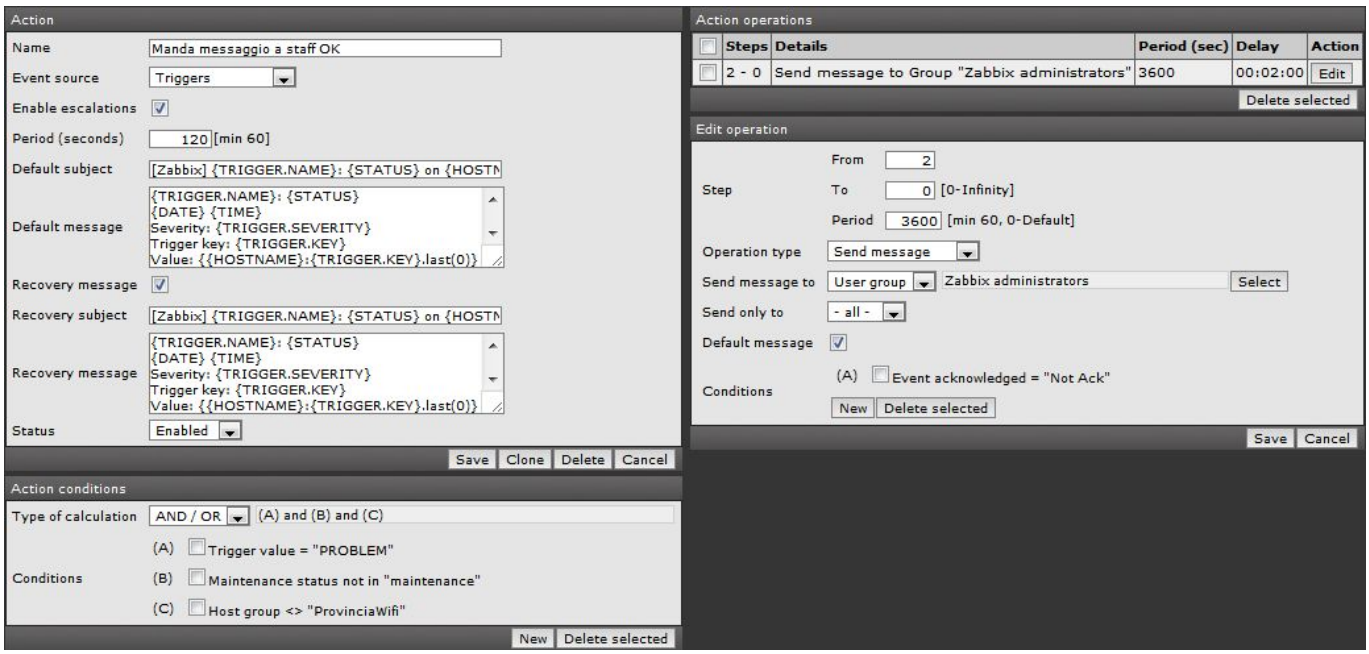


Fig. 11 Una action che prevede escalation.

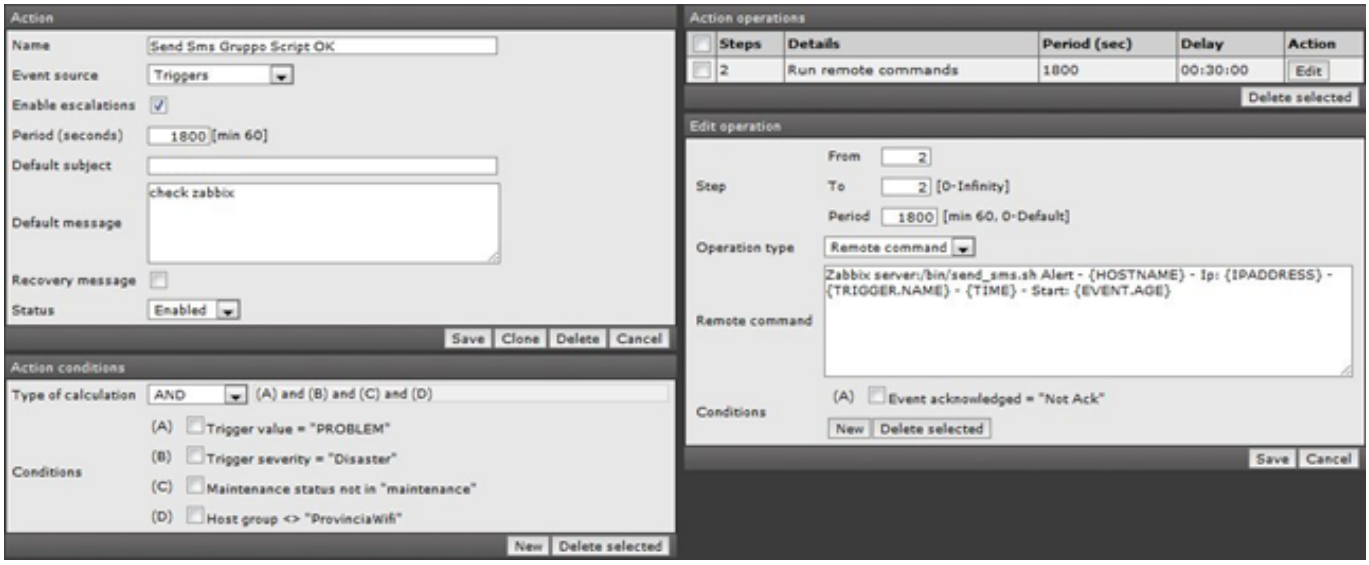


Fig. 12 Esecuzione di un comando remoto tramite Zabbix.

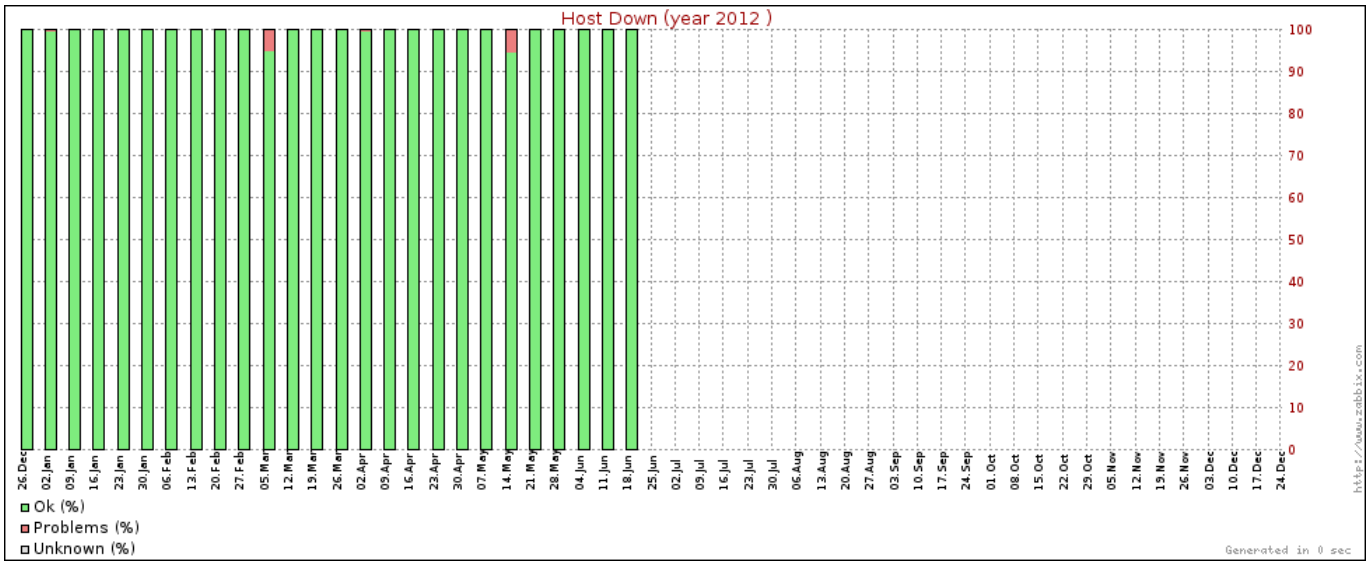


Fig. 13 Availability report.

Networking

La Stazione di Trasmissione Wireless nel Comune di Montopoli di Sabina.†

Augusto Pifferi,[a] Gianni Agostini,[a] Massimiliano Catricalà,[a] Angelo De Simone,[a] Luca Ianniello,[a] Giuseppe Nantista,[a] Claudio Ricci,[a] Luigi Rossi,[a] Marco Simonetti.[a]

La commessa CNR PM.P07.014.005 del Dipartimento di Progettazione Molecolare è espressamente dedicata allo sviluppo e all'implementazione di tecnologie volte al superamento del "Digital Divide". Il sistema più semplice, economico e rapido per portare banda Internet in un territorio vasto, non densamente abitato è quello di installare una rete wireless in frequenza libera 5,4GHz. Nell'accordo con il comune di Montopoli di Sabina è stata individuata la Torre medievale, sul punto più elevato del centro abitato e che domina il paese e il territorio intorno, quale luogo ove montare le antenne di trasmissione per la diffusione del segnale wireless. In questo rapporto viene descritta la nostra installazione.
Keywords: Anti Digital Divide, Stazione di Trasmissione Wireless.

1 Introduzione

Il progetto "Anti Digital Divide", sviluppato nell'ambito del modulo di commessa CNR PM.P07.014.005 del Dipartimento di Progettazione Molecolare, prevede l'espansione nel territorio della copertura con segnale wireless per poter raggiungere in maniera capillare tutte le zone ove vi sia carenza di una rete di telecomunicazioni digitale basata su supporti fisici quali cavi in rame e/o fibre ottiche. È di conseguenza fondamentale individuare le aree ed i Comuni ove installare ripetitori radio per i collegamenti digitali.

Attraverso contatti con gli amministratori degli Enti Locali del territorio della Sabina Reatina nel settembre 2010 il comune di Montopoli di Sabina ha espresso il suo interesse a entrare nella rete del CNR e rendere disponibili i siti necessari alla infrastruttura. Il 17 settembre 2010 il DPM e il Comune di Montopoli hanno siglato una Convenzione Operativa e il 24 febbraio 2011 è stato firmato il Contratto di Servizio con l'Istituto di Cristallografia per l'avvio delle attività.

In questo accordo è stato introdotto un elemento di novità, ovvero sperimentare su Montopoli un modello di "Comune Digitale", il primo nella Sabina, sul quale avviare servizi avanzati per l'Ente Locale e per il cittadino. Questo modello potrà essere poi replicato in un progetto più grande che potrebbe coinvolgere moltissimi comuni dell'area a sud della Provincia di Rieti.

2 Il progetto Montopoli

Montopoli di Sabina, comune di circa 4.200 abitanti in Provincia di Rieti, è situato a breve distanza dai Monti Sabini, dal confine con la Provincia di Roma e da quello con la Provincia di Viterbo. La posizione "strategica" del borgo principale, su un'altura a circa 330 metri slm, con visibilità diretta a 360° sul territorio circostante per decine di chilometri lo rende ideale per l'installazione di apparati Wireless per collegamenti hyperlan sulla frequenza di 5,4GHz.

Foto 1. Torre Ugonesca di Montopoli di Sabina prima dell'installazione dell'impianto.

Uno dei punti più alti del borgo è rappresentato dalla "Torre Ugonesca" (Foto 1), risalente all'anno mille, di

[a] *CNR - Istituto di Cristallografia, Strada Provinciale 35/d, Montelibretti, Italia*

† Rapporto tecnico IC-RM 11/06 protocollato in data 05/08/2011 n. IC/1500

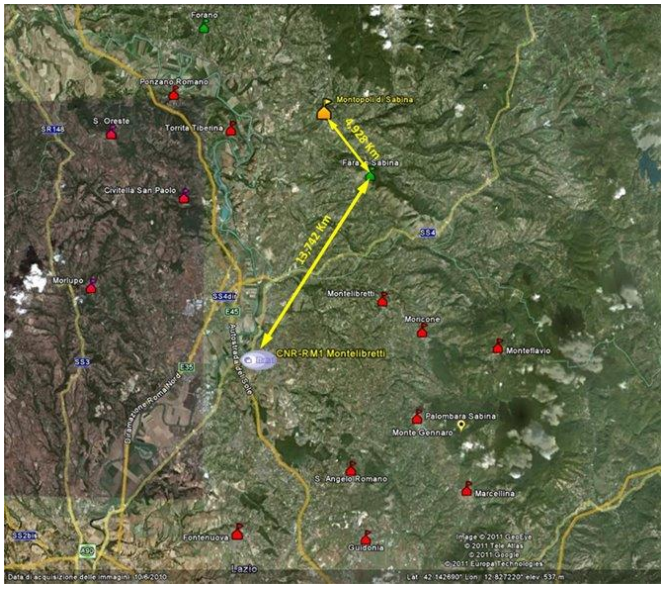


Fig. 1 Dorsale di collegamento tra l'Area della Ricerca RM 1 e Montopoli di Sabina.

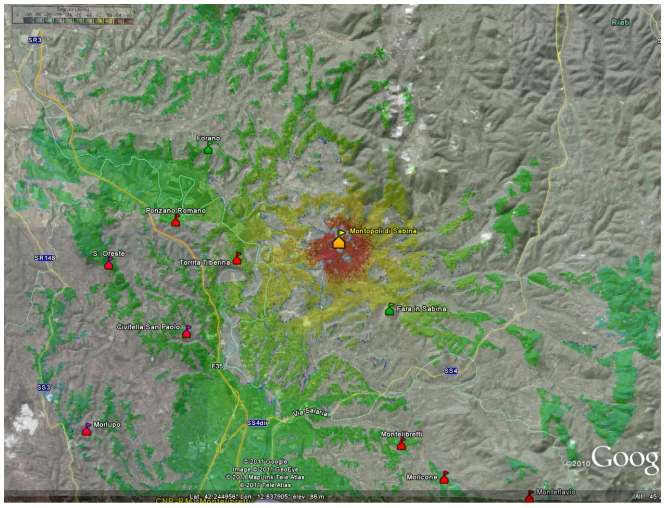


Fig. 3 Simulazione della Copertura radio dalla torre di Montopoli (Radio Mobile).

proprietà comunale. Si tratta di una massiccia struttura in pietra il cui ampio terrazzo è stato utilizzato per l'installazione della stazione radio previo accordo con il Comune.

Il collegamento dorsale per il trasporto della Banda Dati è stato realizzato mediante una coppia di apparati tra la torre di Montopoli e la sede del Comune di Fara in Sabina, distanti tra loro 4,928Km, che a sua volta è collegato all'Area della Ricerca RM 1 con un link da 100Mbps Motorola PTP 500 (Fig. 1). La copertura del territorio è stata invece assicurata con una Base Station (BSU) a 3 settori da 120° ciascuno.

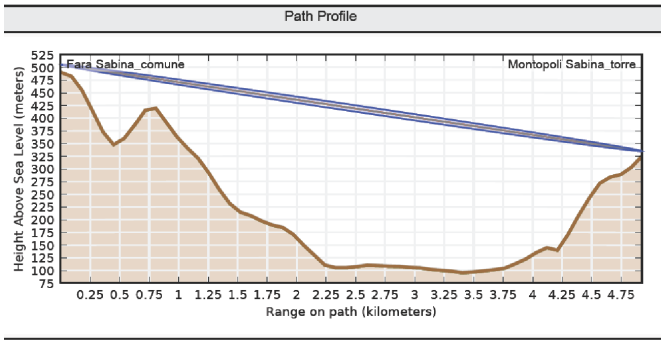


Fig. 2 Profilo del link con software PTP Link Planner.

Prima della realizzazione dell'infrastruttura sono stati eseguiti studi preliminari, con simulazioni di profili (Fig. 2) e relative caratteristiche radio, per i link mediante il software della Motorola PTP Link Planner, mentre per la copertura del territorio dalla BSU sulla torre (Fig. 3) è stato utilizzato il programma Radio Mobile (copyright of Roger Coudé).

MOTOROLA

Summary	
Link Name	Fara Sabina_comune to Montopoli Sabina_torre
Customer Company Name	CNR-IC
Link Type	Line-of-Sight
Equipment Type	PTP54500
Maximum Obstruction	0 meters
Link Distance	4.928 kilometers
Free Space Path Loss	121.26 dB
Excess Path Loss	0.00 dB
User IP Throughput Expectation Aggregate	Aggregate 102.40 Mbps assuming PTP-500 Series running the 500-04-00 software
RF Frequency Band	5.4 GHz (5470 to 5725 MHz)

Tabella 1. Dati generali del link Fara in Sabina (comune) - Montopoli di Sabina (torre).

Installation Notes for Fara Sabina_comune	
Coordinates	42.20998N 012.72927E
Antenna Height	15.0 meters AGL
Antenna Type	Motorola Integrated Dual Polar Antenna
Bearing to Montopoli Sabina_torre	322.39° from True North
Antenna Tilt angle	-2.0°
Link Name	Fara Sabina_comune to Montopoli Sabina_torre
Link Location	Fara Sabina_comune
Telecomms Interface	None
Dual Payload	Enabled
Master Slave Mode	Master
Link Mode Optimisation	IP Traffic
TDD Synchronisation Mode	Disabled
Max Transmit Power	25 dBm while aligning 27 dBm in normal operation
Platform Variant	Integrated Antenna
Channel Bandwidth	15 MHz
Link Symmetry	Symmetric
Predicted Receive Power	-50 dBm ± 5 dB
Predicted Link Loss	121.30 dB ± 5.00 dB

Tabella 2. Caratteristiche del link.

Installation Notes for Montopoli Sabina_torre	
Coordinates	42.24511N 012.69283E
Antenna Height	10.0 meters AGL
Antenna Type	Motorola Integrated Dual Polar Antenna
Bearing to Fara Sabina_comune	142.36° from True North
Antenna Tilt angle	2.0°
Link Name	Fara Sabina_comune to Montopoli Sabina_torre
Link Location	Montopoli Sabina_torre
Telecomms Interface	None
Dual Payload	Enabled
Master Slave Mode	Slave
Link Mode Optimisation	IP Traffic
TDD Synchronisation Mode	Disabled
Max Transmit Power	25 dBm while aligning 27 dBm in normal operation
Platform Variant	Integrated Antenna
Channel Bandwidth	15 MHz
Predicted Receive Power	-50 dBm ± 5 dB
Predicted Link Loss	121.30 dB ± 5.00 dB

Tabella 3. Caratteristiche del link.

3 Dettaglio dell'Impianto

All'interno della Torre nel sottotetto è stato collocato un armadio in vetroresina (Foto 2) entro il quale sono stati alloggiati tutti i dispositivi elettronici necessari ai trasmettitori radio, il router per l'instradamento del traffico dati verso l'Area della Ricerca e le batterie per l'alimentazione.

3.1 Il sistema di alimentazione

Tutti gli apparati sono alimentati 18-24 Vcc tramite specifici alimentatori PoE (Power over Ethernet) con ingresso a 220Vac. Al fine di filtrare i notevoli disturbi provenienti dalla Rete Elettrica, che in zona è particolarmente instabile soprattutto durante condizioni atmosferiche avverse, e dai fulmini stessi che generano forti cariche elettrostatiche, si è preferito adottare per l'alimentazione elettrica una soluzione che avesse caratteristiche di filtraggio e immunità ai disturbi elevate e, in caso di mancanza di energia elettrica, una autonomia sufficiente a tenere accesi gli apparati per il tempo necessario al rientro della alimentazione di rete o per gli interventi di ripristino dei guasti o distacco degli interruttori.

Il sistema consiste di due batterie a secco sigillate da 36Ah poste in serie e ricaricate da un caricabatteria alimentato a 220Vac. In uscita vi è un regolatore di tensione del tipo usato per i pannelli fotovoltaici che è in grado di interrompere l'erogazione di corrente elettrica nel caso in cui le batterie scendessero sotto una predeterminata soglia di tensione per non deteriorare le batterie stesse durante prolungate mancanze di energia elettrica del gestore. Il sistema genera l'alimentazione PoE per tutti gli apparati invece di avere un singolo alimentatore per ciascuna apparecchiatura. Questa soluzione, economica ma efficace, consente un notevole risparmio rispetto ai costosi UPS a doppia conversione che sarebbero necessari per filtrare efficacemente i disturbi in ingresso.

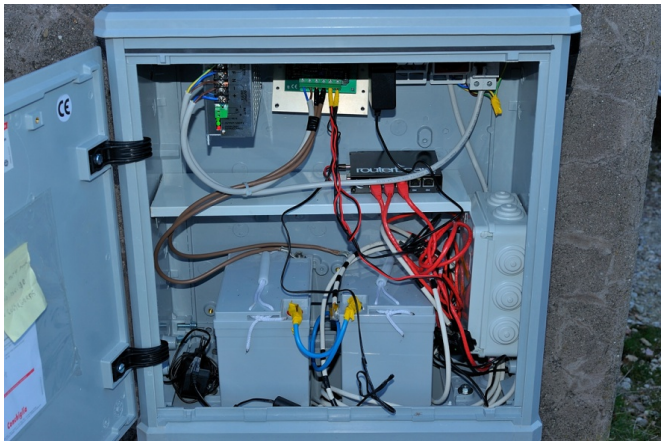


Foto 2. Armadio per la custodia degli apparati e del gruppo di alimentazione.

3.2 Gli apparati radio

3.2.1 Link punto-punto Fara Sabina – Montopoli di Sabina

Per il link punto-punto sono stati montati una coppia di Canopy Backhaul BH20 con lente ceramica che restringe l'angolo di emissione da 60° a 18° con che aumenta di 9dB il guadagno d'antenna per una maggiore immunità ai disturbi e prestazioni più elevate.

Test sulle performance della tratta hanno dato i seguenti risultati:

Current Results Status for LUID: 2 Test Duration: 2 Pkt Length: 1522	
Downlink Rate:	6938112 bps (6.94 Mbps)
Uplink Rate:	6856704 bps (6.86 Mbps)
Aggregate Rate:	13794816 bps (13.79 Mbps, 1120 pps)
Pkt Xmt (Act/Exp):	1116/0 (558 pps)
Pkt Rcv (Act/Exp):	1125/0 (562 pps)
Downlink Efficiency:	100 Percent
Downlink Index (Act/Max):	100/100
Frag Count:	27102/27102
Uplink Efficiency (Act/Exp):	98 Percent
Uplink Index (Act/Max):	98/100
Frag Count (Act/Exp):	27098/26784

3.2.2 Base Station Unit (BSU)

La BSU è un router Mikrotik RB433AH equipaggiato con 3 moduli radio Wireless Mikrotik R5H per 3 antenne da 120° di apertura puntate in direzione di Fara Sabina, Poggio Mirteto e Magliano Sabina.

3.2.3 Router

Il punto-punto e la BSU sono collegati ad router RB450G sempre della Mikrotik.

Il sistema è già predisposto per accogliere la partenza di altri link punto-punto in direzione di eventuali altri comuni che volessero entrare nel progetto Anti Digital Divide.

Foto 3a,b,c. Fasi dell'installazione delle antenne sul terrazzo della Torre.

Foto 4. Impianto ultimato. Vista da terra.

4 Documentazione Fotografica e Simulazioni

La documentazione fotografica delle varie fasi di impianto (comprendendo tutte le foto della presente relazione) è stata eseguita con Fotocamera Reflex Digitale Nikon D300 munita di lente Nikkor 18-200 VR-II.

Le immagini sono state elaborate con applicativi Macromedia Fireworks 2004 e Adobe Photoshop CS 5. Quest'ultimo applicativo ha permesso la funzione di "photostitching" per la creazione di immagini panoramiche unendo più scatti.

Foto 5. Ricostruzione fotografica a 360° della visuale dalla Torre Ugonesca di Montopoli.

La foto panoramica permette di valutare con grande facilità la possibile copertura di trasmissione effettiva di

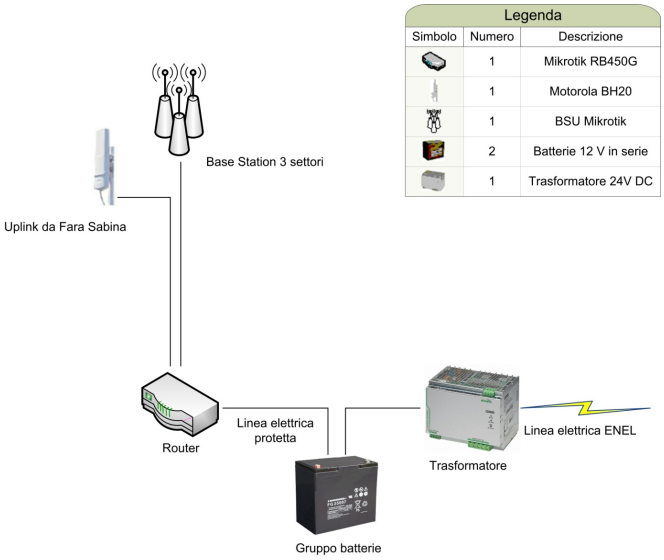


Fig. 4 Diagramma logico funzionale dell'impianto di Montopoli di Sabina.

un antenna come se si fosse dal "punto di vista" di essa. Nella foto 5 si può notare come dalla Torre Ugonesca di Montopoli sia possibile indirizzare il segnale a una zona relativamente vasta, che comprende diversi agglomerati urbani (non facilmente individuabili in questa versione ridotta dell'immagine).

Le immagini, sottoposte a capillare post-processing, possono essere utilizzate anche per Slides in Microsoft Power Point, sia ad uso di documentazione interna del lavoro svolto sia ad uso di divulgazione esterna (conferenze, seminari, eventi eccetera).

5 Conclusioni

Documentazione Fotografica e Simulazioni. L'istallazione di un impianto avanzato di telecomunicazione comporta sia un lavoro di studio e simulazione che un lavoro di documentazione, oltre alle fasi più "ovvie" di assemblaggio della struttura e posizionamento della medesima sulla location scelta. L'installazione di una struttura già pre-assemblata in base alle esigenze permette un notevole risparmio di tempo e di risorse, e la documentazione e la simulazione aiutano in tutte le fasi della lavorazione. In tempi relativamente brevi è possibile sottrarre significative porzioni di territorio al problema del "Digital Divide".

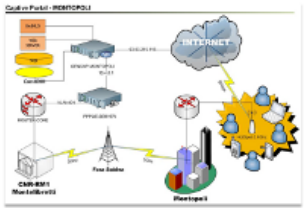
Il numero crescente di questo tipo di installazioni nell'ambito del Progetto rende necessario anche un capillare lavoro di documentazione, sia ad uso interno (schede tecniche, database di attrezzature, archivio fotografico, simulazioni sperimentali ecc...) sia ad uso esterno divulgativo (Brochures, Presentazioni in Microsoft Power Point, preparazione di Flyers o Depliant da mostrare in incontri o seminari ecc.). Il supporto fotografico è indispensabile per simulare l'angolo possibile di copertura di un'antenna, in particolare utilizzando tecniche di-

gitali di “fotostitching” che permettono di creare un’immagine panoramica comunemente non ottenibile con un singolo scatto (anche in caso di una lente marcatamente grandangolare). Le comuni tecniche di fotomontaggio-fotoritocco permettono anche di valutare l’impatto ambientale di un impianto prima ancora che esso venga assemblato e installato: lo si simula sovrapponendone l’immagine a quella della location che deve ospitarlo, e valutando visivamente l’effetto finale (questa tecnica è di fondamentale importanza ad esempio nella stesura di progetti e “DIA”).

Networking

Un Captive Portal per l'utenticazione su Reti Wifi Dedicate agli Internet Access Point Liberi.†

Augusto Pifferi,*[a] Luca Ianniello,[a] Claudio Ricci,[a] Luigi Rossi,[a] and Marco Simonetti[a]



In questo documento verrà descritta l'attività di realizzazione di un sistema Captive Portal per l'accesso a internet sviluppato dal Servizio Reti dell'Area della Ricerca RM1. Il progetto aveva per obiettivo quello di consentire ai comuni dell'area sabina di offrire ai propri cittadini e visitatori un accesso a internet gratuito e sicuro. Descriveremo le specifiche di progetto, l'architettura, il software e i risultati ottenuti in termini di accessi registrati in un arco di tempo.

Keywords: Captive Portal, Hotspot.

1 Introduzione

I piccoli comuni dell'area Sabina hanno scarse opportunità di collegamenti internet veloci e fruibili da tutti. Il Comune di Montopoli di Sabina si è posto il problema di permettere ai propri cittadini e a coloro che visitano il paese, sia a scopo turistico che a scopo lavorativo, di fornire uno strumento di collegamento ad internet libero sull'esempio di altri Enti Locali in altre aree del territorio Nazionale. In virtù della Convenzione Operativa firmata tra il Comune di Montopoli ed il Dipartimento di Progettazione Molecolare del CNR, l'Amministrazione comunale ha chiesto all'Istituto di Cristallografia di allestire una piattaforma **CAPTIVE PORTAL** per l'autenticazione e registrazione di utenti per il libero accesso alla navigazione internet ed installare un primo wireless Hotspot nella piazza comunale.

Il portale, deve essere in grado di consentire la navigazione internet con procedure semplici di registrazione dell'utente e presentare nella sua pagina iniziale il riferimento al comune quale promotore dell'iniziativa.

2 Il Progetto

La tecnica di Captive Portal forza un client http connesso ad una rete di telecomunicazioni a visitare una speciale pagina web (usualmente per l'autenticazione) prima di poter accedere alla navigazione. Ciò si ottiene intercettando tutti i pacchetti, relativi a indirizzi e porte, fin dal momento in cui l'utente apre il proprio browser e tenta l'accesso a Internet. In quel momento il browser viene rediretto verso una pagina web la quale può richiedere l'autenticazione oppure semplicemente l'accettazione delle condizioni d'uso del servizio o una pagina pubblicitaria.

Il termine Hotspot comunemente si riferisce ad un'intera area dove è possibile accedere ad Internet in modalità senza fili (wireless), attraverso l'uso di un Router collegato a un provider di servizi Internet.

Nell'accezione generica del termine è possibile trovare ormai Hotspot per accedere ad Internet in ristoranti, stazioni ferroviarie, aeroporti, librerie, alberghi, centri commerciali ed in moltissimi altri luoghi aperti al pubblico. Anche diverse amministrazioni locali hanno avviato un piano di accesso pubblico spesso gratuito.

Tuttavia, in Italia si possono individuare ancora pochi punti di accesso realmente gratuiti per accedere alla Rete in questa modalità. Dal punto di vista economico, le tipologie di accesso sono molteplici ma la maggior parte degli esercizi pubblici mette a disposizione il proprio Hotspot dietro pagamento di tariffe a gettone, che dipendono dal tempo di collegamento del client piuttosto che dall'effettivo uso delle risorse di rete.

Per questo motivo, unitamente ad una legislazione particolarmente restrittiva ancora oggi non del tutto superata, in Italia questo tipo di servizio si è diffuso tutto sommato in misura ridotta e solo di recente, rispetto alle medie europee.

3 Specifiche del progetto

Le specifiche richieste per il Captive Portal sono:

- Uso di un software Open Source su piattaforma Linux;
- Pagina di registrazione utenti per l'ottenimento delle credenziali d'accesso;

[a] *CNR - Istituto di Cristallografia, Strada Provinciale 35/d, Montelibretti, Italia*

† Rapporto tecnico IC-RM 2013/11 protocollato in data 19/09/2011 n. IC/1616

- Impedire la navigazione ai client non autenticati;
- Limitazione del traffico dati nella misura di banda utilizzabile, dati trasmessi e tempo di collegamento;
- Impedire l'accesso tramite account già connessi;
- Sistemi di sicurezza per la salvaguardia del sistema operativo e dei dati;
- Log degli accessi;
- Recupero della password persa.

La scelta della piattaforma per il Captive Portal è caduta sul software Open Source "CoovaChilli" le cui caratteristiche principali sono mostrate nella figura qui di seguito:

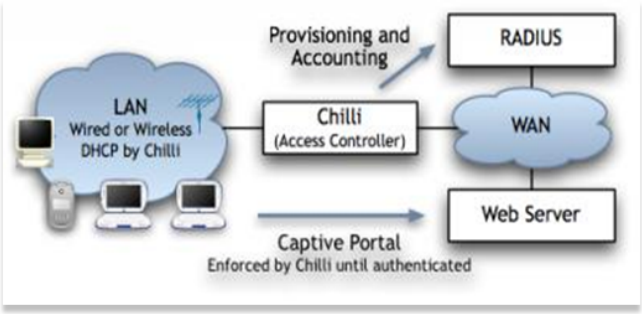


Fig. 1 Schema a blocchi di CoovChili.

CoovaChilli è un Access Control Software che permette la cattura e il reindirizzamento dei pacchetti generati dell'utente che si collega all'HotSpot mostrando una pagina di autenticazione (login) come unica risorsa web consultabile e quindi passaggio obbligatorio per accedere alla navigazione

4 Realizzazione del CAPTIVE

Il Server sul quale è stato installato il Captive Portal ha le seguenti caratteristiche:

Produttore modello	IBM eserver xSeries 345
Processore	Intel(R) Xeon(TM) CPU 3.80GHz L1 cache 8KiB L2 cache 2048KiB Intel(R) Xeon(TM) CPU 3.80GHz L1 cache 8KiB L2 cache 2048KiB
Memoria RAM	Memory 2 GB
Dischi Fissi	SCSI storage PCI-X Fusion-MPT Dual Ultra320 SCSI 36 GB Raid-1 SCSI storage PCI-X Fusion-MPT Dual Ultra320 SCSI 36 GB Raid-1
Scheda video	VGA ATI Technologies Inc. Rage XL

CoovaChilli, il software per il controllo degli accessi, funge da client di un Server RADIUS (**Remote Authentication Dial-In User Service**) che è attualmente lo standard de-facto per l'autenticazione remota tramite un gruppo di protocolli "**AAA**" **Authentication, Authorization e Accounting**, necessari rispettivamente per

Fig. 2 Pagina di reindirizzamento di Coovachili

le funzioni di autenticazione, controllo degli accessi e tracciamento del consumo delle risorse da parte degli utenti.

Uno dei requisiti per il funzionamento dell'applicativo è la presenza del web-server **Haserl** (un programma di 20Kb molto utilizzato nelle apparecchiature embedded) che oltre ad avere come caratteristica principale quella di fungere da demone-web ha anche quella di interpretare bash-scripting (Unix-command-line) per la generazione di pagine dinamiche come un vero e proprio CGI. il Sistema Operativo utilizzato è **GENTOO LINUX** sul quale è stata installata e configurata l'intera piattaforma. Gentoo Linux è una speciale distribuzione di Linux che può essere facilmente ottimizzata e personalizzata per qualsiasi applicazione o necessità. L'estrema velocità, la grande configurabilità e l'ottima collaborazione fra gli sviluppatori e gli utenti sono i grandi punti di forza di Gentoo. Il Server RADIUS utilizzato in questa piattaforma è anch'esso di origine Open Source ed è **FreeRadius**.

Per la parte dei dati relativi alle credenziali d'accesso e gli attributi richiesti per il funzionamento del protocollo "**AAA**", **FreeRadius** e' stato configurato per essere interfacciato con il demone **Mysql**.

Attraverso la pagina di login l'Access Controller instaura la comunicazione con il Server RADIUS il quale a sua volta, seguendo le impostazioni configurate, interroga il data-base per l'avvio dei meccanismi di autenticazione remota (verifica della password, assegnazione di un id univoco, assegnazione attributi di controllo etc.).

Per poter accedere alla navigazione è necessario essere in possesso delle credenziali: una userid e una password.

Poiché il software a disposizione per la gestione delle credenziali d'accesso offre solo un backend da operatori, si è reso necessario studiare e sviluppare un software per la registrazione degli utenti.

Per rendere questo software usufruibile dal più ampio numero di utenti e compatibile con il più ampio numero di dispositivi si è optato per l'utilizzo del linguaggio **PHP** e **JavaScript**.

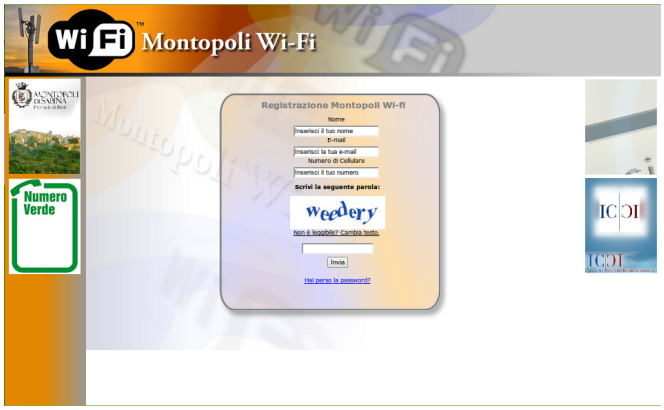


Fig. 3 Pagina di registrazione Captive Montopoli.

L'interfaccia di registrazione (Fig. 3) presenta 4 campi che l'utente che esegue la registrazione è obbligato a riempire:

Il campo Nome, il campo e-mail, il campo numero di cellulare e il campo captcha.

In tutti i campi sono stati impostati dei controlli, a livello software, che obbligano l'utente a compilare i dati richiesti.

Il campo nome non può essere vuoto, deve essere modificato dallo stato di partenza, non deve essere già presente nel DB.

Il campo e-mail non può essere vuoto, deve essere modificato dallo stato di partenza, deve contenere il carattere chiocciola (@) e la parte relativa al dominio deve essere di almeno 5 caratteri compreso punto di separazione.

Il campo numero di cellulare non può essere vuoto e deve contenere solo caratteri numerici e non deve essere già presente nel DB.

In fine il campo **CAPTCHA*** deve essere compilato correttamente per poter superare la verifica. Una volta compilati correttamente tutti i campi richiesti viene spedito un messaggio **SMS** al numero indicato nel form tramite un Gateway GSM; il messaggio contiene la password necessaria all'accesso. Questo meccanismo fa si che l'utente che compila il campo numero di cellulare con dati mendaci non sarà poi abile ad effettuare l'accesso alla navigazione in quanto non provvisto della necessaria password.

E' stato previsto e sviluppato anche il software per il recupero della password per tutti quegli utenti che hanno già effettuato la registrazione ma non sono più in possesso del messaggio SMS originale contenente la

Fig. 4 Frame della registrazione utente

Fig. 5 Frame per il recupero password.

* Con l'acronimo inglese CAPTCHA si denota nell'ambito dell'informatica un test fatto di una o più domande e risposte per determinare se l'utente sia un umano (e non un computer o, più precisamente, un bot). L'acronimo deriva dall'inglese "Completely Automated Public Turing test to tell Computers and Humans Apart" (Test di Turing pubblico e completamente automatico per distinguere computer e umani)

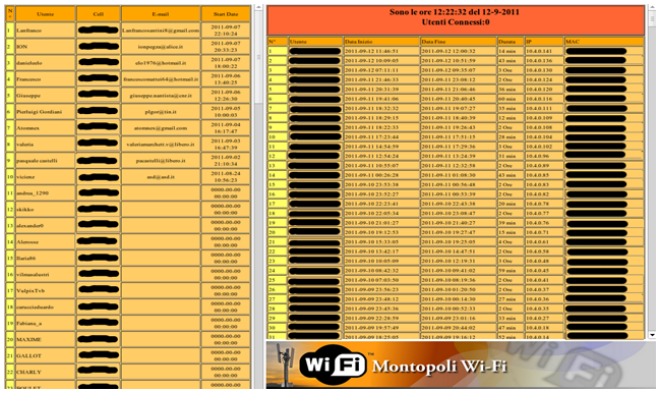


Fig. 6 Registrazione degli accessi al Captive Portal.

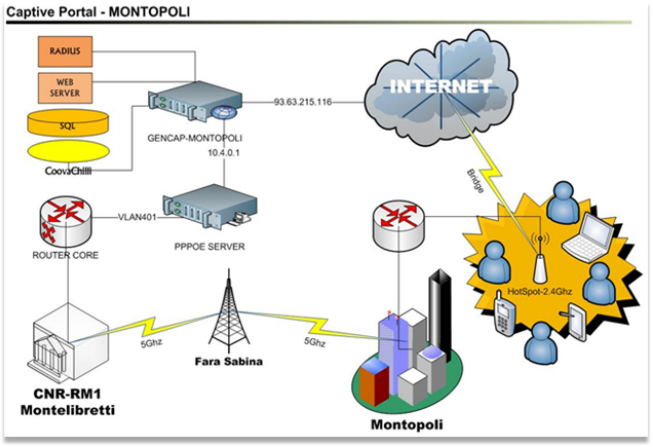


Fig. 7 Layout di funzionamento della “Piazza digitale” realizzata a Montopoli di Sabina

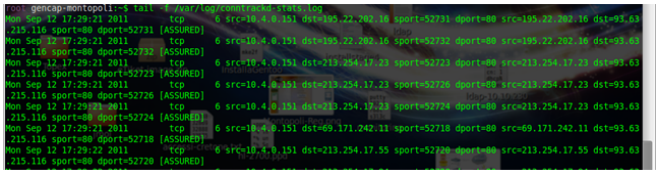


Fig. 8 Schermata del demone Conntrackd che mostra le connessioni stabilite con successo.

password.

Utilizzando l’apposito link, presente sia nella pagina di registrazione ”*Hai perso la password?*” che nella pagina di login “*Password dimenticata? Clikka qui*!” è possibile recuperare la propria password di accesso inserendo il numero di telefono utilizzato durante la registrazione nell’apposito campo del form insieme al codice CAPTCHA corretto, in questo modo si invia una richiesta al server dati (MySQL) che, una volta trovata corrispondenza tra gli utenti registrati, spedisce tramite un messaggio SMS la password al numero di telefono in questione.

Per tenere sotto controllo il flusso di accessi ma soprattutto per capire meglio l’ottica e la portata dell’impatto del progetto stesso è stata sviluppata anche una pagina WEB che riporta in real-time gli accessi e le registrazioni che vengono effettuate tramite il portale (Fig. 6).

Nella colonna a sinistra della pagina sono elencati i dati inseriti al momento della registrazione: nome, numero di cellulare, e-mail e data registrazione.

Nella colonna a destra sono mostrati: l’utente identificato dal numero di telefono, la data e l’ora di inizio e fine collegamento dal momento dell’avvenuto login con successo, la durata effettiva della connessione, il MAC-ADDRESS e l’indirizzo IP associato.

In 5 mesi di funzionamento dell’HotSpot risultano effettuate 97 registrazioni e 1660 accessi.

5 L’Access Point di Montopoli di Sabina (RI)

Nella Piazza Comunale a Montopoli di Sabina è stato installato un Router con una interfaccia LAN Wireless 2.4Ghz che funge da punto di accesso per l’HotSpot.

Lo stesso router ha una interfaccia WAN 5Ghz che viene usata per effettuare la connessione alla rete Wireless verso il CNR passando attraverso la dorsale che si appoggia a Fara Sabina.

La connessione viene garantita, autenticata e autorizzata tramite un link PPPoE verso l’apposito server PPPoE in sede CNR (che è direttamente interfacciato a un server RADIUS per svolgere le idonee operazioni AAA).

Appena in rete il router di Montopoli instaura una comunicazione (questa volta PPTP) con un router di core, anch’esso posizionato nei CED dell’Area della Ricerca RM 1.

L’ultima operazione che viene compiuta da questi sistemi è la realizzazione di un bridge fra la LAN 2.4Ghz di Montopoli e la VLAN in cui risiede il captive portal. In questo modo chi si collega alla rete wireless di Montopoli si trova nello stesso dominio di broadcast del captive portal, ottiene dinamicamente un indirizzo IP e viene intercettato dal sistema che richiede la fase di autorizzazione/autenticazione prima di concedere l’accesso a internet.

La particolare struttura del Portale fa si che tutti gli utenti che ottengono l’accesso alla navigazione vengano identificati su internet attraverso lo stesso indirizzo IP pubblico a causa del mascheramento che viene effettuato da parte del gateway, in questo caso CoovaChilli, per il transito dei pacchetti.

Per garantire comunque la rintracciabilità dell’utilizzatore finale, nel caso di eventuali infrazioni delle normative vigenti, e stato installato e configurato un software, sempre di matrice Open Source, dal nome Conntrackd.

Questo demone si occupa di registrare L’indirizzo IP sorgente e quello di destinazione di tutte le connessioni che avvengono attraverso il Captive Portal.

Per evitare di registrare informazioni non pertinenti ed inutili, il demone è stato configurato in modo da tenere traccia solo dei collegamenti che vanno a buon termine

quindi che arrivano allo stato di **ESTABILISHED** o come riporta il demone stesso **ASSURED**.

Registrando solo e unicamente gli indirizzi IP (sorgente e destinazione) si garantisce agli utilizzatori finali l'anonimato della navigazione e quindi il rispetto della privacy poiché con i dati registrati e' possibile risalire solo ai server contattati e non alle pagine visualizzate.

Per quanto riguarda la navigazione agli utenti e' stato concessa piena liberta di utilizzo limitando, tramite RADIUS, l'accesso simultaneo da parte di più utenti con le stesse credenziali e permettendo un limite massimo di traffico dati al giorno di 500MB.

6 Conclusioni

Rispetto ad altri paesi, in Italia solo ora si stanno attuando politiche di accesso libero ad internet conformando la nostra legislazione, il più delle volte molto restrittiva, a quella più liberale della Comunità Europea e dell'area Americana. Il disagio derivante dalla difficoltà di collegamento ad internet dei giovani, soprattutto nelle realtà dei piccoli comuni e nelle aree rurali, è ancora fortemente sentito. Molti Enti Locali, Province e Regioni si stanno muovendo in questa direzione promuovendo progetti per l'attivazione di quanti più Access Point liberi possibile sul territorio (ad esempio "Provincia WiFi" della Provincia di Roma con la quale l'istituto di Cristallografia collabora ormai da più di due anni). Nella provincia di Rieti questa è la prima collaborazione tra Consiglio Nazionale delle Ricerche ed Enti Locali per la realizzazione di "Piazze digitali" che si è subito rivelato un successo.

Sull'onda di questo risultato si sono rivolti al nostro Istituto WISP (Wireless Internet Service Provider) locali per la realizzazione di impianti simili presso esercizi pubblici privati (Acquapiper di Guidonia e Terme di Cretone) concretizzando una reale collaborazione fra Enti di Ricerca e privati.

Riferimenti

1 A. Pifferi, G. Agostini, M. Catricalà, A. D. Simone, L. Ianniello, G. Nantista, C. Ricci, L. Rossi, M. Simonetti, (PM.P07.014.005) Sviluppo ed applicazioni di reti telematiche anti "Digital Divide": LA STAZIONE DI TRASMISSIONE WIRELESS NEL COMUNE DI MONTOPOLI DI SABINA".Istituto di Cristallografia-Rapporto Tecnico IC-RM 11/07 prot. 1500 del 05/08/2011.

2 http://www.coova.org/.

3 http://www.gentoo.org/.

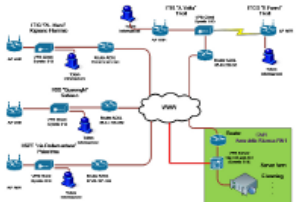
4 http://freeradius.org/.

5 http://conntrack-tools.netfilter.org/.

E-Learning & Scientific Communication

Progetto Regione Lazio: Interventi di Innovazione e Potenziamento del Sistema Regionale d'istruzione – Az.B. Proposta Formativa "Uno per tutti-tutti per uno".†

Augusto Pifferi,[a] Giovanni Agostini,[a] Massimiliano Catricalà,[a] Angelo De Simone,[a] Luca Ianniello,[a] Claudio Ricci,[a] Marco Simonetti,[a] Luigi Rossi,[a] Guido Righini,[b] Giuseppe Nantista.[a]



Il Progetto "Uno per tutti – tutti per uno" prevede l'interconnessione di cinque plessi scolastici mediante una "Virtual Private Network", all'interno della quale, sarà possibile scambiare contenuti didattici attraverso sistemi multimediali moderni. Nel rapporto sarà descritto la piattaforma di e-learning comune ai cinque plessi scolastici che fornirà i corsi realizzati dai docenti delle scuole coinvolte nel progetto.

Keywords: Virtual Private Network, e-Learning.

1 Introduzione

Il progetto nasce da un'attenta analisi delle esigenze degli Istituti Tecnici e degli Istituti d'Arte riguardo la necessità di miglioramento della didattica curricolare, e dell'offerta formativa complementare e dell'orientamento.

Il presente progetto prevede l'interconnessione di 5 plessi scolastici mediante una "Virtual Private Network" (VPN) all'interno della quale sarà possibile scambiare contenuti didattici attraverso moderni sistemi multimediali e la realizzazione di una piattaforma di e-learning comune per la diffusione di corsi creati dal personale docente delle scuole coinvolte.

Le scuole partecipanti al progetto sono:

- ITCG "Enrico Fermi", Tivoli
- ITIS "Alessandro Volta", Tivoli
- IISS "Quarenghi", Subiaco
- IISPT "via Pedemontana", Palestrina
- IIS "Pier Luigi Nervi", Rignano Flaminio

2 Dettaglio di Progetto

2.1 Rete WAN (Wide Area Network)

Per rete WAN si intende la rete geografica attraverso la quale le sedi scolastiche si collegano in Internet. Attualmente ognuna di queste sedi è connessa da gestori di telecomunicazioni con tipologie e caratteristiche differenti. Nella maggior parte dei casi la qualità e la velocità di connessione è buona ma non ottimale per gli scopi previsti soprattutto perché la tecnologia utilizzata è l'**ADSL** (acronimo inglese di **Asymmetric Digital Subscriber Line**), la quale per sua caratteristica di traffico sbilanciato favorisce il flusso di dati principalmente in una direzione detta "download". Nel senso inverso, detto "upload", la velocità di trasferimento dati è notevolmente inferiore. Per questo progetto il collegamento ideale sarebbe quello perfettamente bilanciato **HDSL** (acronimo inglese di **High data rate Digital Subscriber Line**) che consente di raggiungere velocità fino a 8 Mbps sincroni (sia in download che in upload) con una connessione sempre attiva. Infatti le trasmissioni dati con dispositivi multimediali necessitano sia di ricevere che di inviare flussi dati di notevole consistenza. La soluzione ideale è quella di sostituire i collegamenti ADSL con gli HDSL su una rete proprietaria come ad esempio quella Wireless del Consiglio Nazionale delle Ricerche presente nell'area della Sabina e della valle dell'Aniene. Nella fase attuale non è stato possibile collegare le scuole alla rete wireless del CNR, ma nel futuro prossimo, per le scuole di Tivoli e di Rignano questo sarà attuabile. Le restanti scuole, in un secondo tempo, quando il segnale radio potrà raggiungere le città di Subiaco e Palestrina, potranno essere immesse nella stessa rete. Tra le sedi dell'ITCG "E. Fermi" e dell'ITIS "A. Volta" è stato realizzato un link punto-punto ad alta capacità (>10Mbps), che collega le reti WLAN dei due plessi scolastici, vista la loro reciproca visibilità ottica (le reti wireless a 5.4 GHz in banda libera necessi-

[a] *CNR - Istituto di Cristallografia, Strada Provinciale 35/d, Montelibretti, Italia*
[b] *CNR - Istituto di Struttura della Materia, Strada Provinciale 35/d, Montelibretti, Italia*

† Rapporto tecnico IC 11/01 registrato con numero di protocollo IC/1236 del 22/06/2011

tano di collegamenti tra punti in visibilità **LOS – Line Of Sight**).

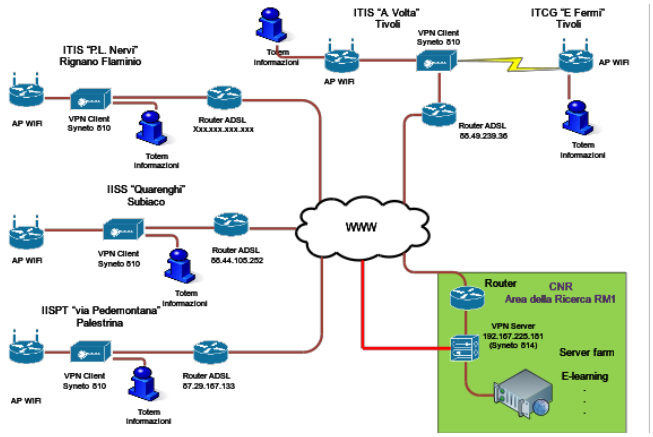


Fig. 1 Schema generale della Rete.

2.2 Reti WLAN d'Istituto (Wireless Local Area Network)

Con reti WLAN qui identifichiamo le reti locali interne a ciascun istituto scolastico realizzate ad hoc per il progetto mediante tecnologia wireless. Alla WLAN vengono collegati tutti i personal computers, le periferiche (Stampanti, Fax, Access Point, Totem informativi, etc.). Nel progetto è previsto che le reti WLAN di ciascun istituto possano collegarsi tra di loro attraverso una VPN (Virtual Private Network). Con questa tecnologia le diverse reti potranno connettersi per formare un unico grande ambiente operativo utilizzando i vecchi collegamenti alle linee ADSL per l'accesso ad internet e sempre attraverso Internet scambiare pacchetti dati attraverso "tunnel" non tracciabili da reti esterne.

Per realizzare questa configurazione è necessario un server VPN collocato in posizione baricentrica rispetto agli "utenti" da servire. In questo caso la posizione ideale è presso le strutture dell'Area della Ricerca Roma 1 del Consiglio Nazionale delle Ricerche che possiede collegamenti in fibra ottica verso la rete Internet con garanzie di continuità, protezione ed affidabilità. Ogni sede scolastica deve essere dotata di un Client VPN. In questo modo il traffico per i servizi multimediali interni delle scuole viene confinato entro questa rete virtuale.

2.3 Piattaforma di e-learning

Il progetto prevede una piattaforma di e-learning sulla quale caricare i corsi elaborati dallo staff docente delle 5 scuole. Anche in questo caso il sito ottimale dove localizzare il Server deve essere baricentrico e ben collegato in internet con linee ad alta capacità ed affidabilità. Il Consiglio Nazionale delle Ricerche mette a disposizione presso i locali CED dell'Area della Ricerca RM 1 un server dedicato per l'e-learning. La piattaforma utilizzata è "MOODLE", un sistema Open Source che può essere configurato ed amministrato anche remotamente dagli addetti ai lavori delle scuole. Nel presente progetto è incluso un corso per amministratori della piattaforma.

3 Esecuzione del Progetto

3.1 la Rete VPN

Le reti VPN utilizzano collegamenti che necessitano di autenticazione per garantire che solo gli utenti autorizzati vi possano accedere; per garantire la sicurezza che i dati inviati in Internet non vengano intercettati o utilizzati da altri non autorizzati, esse utilizzano sistemi di crittografia.

Le reti VPN sicure adottano dunque protocolli che provvedono a cifrare il traffico transitante sulla VPN. Oltre alla cifratura, una VPN sicura deve prevedere nei suoi protocolli dei meccanismi che impediscano violazioni della sicurezza, come ad esempio il furto dell'identità digitale o l'alterazione dei messaggi.

Generalmente una VPN comprende due parti: una interna alla rete, e quindi protetta, che preserva la trasmissione, e una meno affidabile e sicura che è quella esterna alla rete private, ad esempio via Internet.

Nelle VPN c'è in genere un firewall tra il computer del dipendente o di un cliente e il terminale della rete o del server. L'utente, per esempio, quando stabilisce la connessione con il firewall, deve autenticare i dati che vuole trasmettere, passando attraverso un servizio di autenticazione interno.

Un utente autenticato può essere provvisto di privilegi particolari per accedere a risorse che generalmente non sono accessibili a tutti gli utenti. La maggior parte dei programmi client richiede che tutto il traffico IP della VPN passi attraverso un "Tunnel" virtuale tra le reti utilizzando Internet come mezzo di collegamento. Dal punto di vista dell'utente ciò significa che, mentre la connessione VPN è attiva, tutti gli accessi esterni alla rete sicura devono passare per lo stesso firewall come se l'utente fosse fisicamente connesso all'interno della rete sicura. Questo riduce il rischio che utenti esterni possano accedere alla rete privata dell'azienda. Il Tunneling è la trasmissione di dati attraverso una rete pubblica, che fa sì che i nodi di routing della rete pubblica non siano in grado di rilevare che la trasmissione è parte di una rete privata.

Il Tunneling permette dunque di usare la rete pubblica per trasportare dati per conto di clienti autorizzati all'accesso alla rete privata facendo si che la comunicazione end-to-end tra utenti rimanga a livello logico confinata all'interno della rete privata stessa.

In genere il Tunneling viene creato incapsulando i dati e il protocollo nel protocollo di rete pubblica, così che i dati che transitano per il tunnel non siano comprensibili a terzi che stiano eventualmente esaminando i dati trasmessi.

La sicurezza della connessione VPN è di importanza fondamentale, perché la rete su cui gli altri computer stanno lavorando potrebbe non essere sicura, o esserlo solo parzialmente. La VPN deve quindi garantire un livello di sicurezza tale da proteggere i computer che stanno lavorando simultaneamente sulla stessa rete, tra i quali uno potrebbe essere stato infettato da un virus, un worm o un trojan.

3.2 Sede CNR Area della Ricerca RM 1

Presso il CED dell'Area della Ricerca RM 1 è stato installato un "appliance" Syneto 814. L'apparato funge da firewall e da server per la rete VPN. Il protocollo utilizzato per instaurare la comunicazione VPN è l'IPsec. In telecomunicazioni IPsec è l'abbreviazione di **IP Security** ed è uno standard per ottenere connessioni basate su reti IP sicure. La sicurezza viene raggiunta attraverso la cifratura e l'autenticazione dei pacchetti IP. La sicurezza viene fornita quindi a livello di rete cui l'IP appartiene. La capacità di fornire protezione a livello di rete rende questo protocollo trasparente al livello delle applicazioni che non devono essere modificate. Il Router firewall Syneto 814 consente quindi a tutto il traffico della rete costituita dalle Wireless LAN delle 5 scuole di far si che all'interno della rete tutti gli host siano visibili tra di loro e le eventuali comunicazioni verso internet avvengano esclusivamente attraverso questa porta di accesso. All'interno della rete è anche raggiungibile il server di e-lerning di cui si parlerà più avanti. Il firewall è raggiungibile dai client VPN attraverso l'IP pubblico 192.167.225.181.

3.3 ITCG "Enrico Fermi", Tivoli

Presso il plesso scolastico dell'Istituto Fermi non è stato necessario installare un apparato VPN Client in quanto esistendo visibilità ottica con il plesso scolastico dell'Istituto Volta, i due edifici sono stati collegati con un link Wireless point-to-point realizzato mediante due trasmettitori radio per collegamenti in Hyperlan sulla frequenza libera di 5,4 GHz. Pertanto i router wireless della WLAN del Progetto Capitale Umano attivati presso il Fermi sui tre piani dell'edificio sono stati collegati serialmente tra di loro e il primo della catena, quello posto sopra l'ingresso dell'aula informatica "Neuman" al primo piano dell'edificio, all'antenna del link Fermi-Volta. L'antenna è stata configurata come un bridge in grado cioè di far passare tutti i pacchetti dati indipendentemente dall'IP di origine.

Il totem informativo è stato collegato in modalità wireless.

3.4 ITIS "A. Volta", Tivoli

Sulla facciata esterna dell'edificio è stata installata l'antenna ricevente del link Fermi-Volta. Un apparato VPN Client Syneto 810 è stato inserito nel rack dati all'interno dell'aula d'informatica al piano terreno. Il router ADSL per il traffico verso internet dell'Istituto Volta è stato collegato sulla porta WAN (porta 1) del Syneto 810 mentre il cavo proveniente dall'antenna del link Fermi-Volta è stato collegato alla porta LAN (porta 1). La porta LAN (porta 2) dello stesso apparato è stata collegata al primo Access Point della WLAN del Volta. Nel caso dei due Istituti, Fermi e Volta, si è preferito utilizzare un solo client VPN e collegare tra loro le due WLAN per mezzo del ponte Wireless. In questo modo le due reti sono sullo stesso piano d'indirizzamento e i client che si collegano sulla rete hanno piena visibilità degli altri apparati. Si è scelto di allocare il Client VPN presso il Volta in quanto questo Istituto ha un collegamento ADSL Telecom con più di un indirizzo IP pubblico disponibile. Attraverso questo IP viene proiettata la rete verso internet ed instaurato il Tunnel verso il server VPN del CNR. L'Enrico Fermi ha invece un collegamento ADSL fornito da Tiscali che non rende disponibili IP pubblici oltre quello da contratto.

Il totem informativo è stato collegato in modalità wireless.

L'IP pubblico utilizzato è 88.49.239.36.

3.5 IISS "Quarenghi", Subiaco

Presso l'Istituto Quarenghi è stato installato un Client VPN Syneto 810. Sulla porta WAN (porta 1) è stato collegato il router ADSL per il traffico verso internet mentre sulla porta LAN (porta 2) è stato collegato il primo degli Access Point della WLAN. Il totem informativo è stato collegato alla porta LAN (porta 3) del Synerto.

L'IP pubblico utilizzato è 88.44.105.202.

3.6 IIS "Pier Luigi Nervi", Rignano Flaminio

Presso l'Istituto P.L. Nervi è stato installato un Client VPN Syneto 810. Sulla porta WAN (porta 1) è stato collegato il router ADSL per il traffico verso internet mentre sulla porta LAN (porta 2) è stato collegato il primo degli Access Point della WLAN. Il totem informativo è stato collegato alla porta LAN (porta 3) del Synerto.

Non è stato possibile configurare una VPN in quanto il collegamento ADSL dell'Istituto non aveva IP pubblici liberi da dedicare. Sarà oggetto di attività futura.

3.7 La piattaforma di e-learning

Gli istituti scolastici partecipanti al progetto "Tutti per Uno e Uno per Tutti" sono siti nelle città di Tivoli, Rignano Flaminio, Palestrina e Subiaco e quindi era necessario disporre di una soluzione informatica che rendesse possibile la condivisione dei contenuti didattici prodotti dai docenti. Oltre a questo requisito era importante disporre di un programma che rendesse agevole sia ai docenti che all'amministratore del server la gestione dei corsi e degli studenti. La soluzione adottata è stata quella di collegare tra loro gli Istituti scolastici con una rete infor-

matica ad alte prestazioni e di adottare un software unico di gestione dei contenuti didattici e degli iscritti ai corsi.

Fig. 2

Tra i vari prodotti disponibili si è scelto Moodle (http://moodle.org/?lang=it) per le seguenti ragioni:

- la piattaforma Moodle può essere gestita attraverso una semplice interfaccia grafica web;
- gli insegnanti tramite l'interfaccia web possono creare, gestire i corsi, e seguire gli studenti.
- Gli studenti possono essere coinvolti nella produzione di nuovi contenuti didattici. Il materale da loro prodotto sarà utilizzabile per arricchire e aggiornare i corsi.
- il software è di tipo open-source, cioè libero da vincoli di licenza commerciale, e mantenuto in modo gratuito dalla comunità degli utenti.
- La piattaforma è adottata da molte università e è quello dell'Università degli Studi di Roma.
- La gestione dei contenuti didattici è stata centralizzata su un server dell'Area di Ricerca di Roma1 del CNR. Le prestazioni del server e della rete informatica a cui è connesso, consentono ad un buon numero di studenti di accedere contemporaneamente e nell'arco delle 24 ore, sia in classe che a casa, ai corsi presenti sulla della piattaforma Moodle;

Fig. 3

Moodle (acronimo di *Modular Object-Oriented Dynamic Learning Environment*) è un piattaforma web open source per l'e-learning, chiamata anche Course Management System, progettata per aiutare gli insegnanti e gli educatori a creare e gestire corsi on-line con ampie possibilità di interazione tra studente e docente. Attraverso questo strumento informatico è possibile realizzare corsi di formazione, seminari, distribuzione materiale informativo e ecc. senza la contemporanea presenza, nello stesso luogo, dei docenti e degli studenti. Il software è di tipo modulare e quindi estremamente flessibile per la creazione dei corso. I moduli a disposizione dei docenti sono i seguenti:

- **Lezioni** con domande multiple, vero/falso, a completamento, ecc.
- **Lezioni** dei partecipanti per la discussione degli argomenti del corso;
- **Chat** per discussioni e spiegazioni in tempo reale tra docente e studente su singoli argomenti;
- **Quiz** per la valutazione delle competenze acquisite dagli studenti;
- **Blog** (diari);
- **Glossario**;
- **Videoconferenze**;
- **Wiki** per la realizzazione di nuovo materiale didattico attraverso la collaborazione tra docenti e studenti;

La piattaforma Moodle consente di assegnare i seguenti ruoli agli iscritti:

- **Amministratore**: Gli Amministratori normalmente possono fare tutto nel sito e in tutti i corsi presenti.
- **Creatore Corsi**: I creatori di corsi possono creare nuovi corsi e insegnare negli stessi.
- **Docente**: I docenti possono fare tutto all'interno di un corso, compresi la modifica delle attività e della valutazione degli studenti.
- **Docente non editor**: I docenti svolgono il corso, seguono gli studenti ma non possono modificare il corso e le attività presenti.
- **Studente**: Partecipa ai corsi e alle attività in essi presenti.
- **Ospite**: Può solo prendere visione di alcuni corsi e consultare la homepage del sito.

Il software è stato ottenuto dal sito:http://moodle.org/ nella versione 1.9, successivamente aggiornato alla versione 2.3, ed installato sul server dell'Area di Ricerca di Roma1 e adattato alle esigenze dei cinque istituti scolastici. La piattaforma è raggiungibile al seguente indirizzo: http://fermi.mlib.cnr.it

Dopo aver installato il software, è stato preparato un corso di base sul Moodle rivolto agli insegnanti che dovranno creare e gestire i corsi su questa piattaforma. E' stata anche realizzato un corso di prova per i docenti dove svolgere delle esercitazioni sulla creazione delle diverse attività didattiche.

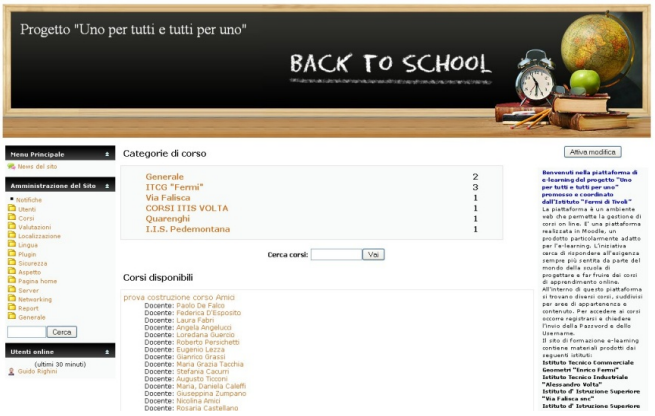


Fig. 4

Nelle sedi dei cinque istituti scolastici si sono tenute una serie di lezioni di 150 ore complessive sull'utilizzo del software e delle esercitazioni pratiche sulla preparazione delle lezioni, dei questionari, dei glossari, e sulla pianificazione dello svolgimento del corso. Nella sola sede dell'Istituto Tecnico Commerciale "Fermi" di Tivoli si è tenuto anche un corso avanzato sulla amministrazione della piattaforma e sulla gestione degli iscritti al corso. Alla fine del corso gli insegnati hanno realizzato i contenuti didattici previsti per il progetto "Tutti per Uno e Uno per Tutti".

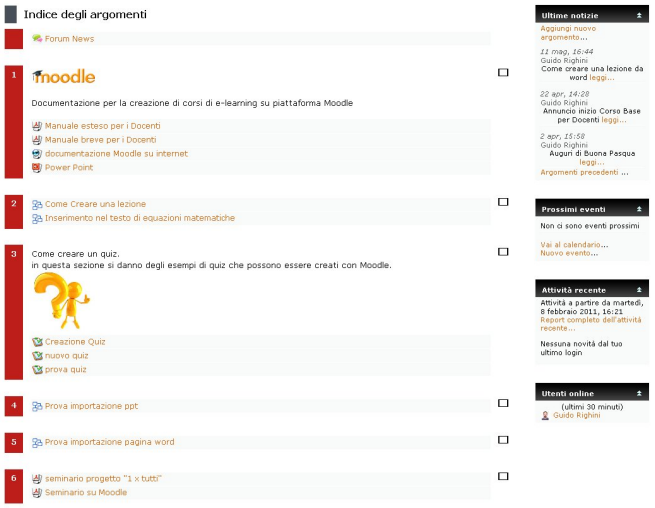


Fig. 5

4 Conclusioni

Il presente progetto finanziato dalla Regione Lazio con un contributo di € 20.000,00 è terminato nell'Aprile 2011. La conclusione del progetto è stata ratificata con un evento tenutosi il giorno 12/04/2011 presso l'Istituto E. Fermi di Tivoli.

Riferimenti

1 documentazione moodle http://moodle.org.

2 piattaforma informatica di e-learning del progetto: http://fermi.mlib.cnr.it.

E-Learning & Scientific Communication

Piano Regionale di Implementazione per una Cultura di Orientamento Formativo – Progetto “Il Verde Orienta”.†

Augusto Pifferi,[a] Luca Ianniello,[a] Claudio Ricci,[a] Guido Righini[b]

Il rapporto descrive la soluzione tecnica adottata dal CNR a supporto degli obiettivi del Progetto “Il Verde Orienta”. La piattaforma informatica realizzata e i corsi di formazione per i docenti svolti dal CNR hanno consentito a 15 istituti scolastici della provincia di Roma di realizzare e condividere contenuti didattici in modo cooperativo e renderli disponibili ad una utenza diffusa nel territorio.
Keywords: Educazione Ambientale, Formazione a Distanza, Condivisione contenuti Didattici.

1 Introduzione

A valle dell’esperienza conseguita nel progetto “Capitale Umano - Uno per tutti-tutti per uno”,[1] nel quale il CNR ha contribuito alla realizzazione di una rete Virtuale Privata (VPN) tra cinque scuole e di una piattaforma di e-learning (http://fermi.mlib.cnr.it), si sono create le premesse per la realizzazione di nuovi progetti. Il successo di questa iniziativa è stato tale che nell”ambito del “Piano regionale di implementazione di una cultura della didattica orientativa”; Progetti finanziati - D.D.G. n. 56 del 13 luglio 2010 l’Istituto Tecnico “E. Fermi” di Tivoli si è visto riconoscere un finanziamento, dall’Ufficio Scolastico Regionale del Lazio, per un progetto che è stato intitolato “Il Verde Orienta”. In questo modulo sono previsti dei corsi con docenti esperti del CNR per l’utilizzo della piattaforma di e-learning realizzata dall’Istituto di Cristallografia e la creazione di un portale didattico espressamente dedicato a questo progetto.

2 Descrizione del Progetto

Il progetto si pone l’obiettivo di individuare, perseguire ed implementare modelli innovativi per l’attuazione di opportune didattiche orientative in un curriculum verticale.

La metodologia di attuazione prevedeva:

- la formazione dei docenti coinvolti finalizzata all’acquisizione di un codice metodologico- didattico comune.
- la strutturazione di percorsi co-progettati aventi come filo conduttore l’Educazione Ambientale che evidenzi le possibilità del territorio, rappresenti una opportunità di divulgazione di conoscenze naturalistiche e permetta la partecipazione attiva degli studenti (anche in fase progettuale) e delle famiglie in fase di realizzazione.
- La socializzazione degli obiettivi e degli esiti con l’opportuno utilizzo della strumentazione tecnologica innovativa già implementata nell’istituto capofila.

Le sequenziali finalità della suddetta metodologia sono:

- La prevenzione della dispersione scolastica e la rinnovata attenzione a modalità didattiche che tengono conto delle esperienze informali dei ragazzi.
- Un nuovo modo di fare Scuola sempre più aperto al territorio che non si esaurisca tra le mura di un aula, ma si traduca nel vivere quotidiano in forme autonome e consapevoli.

Scuola capofila: Istituto Tecnico Commerciale e per Geometri “E. Fermi” Tivoli

Scuole aderenti al progetto:

1. ICS “Baccelli” Tivoli;
2. ICS “Pacifici” Tivoli – Villa Adriana;
3. SMS “Giovanni XXIII” Villanova;
4. ICS “Vicocaro”;
5. SMS “E. Segrè” Tivoli;
6. ICS “Poli”;
7. ICS “Castel Madama”;

[a] CNR - Istituto di Cristallografia, Strada Provinciale 35/d, Montelibretti, Italia
[b] CNR - Istituto di Struttura della Materia, Strada Provinciale 35/d, Montelibretti, Italia

† Rapporto Tecnico IC 11/09 registrato con numero di protocollo IC/1507 del 22/08/2011

8. ICS “Don Milani” Guidonia;
9. ICS “De Filippo” Guidonia;
10. ICS “Leonardo da Vinci” Guidonia;
11. ICS “Marcellina”; IC “Palombara”;
12. IC “Gulluni” Colonna;
13. SMS “Minniti” Guidonia;
14. Istituto Istruzione Professionale “Palestrina”

3 Attività del CNR nell’ambito del progetto

Una delle finalità del progetto è la diffusione dei materiali didattici prodotti; questi materiali devono essere disponibili ai docenti, agli studenti e ai genitori delle scuole aderenti al progetto. Data la diffusione territoriale delle scuole è preferibile l’uso di una piattaforma informatica per l’e-learning. Le piattaforme di e-learning, sfruttando la diffusione della rete informatica consentono di realizzare questo obbiettivo. Il CNR ha realizzato una piattaforma informatica di e-learning ad hoc su uno dei suoi server adattandola alle esigenze del progetto. Inoltre, esperti del CNR hanno tenuto delle lezioni specifiche sull’uso del software di e-learning ai docenti delle scuole partecipanti.

4 Descrizione dettagliata dell’attività svolte.

4.1 Scelta dell’infrastruttura informatica.

Il progetto ha previsto la condivisione delle risorse didattiche prodotte, non limitata ai soli edifici scolastici ma a tutto il territorio della provincia romana. In considerazione di questa esigenza si è scelto di utilizzare il server del Servizio Reti dell’Area di Ricerca di Roma 1 CNR dedicato alla didattica perché collegato alla rete internet con linee ad alta capacità ed affidabilità. Le prestazioni del server e della rete informatica a cui è connesso consentono ad un buon numero di studenti di accedere contemporaneamente e nell’arco delle 24 ore, sia in classe che a casa, ai corsi presenti sulla piattaforma informatica. Al sito si è assegnato un nome specifico (verdeorienta.mlib.cnr.it) per renderlo facilmente riconoscibile tra quelli presenti sul server e sulla rete internet nazionale.

4.2 Scelta della piattaforma informatica di e-learning.

Si è scelti di utilizzare come piattaforma informatica di e-learning, il software Moodle per i seguenti motivi:

- gestione facilitata e sicura del sito attraverso una semplice interfaccia grafica web;
- gli insegnanti, tramite un interfaccia grafica, possono creare, in remoto e in modo semplice, i contenuti didattici richiesti dal progetto, possono seguire gli studenti durante lo svolgimento del corso attraverso gli strumenti di comunicazione presenti. Per la comunicazione sono disponibili i servizi di forum, chat, messaggistica;
- gli studenti possono essere coinvolti nella produzione di nuovi contenuti didattici da mettere a disposizione del progetto;
- la piattaforma è molto flessibile e si adatta ad ogni tipo di esigenza didattica. Per questa sua caratteristica è stata adottata sia da scuole materne che da università, sia esse di piccole che di grande dimensione;
- il software è open source e con licenza d’uso gratis. Il supporto tecnico e una ampia documentazione è disponibile nel sito https:/moodle.org. Il software è curata dalla comunità degli utilizzatori presente in più di 210 nazioni. Il software può essere installato sia su personal computer che su grandi server e esiste un unica versione per ogni tipo di sistema operativo. Questa caratteristica è un vantaggio perché i corsi realizzati possono essere utilizzati su sistemi operativi diversi. Le interfacce grafiche degli utenti possono essere personalizzate secondo le esigenze degli utilizzatori.

Descrizione della piattaforma

Moodle[2] (acronimo di Modular Object-Oriented Dynamic Learning Enviroment) è una piattaforma web open source per l’e-learning, chiamata anche Course Management System, progettata per aiutare gli insegnanti e gli educatori a creare e gestire corsi on-line con ampie possibilità di interazione tra studente e docente. Attraverso questo strumento informatico è possibile realizzare e svolgere corsi di formazione senza la contemporanea presenza, nello stesso luogo, dei docenti e degli studenti. Il software è di tipo modulare e quindi estremamente flessibile per la creazione di corsi con finalità didattiche diverse. I moduli a disposizione dei docenti sono i seguenti:

- **Lezioni** con domande multiple, vero/falso, a completamento frase, numeriche, ecc.;
- **Forum** dei partecipanti per la discussione degli argomenti svolti nel corso;
- **Chat** per discussioni e spiegazioni, in tempo reale, tra docente e studente su singoli argomenti;
- **Quiz** per la valutazione delle competenze acquisite dagli studenti. Il modulo include anche strumenti di valutazione dell’efficacia del quiz proposto;
- **Blog** (diari)
- **Glossario** dei termini utilizzati nel corso. Per la sua realizzazione vengono coinvolti i partecipanti del corso;
- **Videoconferenze**;
- **Wiki** per la creazione di nuovo materiale didattico attraverso al collaborazione insegnante e studenti.

La piattaforma Moodle consente una gestione semplice dei ruoli dei partecipanti al corso. I ruoli che possono essere assegnati sono:

- **Amministratori**: sono incaricati di gestire ogni aspetto della piattaforma;
- **Creatori di corsi**: sono incaricati di creare i corsi, inserendo e modificando le attività e le risorse, oltre a insegnare negli stessi;
- **Docenti**: sono incaricati di svolgere il corso e di seguire gli studenti. Possono modificare lo svolgimento del corso e valutano gli studenti;
- **Docenti non editor**: sono incaricati dai docenti di svolgere il corso ma non possono modificare le attività presenti;
- **Studenti**: partecipano ai corsi e alle attività in essi presenti;
- **Ospite**: può prendere visione di alcune attività dei corsi e consultare la pagina iniziale del sito.

La struttura della piattaforma è stata modificata in base alle esigenze del progetto "Il Verde Orienta" e installata su un server dell'Area di Ricerca di Roma1 del C.N.R. il cui indirizzo è il seguente:

http://verdeorienta.mlib.cnr.it

Qui di seguito una figura rappresentante la prima pagina del sito (vedi fig. 1).

Dopo aver installato il software, è stato organizzato un breve corso di 30 ore su Moodle per il personale docente coinvolto nel progetto. Il corso si è svolto presso la sede dell'Istituto Tecnico Commerciale e per Geometri "E. Fermi" di Tivoli ed è stato tenuto da docenti dell'istituto e da due esperti del C.N.R.

Fig. 1 Homepage del sito Verde Orienta.

5 Conclusioni

La realizzazione di una piattaforma di e-learning dedicata si è dimostrata ancora una volta una scelta opportuna quanto utile. Questo servizio, nato per assolvere uno degli obiettivi di un progetto specifico, è utilizzabile in tutte quelle occasioni, istituzionali e/o commerciali, in cui occorra erogare corsi la cui fruibilità necessiti di tempi brevi di realizzazione, ampia diffusione tramite i moderni sistemi di rete e semplicità di realizzazione. Non è escluso che in futuro questa servizio possa essere utilizzato per nuovi progetti che coinvolgono la scuola italiana. Il successo ottenuto ha reso necessaria la realizzazione di una nuova piattaforma, configurata con le ultime release di Moodle, PHP e MySQL che presto affiancherà quella esistente.

Riferimenti

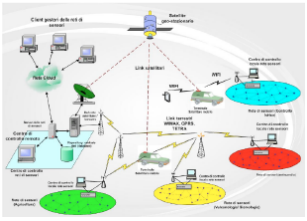
1 G. Righini, A. Pifferi, M. Catricalà, A. D. Simone, L. Ianniello, C. Ricci, M. Simonetti, L. Rossi, G. Agostini, G. Nantista, Progetto regione lazio: Interventi di innovazione e potenziamento del sistema regionale d'istruzione – az.b. proposta formativa "uno per tutti-tutti per uno", SMART eLAB 2 (2013) 20–24. doi:10.30441/smart-elab.v2i0.69.

2 Homepage software moodle https//moodle.org.

Networking

Modelli di localizzazione per reti logistiche di emergenza multirischio.†

Giuseppe Confessore,[a] Salvatore Fiorino,[b] Marco Simonetti,[a] Giuseppe Stecca[a] Antonio Toscano[c]



Il presente lavoro rientra nell'ambito degli studi condotti dal gruppo di lavoro per il progetto PON 2007 – 2013 – ASSE I (Piano Operativo Nazionale) denominato SIGMA (Sistema Integrato di sensori In ambiente cloud per la Gestione Multirischio Avanzata). Il progetto vede tra gli attori principali per la progettazione e lo sviluppo della piattaforma il CNR. Lo scopo del lavoro è l'analisi e la formalizzazione di problematiche di logistica in situazioni di rischio, note anche come logistica di emergenza. In particolare la problematica affrontata è la progettazione del network logistico consistente delle facilities dove collocare il personale e le attrezzature di intervento e delle connessioni tra le facilities e i luoghi di intervento. Il problema è stato modellato tramite delle variazione al problema CFLP (Capacitated Facility Location Problem). E' stato sviluppato il modello di programmazione mista (MILP - Mixed Integer Linear Programming) tramite l'ambiente CPLEX Optimization Studio v 12.5. Sono stati condotti dei test ed è stata fatta analisi di sensitività a partire da istanze relative al Sistema Informativo Territoriale Regionale (SITR) Siciliano.

Keywords: Monitoring System, Emergency logistics, MILP (mixed integer linear programming), Location - allocation, CPLEX.

1 Introduzione

Il presente articolo descrive alcuni modelli di ottimizzazione per la logistica di emergenza sviluppati nell'ambito del progetto PON 2007 – 2013 – ASSE I (Piano Operativo Nazionale) denominato **SIGMA** (*Sistema Integrato di sensori In ambiente cloud per la Gestione Multirischio Avanzata*) che vede tra gli attori principali per la progettazione e lo sviluppo della piattaforma il CNR. Il lavoro di modellazione e ottimizzazione di processi decisionali è stato sviluppato attraverso l'applicazione di competenze proprie della ricerca operativa e dell'ingegneria gestionale e finalizzate allo sviluppo di metodologie e strumenti per il supporto alle decisioni strategiche, tattiche ed operative.

Il Sistema Integrato di sensori in ambiente cloud per la Gestione Multirischio Avanzata (SIGMA) è un'architettura multilivello che ha la funzione di acquisire, integrare ed elaborare dati eterogenei provenienti da diverse reti di sensori (meteo, sismiche, vulcaniche, idriche, pluviali, del traffico auto e navale, ambientali, video, ecc..) con lo scopo di potenziare i sistemi di controllo e di monitoraggio sia ambientali che di produzione industriale per fornire dati utili alla prevenzione e gestione di situazioni di rischio tramite servizi erogati al cittadino ed alle imprese, sia pubbliche che private. Il sistema verrà progettato per consentirne l'utilizzo anche in aree e situazioni critiche nelle quali non siano disponibili le normali infrastrutture di comunicazione necessarie a veicolare i dati raccolti dalle reti di sensori.

La parte innovativa del lavoro riguarda la modellazione degli eventi di rischio che vengono suddivisi in classi e risorse specifiche per ciascuna di queste tipologie. Nel presente lavoro, verranno poi descritti alcuni concetti legati alla realizzazione e configurazione nell'infrastruttura di telecomunicazione che veicola le informazioni e al sistema informativo che ne permette la raccolta e l'utilizzo dei dati. Lo scopo del lavoro è l'analisi e la formalizzazione di problematiche di logistica in situazioni di rischio note anche come logistica di emergenza o emergency lo-

[a] *CNR - Istituto delle Tecnologie Industriali e Automazione, Strada Provinciale 35/d, Montelibretti, Italia*

[b] *CNR - Istituto di Studi sul Mediterraneo Antico, Strada Provinciale 35/d, Montelibretti, Italia*

[b] *Nuconga s.r.l. (http://www.nuconga.com) – Tesista presso l' Istituto delle Tecnologie Industriali e Automazione (ITIA).*

gistics[1]. In particolare la problematica affrontata è la progettazione del network logistico consistente delle facilities dove collocare il personale e le attrezzature di intervento e delle connessioni tra le facilities e i luoghi di intervento.

Il problema è stato modellato tramite delle variazioni applicate al problema CFLP (Capacitated Facility Location Problem).

L'articolo è strutturato nel seguente modo: Nella seconda sezione vengono introdotti i concetti di rischio e di logistica di emergenza. Verrà poi descritta in Sezione 3 la progettazione architetturale del sistema. Successivamente, in Sezione 4 vengono descritti i modelli ed algoritmi di localizzazione dei nodi logistici. La Sezione 4 presenta un modello architetturale in grado di fornire supporto alle operazioni di gestione delle emergenze. In Sezione 5 viene descritta l'implementazione del modello tramite il linguaggio di programmazione matematica OPL. Infine la Sezione 6 presenta l'ambiente di test, le simulazioni e le conclusioni.

2 Logistica e logistica d'emergenza

La logistica è la disciplina che si occupa di definire le modalità di gestione (pianificazione, esecuzione e controllo) del flusso di persone, beni e servizi da un punto sorgente (fornitore) ad un punto destinazione (cliente).

La gestione della logistica è una attività fondamentale nelle situazioni di emergenza. In[1] la logistica di emergenza o emergency logistics viene definita come "*A process of planning, managing and controlling the efficient flows of relief, information, and services from the points of origin to the points of destination to meet the urgent needs of the affected people under emergency conditions*". Per la logistica di emergenza è fondamentale la previsione e stima dei rischi. A valle del processo di previsione e di stima dei rischi è necessario definire tutte le attività per gestire un sistema strutturato che preveda il movimento di uomini e mezzi finalizzate a:

- evacuazione della popolazione colpita da un evento
- soccorso dei feriti
- rifornimento di tutti i beni necessari per il primo intervento (cibo, farmaci, vestiario, tende, etc..)
- organizzazione rete di trasporto
- organizzazione rete di depositi
- approvvigionamento di beni e servizi
- selezione aree per destinazione.

Durante l'attività di pianificazione viene individuata l'area che è potenzialmente soggetta ad eventi; attorno ad essa vengono definite le aree necessarie allo svolgimento delle attività emergenziali come:

- raccolta della popolazione colpita nell'immediatezza dell'evento
- ricovero della popolazione colpita dall'evento
- ricovero degli uomini che prestano il soccorso
- centri di coordinamento locale soccorsi e attività collegate
- mezzi di soccorso (ospedali, ambulanze, etc..)
- stoccaggio beni di soccorso e per il funzionamento di tutta la macchina organizzativa.

Dette aree devono essere determinate in base al ruolo che devono svolgere, ad un buon posizionamento rispetto a nodi stradali strategici, all'assenza di nuovi rischi, alla possibilità di usufruire di servizi essenziali quali, ad esempio, acqua ed energia elettrica. L'evacuazione e il supporto logistico sono le due attività principali condotte nelle fasi dell'emergenza in risposta ad un disastro. Le attività di evacuazione si svolgono durante la fase iniziale, mentre le operazioni di supporto logistico tendono a continuare per lungo tempo per sostenere le esigenze di base dei sopravvissuti che rimangono nella zona colpita. La tempestiva disponibilità di beni come il cibo, riparo, medicine e l'organizzazione efficace ed efficiente del trasporto dei feriti hanno un effetto sul tasso di sopravvivenza nelle zone colpite. Pertanto, si rende necessario attivare tutte le misure atte alla minimizzazione dei ritardi nella fornitura e nel trasporto dei beni di prima necessità dai grandi centri di stoccaggio ai centri di distribuzione localizzati in prossimità delle aree colpite e del trasporto dei feriti ai centri medici di emergenza, per i quali possono essere utilizzati diversi tipi di veicoli.

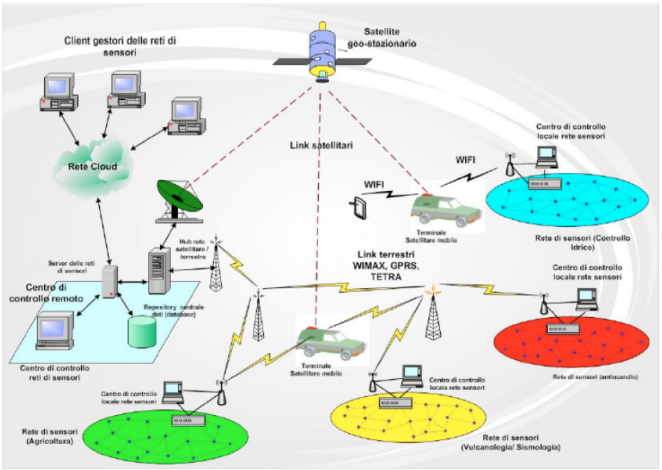


Fig. 1 Piattaforma SIGMA, schema concettuale

2.1 Progettazione architetturale del sistema

L'architettura proposta deve supportare le esigenze specifiche della logistica di emergenza e a tale scopo prevede una struttura a strati che copre tutti i livelli, garantendo indipendenza funzionale dei singoli strati rispetto all'intero sistema. Le funzionalità generali che si desidera raggiungere con questo sistema sono:

- monitoraggio, tramite le reti di sensori, dei parametri che sono indicativi delle situazioni di

rischio

- trasferimento dei dati fisici rilevati dalle reti di sensori verso il centro di elaborazione attraverso l'uso di opportune reti di telecomunicazioni in grado di erogare servizi con continuità ed affidabilità
- garantire uniformità dei dati provenienti dalle diverse reti eterogenee utilizzando filtri e regole ad hoc
- garantire l'accesso in mobilità alle applicazioni e ai dati utilizzati per la gestione delle attività di emergenza, monitoraggio e controllo con elevata qualità di servizio (QoS)
- implementare moduli di Decision Support System (DSS) in grado di fornire modelli previsionali, strumenti di simulazione dei possibili scenari e strumenti di controllo avanzati di supporto alle decisioni
- garantire la scalabilità, la flessibilità e la robustezza di tutto il sistema al fine di poter integrare con il minimo impatto eventuali nuovi servizi e nuove funzionalità.

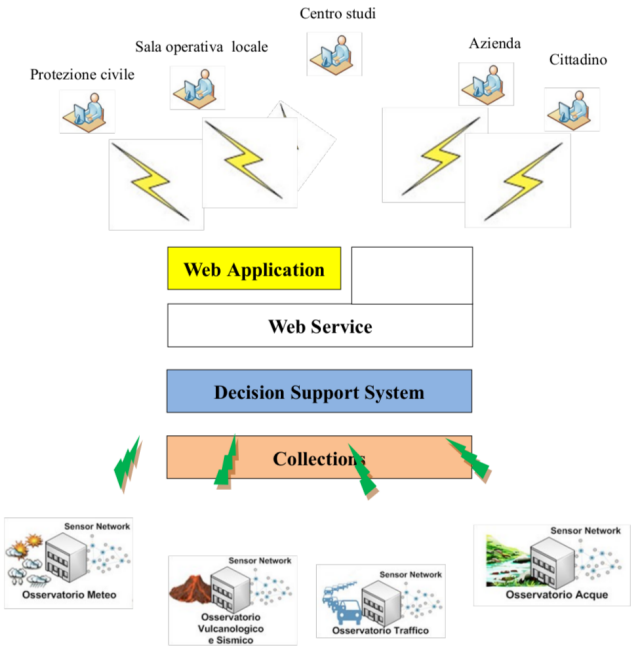


Fig. 2 Architettura del sistema

2.2 Livello "Sensor Network"

Partendo dal livello più basso troviamo le reti di sensori che costituiscono l'ossatura portante in quanto rappresentano il punto di acquisizione e trasmissione dei dati che alimenta l'intero sistema. La rilevazione dei dati proviene da diverse reti eterogenee e pertanto si tratta di dati grezzi non omogenei e non sempre comparabili.

Per garantire affidabilità, robustezza, sicurezza e continuità di servizio è necessaria una infrastruttura di telecomunicazioni ridondante che possa rispondere a qualunque scenario; oltre alle reti wired, si ricorre alle reti di telefonia mobile (GPRS, 3G, LTE), WIMAX, satellitare facendo uso di alcune tecniche messe in atto in campo militare in presenza di uno scenario di guerra dove la gestione delle comunicazioni è affidata a reti definite ad hoc e dove le reti tradizionali sono spesso inesistenti o fuori uso. Inoltre, il ricorso alle Virtual Private Network (VPN) consente di stabilire delle connessioni logiche private utilizzando connessioni fisiche pubbliche; ciò è implementabile tramite la costituzione di un tunnel tra due router e uno strato di crittografia che consente la trasmissione sicura delle informazioni su una rete non sicura.

2.3 Livello "Collections"

Questo strato si pone come collettore delle reti di sensori sul campo e fornitore di collezioni di dati significative per i livelli superiori. In particolare esso ha il compito di:

- interfacciare, tramite drivers, le diverse reti eterogenee di sensori
- raccogliere la grossa mole di dati e su di essi applicare opportuni filtri e regole in grado di uniformarli eliminando ridondanze e dati non significativi o aggregandone parte di essi
- alimentare il database utilizzato per le elaborazioni dello strato superiore di "Decision Support System"

La tempestività e la delicatezza delle attività svolte da questo strato impongono, l'adozione di tutti gli strumenti in grado di garantire elevate prestazioni nella massima sicurezza ed affidabilità.

2.4 Livello "Decision Support System"

Questo livello si preoccupa di implementare l'attività di analisi dei dati, simulazione e di ottimizzazione delle soluzioni in modo da fornire strumenti (cruscotti) decisionali agli operatori del sistema. I dati depositati nel database dal livello sottostante, vengono estrapolati in maniera coerente all'utilizzo attraverso l'uso di viste specifiche; successivamente si procede alla loro elaborazione attraverso i modelli sviluppati e per finire si espongono i dati che sono di utilità per le analisi, il monitoraggio, il controllo e il supporto alle decisioni.

2.5 Livello "Web Service"

L'uso della tecnologia dei Web Service è ormai affermata da diversi anni e consente di realizzare l'interfaccia tra un sistema ed il mondo esterno attraverso lo scambio di messaggi disaccoppiando così i servizi di elaborazione e di logica applicativa rispetto alle applicazioni di vera e propria presentazione all'utente, così da rendere i servizi indipendenti dalla piattaforma client utilizzata (hardware/software).

Attraverso questa struttura è possibile esporre all'esterno una serie di servizi che possono essere utilizzati sia da applicazioni di presentazione web facenti parte del sistema stesso e sia da applicazioni esterne che possiedono una propria interfaccia grafica utente.

Ad esempio, ciò consente di sviluppare una applicazione di mobilità per uno smartphone/tablet che necessità di una interfaccia grafica diversa e più leggera rispetto ad una applicazione desktop per personal computer; il tutto utilizzando sempre lo stesso motore di logica applicativa i cui servizi sono disponibili tramite Web Service senza necessità di fornire dettagli sulla sua implementazione interna.

2.6 Livello "Web Application"

A questo livello vengono realizzate le applicazioni grafiche di interazione con l'utente che consentono di effettuare l'input dei parametri di ingresso e l'output dei risultati oggetto dell'elaborazione. Queste applicazioni vengono tipicamente sviluppate per dare accesso diretto agli utenti interni al sistema stesso. Naturalmente visto il ruolo ricoperto da questo livello, si prevede l'implementazione di un sistema di sicurezza e di gestione delle credenziali che possa essere in grado di garantire l'accesso agli utenti autorizzati e la riservatezza dei dati.

3 Modelli per la localizzazione

Il problema della localizzazione, in generale, è un quesito molto caro alle logiche industriali e commerciali, e si pone principalmente come obiettivo quello di applicare dei modelli di risoluzione che permettano di individuare il luogo di posizionamenti di un nodo (sia esso un magazzino, una fabbrica, centro di smistamento, ecc..) al fine di minimizzare i costi e massimizzare il profitto a parità di servizio fornito ai clienti. Logicamente la scelta delle localizzazioni ottimali deve avvenire in relazione alla funzione obiettivo che vogliamo massimizzare (minimizzare) e che a sua volta è fortemente influenzata dalle caratteristiche del servizio, dalle caratteristiche degli impianti dalla struttura della domanda di servizio e dalla struttura delle funzioni di costo. A seguire verranno introdotti alcuni dei modelli di Programmazione Lineare (PL) che sono di supporto alle decisioni di Facility Location Problem (FPL). Questo problema in letteratura è anche noto come plant location problem; a seconda che ciascuna potenziale facility abbia capacità finita o meno il problema è chiamato Capacitated Facility Location Problem (CFLP) oppure Uncapacitated Facility Location Problem (UFLP).[2] Nel caso di interesse è necessario tener conto della capacità limitata dei siti e quindi verranno sviluppati modelli Capacitati (CFLP).

3.1 Modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-LETTERATURA)

Analizziamo un problema di tipo CFLP in cui si prevede la gestione di un solo prodotto attraverso una struttura a singolo livello da sorgente (S) a destinazione (D) (es. fornitore, cliente); inoltre si considera il caso in cui ogni nodo (facility) abbia capacità finita e la domanda sia frazionabile.

L'obiettivo che vogliamo raggiungere è la determinazione della:

- Localizzazione, cioè quali nodi (facility) attivare
- Allocazione delle risorse, cioè come distribuire la domanda sulle facility attivate in relazione alle disponibilità e alle logiche individuate
- Minimizzazione, cioè, nello specifico, mantenere il più bassi possibili i costo fissi e quelli variabili.

Il modello dunque può essere definito come segue:

- Un grafo $G = \{S \cup D,\ A\}$, con S che rappresenta l'insieme dei nodi SORGENTE da attivare (facility potenziali), D i nodi DESTINAZIONE (pozzo, beni o clienti da servire) ed A rappresenta l'insieme degli archi che collegano S e D $(A \subseteq S \times D)$;
- $d_j,\ (j \in D)$ è la stima della domanda del nodo j ed è costante durante l'orizzonte temporale di panificazione;
- $q_i,\ (i \in S)$ è il massimo livello di attività del nodo potenziale i ed è costante durante l'orizzonte temporale di pianificazione
- $y_i,\ (i \in S)$ che rappresenta una variabile binaria (1,0) con la quale indichiamo l'attivazione o meno di uno specifico nodo (1 = nodo attivato, 0 = nodo non attivato)
- $x_{ij},\ (i \in S, j \in D)$ rappresenta una variabile che indica la frazione di quantità richiesta dal nodo j e rifornita da i
- $c_{ij},\ (i \in S, j \in D)$ sono i costi legati al flusso dal nodo sorgente i al nodo destinazione j
- $f_i,\ (i \in S)$ rappresenta il costo legato all'attivazione del nodo facility i.

La funzione obiettivo per costi lineari è la seguente:

$$\text{(f.o.)} \quad min \sum_{i \in S} \sum_{j \in D} c_{ij} x_{ij} + \sum_{i \in S} f_i y_i$$

che minimizza i costi complessivi di attivazione e localizzazione facility.

I vincoli invece sono:

1. $\sum_{i \in S} x_{ij} = 1, j \in D$
2. $\sum_{j \in D} d_j xij \leq q_i y_i, i \in S$
3. $x_{ij} \geq 0, i \in S, j \in D$
4. $y_i \in \{0,1\}, i \in S$

dove:

1. garantisce che la domanda di ogni nodo cliente j sia soddisfatta;
2. garantisce che il flusso in uscita dal nodo i non superi il livello massimo consentito q sul nodo stesso;
3. garantisce che ci sia quantità richiesta di generico servizio tra i e j
4. garantisce che il nodo faccia parte degli attivabili.

Il problema CFPL è un problema che rientra tra quelli NP-difficili o NP-ardui (NP-hard, da non-determistic polynomial-time hard, "difficile non deterministico in tempo polinomiale") e non è risolvibile in tempo polinomiale; quindi per trovare una soluzione si ricorre all'utilizzo di algoritmi euristici.

3.2 Modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-VERSIONE 1)

Il modello sopra enunciato è molto generico e proprio per questo si presta a molte customizzazioni per renderlo adatto al caso in cui lo vogliamo applicare. Un esempio di personalizzazione può essere quello in cui possiamo considerare che il nostro non è un semplice modello di localizzazione, ma che stiamo parlando di un modello per situazioni di emergenza e quindi dobbiamo considerare la minimizzazione dei costi anche in base al fattore di rischio. Pertanto dobbiamo costruire una serie di scenari, dipendenti da altri eventi, che rendono variabile la stima della domanda e dei costi di afferenza. Quindi, per ambiti che si possono definire multi-rischio, prendiamo in considerazione quanto segue:

- d_{jl}, $(j \in D, l \in L)$ rappresenta la stima della domanda del nodo j in funzione dell'evento l, con L l'insieme degli eventi considerati
- q_i, $(i \in S)$ è la capacità massima di attività del nodo potenziale i (costante durante l'orizzonte temporale di pianificazione)
- y_i, $(i \in S)$ che rappresenta una variabile binaria (1,0) con la quale indichiamo l'attivazione o meno di uno specifico nodo (1 = nodo attivato, 0 = nodo non attivato)
- x_{ijl}, $(i \in S, j \in D, l \in L)$ rappresenta una variabile che indica la frazione di quantità richiesta dal nodo j e soddisfatta da i a seguito dell'evento l
- c_{ijl}, $(i \in S, j \in D, l \in L)$ sono i costi legati al flusso dal nodo sorgente i al nodo destinazione j in funzione dell'evento l
- f_i, $(i \in S)$ rappresenta i costi legati all'attivazione del nodo facility i.

Pertanto la nuova funzione obiettivo può essere così modificata:

$$(f.o) \quad min \sum_{i \in S} \sum_{j \in D} c_{ijl} x_{ijl} + \sum_{i \in S} f_i y_i$$

Che minimizza i costi complessivi e di attivazione delle facility.

I vincoli, invece, si modificano come segue:

1. $\sum_{i \in S} x_{ijl} = d_{jl}, j \in D, l \in L$
2. $\sum_{j \in D} x_{ijl} \leq q_i y_i, i \in S, l \in L$
3. $x_{ijl} \geq 0, i \in S, j \in D, l \in L$
4. $y_i \in \{0,1\}, i \in S$

3.3 Modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-VERSIONE 2)

Nel modello che andremo ad esplicitare in questo paragrafo, è presente un'ulteriore aggiunta che rende il lavoro ancora più interessante, ovvero andiamo a differenziare il personale che è presente nelle diverse facility (il personale con mansioni diverse viene rappresentato con k). Non vengono messe delle univocità sul personale che dovrà essere utilizzato e l'evento che si deve affrontare, ma viene introdotto un fattore tridimensionale b[j, l, k] o b[Demand] che rappresenta il minimo di personale k da utilizzare per tipo di evento l in una specifica destinazione j. Inoltre tramite un fattore di penalità (o matrice di conversione tra risorse) si potrebbe utilizzare anche altro personale non necessariamente indicato e specializzato per l'evento specifico (per un Incendio anche DPC invece del VdF); l'utilizzo di personale diverso rispetto all'impiego di quello originalmente dichiarato come necessario va ad incidere sul valore della funzione obiettivo.

Quindi, prendiamo in considerazione quanto segue:

- d_{jlk}, $(j \in D,\ l \in L,\ k \in K)$ rappresenta la stima della domanda del nodo j in funzione dell'evento l del personale specializzato k
- q_{ik}, $(i \in S,\ k \in K)$ è il massimo livello di personale di tipo k del nodo potenziale i
- y_i, $(i \in S)$ che rappresenta una variabile binaria (1,0) con la quale indichiamo l'attivazione o meno di uno specifico nodo (1 = nodo attivato, 0 = nodo non attivato)
- x_{ijlk}, $(i \in S, j \in D, l \in L, k \in K)$ rappresenta una variabile che indica la frazione di quantità richiesta dal nodo j e soddisfatta da i a seguito dell'evento l con l'impiego di personale specializzato k
- c_{ijlk}, $(i \in S, j \in D, l \in L, k \in K)$ sono i costi legati al flusso dal nodo sorgente i al nodo destinazione j in funzione dell'evento l con l'impiego di personale specializzato k
- b_{jlk} , $(j \in D, l \in L, k \in K)$ rappresenta il minimo impiego di personale specializzato k nel nodo j in funzione dell'evento l

- w_{lk}, $(l \in L, k \in K)$ rappresenta il fattore di penalità che abbiamo nell'utilizzare specializzato k per l'evento l con k non propriamente specializzato nella risoluzione del problema l
- f_i, $(i \in S)$ rappresenta i costi legati all'attivazione del nodo facility i

Pertanto la nuova funzione obiettivo può essere così modificata:

$$(f.o.)\ min \sum_{i\in S}\sum_{j\in D}\sum_{l\in L}\sum_{k\in K} c_{ijlk}x_{ijlk} + \sum_{i\in S} f_i y_j + \\ + \sum_{j\in D} w_{lk} \times (d_{jlk} - x_{ijlk})$$

Che minimizza i costi complessivi di attivazione e la localizzazione delle facility. I vincoli, invece, si modificano come segue:

1. $\sum_{i\in S} x_{ijlk} \leq d_{jlk},\ j \in D,\ l \in L,\ k \in K$
2. $\sum_{j\in D} x_{ijlk} \leq q_{ik} y_i,\ i \in S,\ l \in L$
3. $x_{ijlk} \geq 0,\ i \in S,\ l \in L,\ j \in D,\ k \in K$
4. $\sum_{i\in S} x_{ijlk} \geq b_{jlk}, j \in D,\ l \in L, k \in K$
5. $y_i \in \{0,1\},\ i \in S$

4 Scelta dello strumento per l'ottimizzazione: CPLEX Optimization Studio

La scelta dello strumento di ottimizzazione è ricaduta su IBM ILOG CPLEX Optimization Studio[3] (o più semplicemente CLEX) che è completamente integrato con OPL (l'IBM è la proprietaria e principale sviluppatrice di entrambi). CPLEX è un solver commerciale (scritto in C) dedicato alla risoluzione e all'ottimizzazione di problemi matematici di vario tipo; è fortemente utilizzato in ambito industriale e di ricerca ed è noto per la sua stabilità e le sue elevate prestazioni (per molto tempo è stato considerato come il più performante ed ha una elevata diffusione sul mercato, oggi esistono ulteriori sistemi allo stesso livello come Gurobi[4], rilasciato da alcuni ex-sviluppatori di CPLEX); CLPEX risolve problemi di PLI tramite diversi algoritmi tra cui diverse implementazioni di Branch&Cut];[5] risolve rilassati continui tramite avanzate routine riconducibili alla tecnica del simplesso.

Come prima operazione viene costruito un albero decisionale in cui ogni nodo corrisponde ad un sotto-problema, poi ogni sotto-problema viene risolto; se ci sono soluzioni frazionarie, vengono introdotti tagli e il modello risultante viene risolto nuovamente (ogni nodo può prevedere più risoluzioni). Se non ci sono più tagli da aggiungere, vengono generati i sotto-problemi tramite branching su una delle variabili frazionarie; l'esplorazione dell'albero continua finché non si giunge alla soluzione ottima. CPLEX è caratterizzato da diversi elementi che lo compongono:

- preprocessing (presolve + probing) nel quale vengono eliminati vincoli e variabili inutili e analizzate le implicazioni logiche derivanti dall'assegnamento di valori interi alle variabili intere;
- i tagli vengono introdotti nel modello in modo statico;
- procedimenti euristici eseguiti "occasionalmente" per migliorare i bound.

CPLEX può essere utilizzato secondo diverse modalità, in relazione all'uso che se ne vuole fare e al contesto di descrizione del problema.

- Modalità interattiva: applicazione con la quale è possibile interagire tramite riga di comando. Si può descrivere il modello del problema (o importarlo da un file esterno) tramite una determinata sintassi, configurare il risolutore tramite l'impostazione di parametri opportuni e infine chiedere l'ottimizzazione del modello specificato
- C Callable Library: libreria di funzioni C tramite le quali si può comandare CPLEX e gestirne le funzionalità
- Concert Technology: le funzionalità di CPLEX sono disponibili sotto forma di librerie (C++, .NET e Java) linkabili in modo dinamico.

Le ultime due modalità permettono di interfacciarsi col risolutore all'interno di un altro software più ampio (embedding), lasciando ad esso il controllo del processo ed e eliminando la necessità di una interazione real-time da parte di un utente.

5 Implementazione, Test e Conclusioni

5.1 Implementazione ed esempio del modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-LETTERATURA)

Partendo dal problema della letteratura possiamo effettuare delle prove sul funzionamento dell'accoppiata CPLEX e OPL, utilizzati dal software IBM ILOG CPLEX Optimization Studio.

Per fare questo, in relazione anche al nostro scopo iniziale, prendiamo in esame una situazione base che si può verificare nella regione Sicilia, la principale fruitrice del nostro lavoro e del bando relativo al progetto SIGMA.

A partire dai dati forniti dal Sistema Informativo Territoriale Regionale (S.I.T.R.) (http://www.sitr.regione.sicilia.it)[6] abbiamo reperito le informazioni di base che ci permettono di creare dei file di partenza (in relazione al nostro modello base creiamo il file .mod e a partire da i primi dati semplici il .dat).

Il modello di riferimento è quello che abbiamo descritto con il nome CFLP-LETTERATURA.

Di seguito vengono spiegate le logiche del caso reale preso in considerazione per testare la nostra prima modellazione del problema. Per far comprendere al meglio il problema e la sua trasposizione in linguaggio matematico, seguono alcune considerazioni e supposizioni importanti che ci rendono più facile intuire il comportamento nei casi reali (nelle successive formulazioni, di volta in volta saremo sempre più specifici e tenteremo di analizzare il più possibile e supporre il meno):

- Per determinare i costi che poi dovremo minimizzare nella nostra funzione obiettivo, siamo partiti da una matrice FACILITY-DESTINAZIONE che contiene le informazioni sulle distanze (archi o strade) tra i vari nodi. • Come ipotesi di partenza fissiamo un costo (nel nostro caso 40 €/km) che chiamiamo costo d'intervento, che rappresenta una stima di quanto dobbiamo spendere per servire una determinata destinazione dalla nostra facility dove sono pronte le forze di soccorso; quindi moltiplicando per 40 tutte le distanze otteniamo i dati inizializzati nella variabile c del file .dat.
- Abbiamo inoltre dei costi specifici (€) di attivazione delle diverse facility rappresentate nel vettore f.
- Abbiamo infine ipotizzato che la capacità di ogni facility sia di 100 unità di personale e che debbano essere servite tutte le destinazioni (quindi il caso peggiore in cui un evento catastrofico sia presente in tutte le nostre destinazioni).

Può essere molto interessante anche capire la sensibilità del modello, in relazione al variare dei parametri; in particolare si possono far variare alcuni dati, come ad esempio, i costi fissi di attivazione (f), le domande (d) ed anche la quantità (q) a disposizione per vedere come cambiano le soluzioni.

Nel vettore delle soluzioni, riportato in appendice, vediamo come il solver, restituisce una soluzione ottima con un valore della (f.o). pari a 7956, dove vengono attivati soltanto due nodi facility, come si può dedurre dal valore della Y (Alì Terme e Ganzirri), che mettono a disposizione il personale per far fronte agli eventi; il vettore X contiene l'informazione sugli archi attivati, cioè come e da chi vengono servite le destinazioni.

Questo caso/esempio iniziale, che può sembrare un semplice esercizio, è in realtà il punto di partenza per il lavoro successivo, al fine di entrare in un contesto che sia meno didattico e più reale e che ci permetta di modellare il problema tenendo entrambi gli occhi ben puntati su quello che si vuole realizzare e sulle possibili implementazioni che modellino il più fedelmente possibile la realtà.

5.2 Implementazione ed esempio del modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-VERSIONE 1)

Il modello di riferimento è quello che abbiamo descritto con il nome CFLP-VERSIONE 1.

Per far comprendere al meglio il problema e la sua trasposizione in linguaggio matematico, seguono alcune considerazioni e supposizioni importanti che ci rendono più facile la descrizione che integrano le considerazioni fatte in merito all'implementazione del modello precedente. Rispetto ad esso, in aggiunta, valgono anche le seguenti considerazioni:

- Abbiamo esplicitato il personale richiesto dai nodi destinazione per sedare l'evento /catastrofe che si è sviluppato.

Dal RUN della configurazione del nostro problema possiamo notare come nella soluzione, ottima con valore della (f.o.) pari a 82404, siano stati distribuiti gli interventi e attivate le facility. Anche in questo caso vengono attivati soltanto due nodi facility, come si può dedurre dal valore della Y (Alì Terme e Ganzirri), che mettono a disposizione il personale per far fronte ai diversi eventi (incendi e alluvione); il vettore delle X ci dice quale sono gli archi attivati, cioè come e da chi vengono servite le destinazioni. Può essere interessante, analizzare il peso delle diverse componenti della funzione obiettivo:

Z=8240 $\rightarrow$ (*valore all'ottimo della funzione obiettivo*);

Z1=42404 $\rightarrow$ (*componente legata alle scelte di servizio*);

Z2=40000 $\rightarrow$ (*componente legata ai costi fissi di attivazione*);

Notiamo come i costi siano dello stesso ordine di grandezza, in pratica similari, e che i costi di attivazione incidono in maniera preponderante sulla scelta delle logiche di servizio. Possiamo anche, al fine di comprendere al meglio la soluzione e il modello stesso, provare a tralasciare i costi fissi, per comprendere come variano le scelte di attivazione delle facility (location) ed archi (allocation).

Balza subito agli occhi un importante decremento del alore della funzione obiettivo, oltre al fatto che, non essendoci più i costi di attivazione (che avevamo detto essere importanti e pesanti) il vettore Y ci mostra che vengono attivate tutte le facility. L'attivazione di tutte le facility era attesa perché a questo punto si deve soltanto ottimizzare il costo di servizio delle diverse destinazioni, che verrà fatto in base alla distanza (visto che i costi sono espressi per €/km). Continuiamo come detto con un'ulteriore complicazione del modello introducendo altri scenari e fattori.

5.3 Implementazione ed esempio del modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-VERSIONE 2)

Il modello di riferimento è quello che abbiamo descritto con il nome CFLP-VERSIONE 2.

Per far comprendere al meglio il problema e la sua trasposizione in linguaggio matematico, seguono alcune considerazioni e supposizioni importanti che ci rendono più facile comprendere il problema e in particolare che lo differenziano dalle precedenti versioni:

- Per determinare i costi che abbiamo nel nostro caso, abbiamo analizzato il problema secondo quanto dichiarato nel modello tenendo in considerazione le distanze tra la facility (i) e il nodo destinazione (j). Valgono le considerazioni già fatte nel caso precedente sulle vie da utilizzare in relazione all'evento/catastrofe che si presenta; in aggiunta in questo caso abbiamo differenziato i costi tenendo presente anche che esiste diverso personale specializzato che ha un costo differente (oltre a definire delle peculiarità/competenze specifiche). Abbiamo ipotizzato dei costi differenti per i diversi gruppi di personale specializzato quantificando in 50 €il costo dei Vigili del Fuoco (VdF) e in 40 €il costo d'intervento della Protezione Civile (DPC)
- Come importante caratterizzazione di questo modello abbiamo elencato il personale presente nelle diverse facility esplicitandolo per competenze/corpo di appartenenza
- Introduciamo un fattore di penalità w che entra in gioco nel momento in cui non si soddisfa di un'unità di personale k la richiesta per l'evento l (nel sito j) e ci peggiora economicamente la situazione;
- Inoltre esplicitiamo i valori delle domande d[Demand] dei nodi destinazione e di b[Demand] che è un ulteriore parametro (intero) utilizzato per indicare il numero minimo di personale specializziamo che imponiamo essere necessario per affrontare la catastrofe. E' importante notare che l'introduzione di tale fattore b serve a prevenire una problematica che potrebbe portare a sostituire interamente una risorsa specializzata con un'altra non specializzata. Poniamo ad esempio il caso in cui, secondo una tabella di equivalenza imponiamo che 10 infermieri valgono come un vigile del fuoco, il nostro sistema potrebbe prevederne l'utilizzo sostitutivo, ma la realtà ci dice che questo non può essere possibile. Quindi la sostituzione è prevista solo in quota parte (parametro b) e accompagnata da penalizzazione (parametro w).

Da quanto riportato nel vettore delle soluzioni in appendice, vediamo l'utilizzo del diverso personale afferente alle facilities attivate, in relazione alla nostra funzione obiettivo.

Per comprendere meglio la composizione della soluzione, possiamo analizzare i diversi fattori che influiscono su di essa:
Z=306074 $\rightarrow$ (*valore all'ottimo della funzione obiettivo*);
Z1=218774 $\rightarrow$ (*componente legata alle scelte di servizio*);
Z2=80000 $\rightarrow$ (*componente legata ai costi fissi di attivazione*);
Z3=7300 $\rightarrow$ (*componente che quantifica la penalità*);

Come possiamo notare dalle soluzioni e dai diversi fattori che la compongono, la penalità per le situazioni non correttamente servite (Z3) è bassa nonostante i fattori moltiplicativi w siano molto alti; questo significa che per come è posto il problema, le facilities e il loro dimensionamento, sono adeguate e possiamo fronteggiare gli eventi che si presentano diminuendo il più possibile i casi di disservizio.

6 Considerazioni e conclusioni

Il presente articolo ha mostrato alcune possibili modellazioni legate alla problematica della logistica di emergenza. In particolare si è trattato il caso di studiare l'ottimizzazione di decisioni strategiche legate alla localizzazione di centri operativi per il soccorso in situazioni di emergenza e della allocazione di tali centri a bacini di utenza. Il lavoro ha previsto la costruzione di modelli derivati dai classici facility location problem in cui sono state inserite considerazioni relative all'utilizzo di multi risorse, la codifica di eventi di rischio, l'utilizzo alternativo tra risorse. Il lavoro ha inoltre previsto la definizione di una architettura informatica che possa supportare i processi decisionali legati alla logistica di emergenza. Infine sono state svolte delle sperimentazioni che hanno permesso di verificare la validità dei modelli in situazioni realistiche. Come estensione futura del lavoro si prevede di aumentare le dimensioni dei tests, di considerare in modo più specifico alcune tipologie di rischi, di implementare la piattaforma sull'architettura descritta, in linea con gli sviluppi del progetto SIGMA di cui questo lavoro rappresenta un contributo.

7 Appendice

(codice dei file .mod e .dat e le soluzioni di CPLEX)

7.1 Modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-LETTERATURA)

Segue il file relativo al modello in considerazione:

```
#######    INIZIO FILE .mod   #######
/*********************************************
* OPL 12.5 Model
*********************************************/
// dichiarazioni variabili e insiemi//
{string} S = ...;
{string} D = ...;
int q [S] = ...;
int d [D] = ...;
float c [S][D] = ...;
int f [S] = ...;
dvar boolean y [S];
dvar int+ x [S][D];
//dichiarazioni termini funzione obiettivo//
dexpr float Z1 = sum (i in S, j in D) c[i][j] * x[i][j];
dexpr int Z2 = sum (i in S) f [i] * y[i];
dexpr float Z = Z1 + Z2;
// funzione obiettivo //
minimize Z;
//dichiarazione dei vincoli//
subject to {
//vincolo (1)//
forall (j in D)
v_1: sum (i in S) x[i][j]>=1;
//vincolo (2)//
forall (i in S)
v_2:  sum (j in D) d[j] * x[i][j] <= q[i] * y[i];
// fine// }
#######    FINE FILE .mod   #######
```

Segue il file dei dati:

```
#######    INIZIO FILE .dat   #######
/*********************************************
* OPL 12.5 Data
*********************************************/
//Destinazioni//
D = {"Alì", "Altolia", "Itala", "Bordonaro", "Faro
Superiore", "Galati Superiore", "Giampilieri", "Messina",
"Rizzotti", "Scaletta Superiori"};
//Facility//
S = {"Alì Terme", "Galati Marina", "Ganzirri",
"Roccalumera", "Tremestri"};
//capacità facility//
q = [100, 100, 100, 100, 100];
//domanda destinazioni//
d = [1, 1, 1, 1, 1, 1, 1, 1, 1, 1];
// inizializzazione matrice costi (i,j) --> servire j da i//
c = #["Alì Terme": [280, 580, 992, 1484, 600, 428, 296,
1172, 1216, 340],"Galati Marina": [700, 424, 452, 964,
116, 272, 452, 512, 696, 392],"Ganzirri": [1660, 1384,
588, 144, 1076, 1232, 1412, 376, 324, 1352],
"Roccalumera": [484, 784, 1196, 1720, 804, 628, 500,
1268, 1416, 544], "Tremestri": [948, 676, 252, 764, 304,
460, 704, 312, 496, 576] ]#;
f = [2800, 4000, 1200, 2200, 4800];
#######    FINE FILE .dat   #######
```

Di seguito le soluzioni restituite dal solver CPLEX:

```
#######    INIZIO SOLUTIONS   #######
// solution (optimal) with objective 7956
// Quality Incumbent solution:
// MILP objective          7.9560000000e+003
// MILP solution norm |x| (Total, Max)
1.20000e+001 1.00000e+000
// MILP solution error (Ax=b) (Total, Max)
0.00000e+000 0.00000e+000
// MILP x bound error (Total, Max)       6.66134e-016
6.66134e-016
// MILP x integrality error (Total, Max)  3.33067e-015
6.66134e-016
// MILP slack bound error (Total, Max)
0.00000e+000 0.00000e+000
x = [[1 1 0 0 1 1 1 0 0 1]
[0 0 0 0 0 0 0 0 0 0]
[0 0 1 1 0 0 0 1 1 0]
[0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0]];
y = [1 0 1 0 0];
#######    FINE SOLUTIONS   #######
```

7.2 Modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-VERSIONE 1)

Segue il file relativo al modello in considerazione:

```
#######    INIZIO FILE .mod   #######
/*********************************************
* OPL 12.5 Model
*********************************************/
// dichiarazioni variabili e insiemi//
{string} S = ...;
{string} D = ...;
{string} L = ...;
int q [S] = ...;
int d [D][L] = ...;
tuple scenario {
string i;
string j;
string l; }
{scenario} Scenario = {<i,j,l> | i in S, j in D, l in L};
float c[Scenario] = ...;
int f [S] = ...;
dvar boolean y [S];
dvar int+ x [Scenario];
//dichiarazioni termini f.o.//
dexpr float Z1 = sum (<i,j,l> in Scenario) c[<i,j,l>] *
x[<i,j,l>];
dexpr int Z2 = sum (i in S) f [i] * y[i];
dexpr float Z = Z1 + Z2;
//f.o.//
minimize Z;
//dichiarazione dei vincoli//
subject to {
//vincolo (1)//
forall (j in D, l in L)
v_1:   sum (i in S) x[<i,j,l>] == d[j][l];
//vincolo (2)//
forall (i in S, l in L)
```

```
v_2:   sum (j in D) x[<i,j,l>] <= q[i] * y[i];
//vincolo (3)//
forall (<i,j,l> in Scenario)
v_3:   x[<i,j,l>] >= 0;
}
#######    FINE FILE .mod   #######
```

Segue il file dei dati:

```
#######    INIZIO FILE .dat   #######
/*********************************************
* OPL 12.5 Data
*********************************************/
//Facility//
S = {"Alì Terme", "Galati Marina", "Ganzirri",
"Roccalumera", "Tremestieri"};
//Destinazioni//
D = {"Alì", "Altolia", "Itala", "Bordonaro", "Faro
Superiore", "Galati Superiore", "Giampilieri", "Messina",
"Rizzotti", "Scaletta Superiore"};
//Eventi o catastrofi//
L = {"Incendio", "Alluvione"};
//Capacità facility//
q = [100, 100, 100, 100, 100];
//Domanda destinazioni per evento//
//per la destinazione j per ogni evento esplicito le
richieste//
d = #["Alì":[3,5], "Altolia":[3,7], "Itala":[4,2],
"Bordonaro":[5,8], "Faro Superiore":[9,2],
"Galati Superiore":[4,6], "Giampilieri":[2,8],
"Messina":[10,10], "Rizzotti":[3,5], "Scaletta Superiore":
[4,6]]#;
//Vettore dei costi per arco i,j ed eventi l//
c=[280,280,580,580,992,1400,1484,2024,600,600,428,428,
296,296,1172,1580,1216,1756,340,340,700,776,424,424,452,
472,964,1096,116,116,272,272,452,452,512,652,696,828,392,
392,1660,2240,1384,1480,588,704,144,204,1076,1196,1232,
1372,1412,1800,376,408,324,440,1352,1600,484,608,784,880,
1196,1340,1720,1820,804,1096,628,760,500,628,1268,1376,
1416,1552,544,636,948,1532,676,676,252,316,764,940,304,
304,460,460,704,704,312,356,496,668,576,576];
f = [28000, 40000, 12000, 22000, 48000];
#######    FINE FILE .dat   #######
```

Di seguito le soluzioni restituite dal solver CPLEX:

```
#######    INIZIO SOLUTIONS   #######
// solution (optimal) with objective 82404
// Quality Incumbent solution:
// MILP objective                  8.2404000000e+004
// MILP solution norm |x| (Total, Max)
1.08000e+002 1.00000e+001
// MILP solution error (Ax=b) (Total, Max)
0.00000e+000 0.00000e+000
// MILP x bound error (Total, Max)
0.00000e+000 0.00000e+000
// MILP x integrality error (Total, Max)
1.77636e-015 1.77636e-015
// MILP slack bound error (Total, Max)
1.77636e-015 1.77636e-015
x = [3 5 3 7 0 0 0 0 9 2 4 6 2 8 0 0 0 0 4 6 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4 2 5 8 0 0 0 0
0 0 10 10 3 5 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
y = [1 0 1 0 0];
#######    FINE SOLUTIONS   #######
```

Soluzioni relative allo scenario che tralascia i costi fissi di attivazione (f) delle facilities:

```
#######    INIZIO SOLUTIONS   #######
// solution (optimal) with objective 30680
// Quality Incumbent solution:
// MILP objective
3.0680000000e+004
// MILP solution norm |x| (Total, Max)
1.11000e+002 1.00000e+001
// MILP solution error (Ax=b) (Total, Max)
0.00000e+000 0.00000e+000
// MILP x bound error (Total, Max)
0.00000e+000 0.00000e+000
// MILP x integrality error (Total, Max)
0.00000e+000 0.00000e+000
// MILP slack bound error (Total, Max)
0.00000e+000 0.00000e+000
x = [3 5 0 0 0 0 0 0 0 0 0 0 2 8 0 0 0 0 4 6 0 0 3 7 0 0 0
0 9 2 4 6 0 0  0 0 0 0 0 0 0 0 0 0 0 0 5 8 0 0 0 0 0 0 0 0
3 5 0 0 0 0 0 0 0 0 0  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4
2 0 0 0 0 0 0 0 0 10 10 0 0 0 0];
y = [1 1 1 1 1];
#######    FINE SOLUTIONS   #######
```

7.3 Modello di localizzazione discreta, singolo prodotto, singolo livello, capacità finita (CFLP-VERSIONE 2)

Segue il file relativo al modello in considerazione:

```
#######    INIZIO FILE .mod   #######
/*********************************************
* OPL 12.5 Model
*********************************************/
// dichiarazioni variabili e insiemi//
{string} S = ...;
{string} D = ...;
{string} L = ...;
{string} K = ...;
int q [S][K] = ...;
tuple scenario {
string i;
string j;
string l;
string k; }
tuple demand {
string j;
string l;
string k; }
tuple penalty {
string l;
string k;}
{scenario} Scenario = {<i,j,l,k> | i in S, j in D, l in L,
k in K};
{penalty} Penalty = {<l,k> | l in L, k in K};
{demand} Demand = {<j,l,k> | j in D, l in L, k in K};
int b[Demand]= ...;
int d[Demand]= ...;
float w[Penalty]= ...;
float c[Scenario] = ...;
int f [S] = ...;
dvar boolean y [S];
dvar int+ x [Scenario];
//dichiarazioni termini f.o.//
```

```
dexpr float Z1 = sum (<i,j,l,k> in Scenario) c[<i,j,l,k>] *
x[<i,j,l,k>];
dexpr int Z2 = sum (i in S) f[i] * y[i];
dexpr float Z3 = sum (j in D, <l,k> in Penalty) w[<l,k>] *
(d[<j,l,k>] - sum (i in S) x[<i,j,l,k>]);
dexpr float Z = Z1 + Z2 - Z3;
//f.o.//
minimize Z;
//dichiarazione dei vincoli//
subject to {
//vincolo (1)//
forall (i in S, l in L, k in K)
v_1: sum (j in D) x[<i,j,l,k>] <= q[i][k] * y[i];
//vincolo (2)//
forall (<i,j,l,k> in Scenario)
v_2:  x[<i,j,l,k>] >= 0;
//vincolo (3)//
forall (j in D, l in L, k in K)
v_3:  sum (i in S) x[<i,j,l,k>] >= b[<j,l,k>];
}
#######    FINE FILE .mod   #######
```

Segue il file dei dati:

```
#######    INIZIO FILE .dat   #######
/*********************************************
* OPL 12.5 Data
*********************************************/
//Facility//
S = {"Alì Terme", "Galati Marina", "Ganzirri",
"Roccalumera", "Tremestieri"};
//Destinazioni//
D = {"Alì", "Altolia", "Itala", "Bordonaro", "Faro
Superiore", "Galati Superiore", "Giampilieri", "Messina",
"Rizzotti", "Scaletta Superiore"};
//Eventi o catastrofi//
L = {"Incendio", "Alluvione"};
//Personale Specializzato//
K = {"VdF", "DPC"};
//Capacità facility per personale specializzato//
q = #["Alì Terme": [75,100], "Galati Marina": [100,150],
"Ganzirri": [100,100], "Roccalumera": [75,50],
"Tremestieri": [25,50]  ]#;
/Vettore C[Scenario] //
c=[350,280,350,280,725,580,725,580,1240,992,1750,1400,
1855,1484,2530,2024,750,600,750,600,535,428,535,428,370,
296,370,296,1465,1172,1975,1580,1520,1216,2195,1756,425,
340,425,340,875,700,970,776,530,424,530,424,565,452,590,
472,1205,964,1370,1096,145,116,145,116,340,272,340,272,
565,452,565,452,640,512,815,652,870,696,1035,828,490,392,
490,392,2075,1660,2800,2240,1730,1384,1850,1480,735,588,
880,704,180,144,255,204,1345,1076,1495,1196,1540,1232,
1715,1372,1765,1412,2250,1800,470,376,510,408,405,324,
550,440,1690,1352,2000,1600,605,484,760,608,980,784,1100,
880,1495,1196,1675,1340,2150,1720,2275,1820,1005,804,1370,
1096,785,628,950,760,625,500,785,628,1585,1268,1720,1376,
1770,1416,1940,1552,680,544,795,636,1185,948,1915,1532,845,
676,845,676,315,252,395,316,955,764,1175,940,380,304,380,
304,575,460,575,460,880,704,880,704,390,312,445,356,620,496,
835,668,720,576,720,576
//Vettore b [Demand] //
b=[5,7,13,21,8,15,6,9,10,25,31,4,7,3,13,18,7,12,14,23,21,17,
15,20,19,17,16,15,7,24,11,13,16,19,9,11,13,14,17,19];
//Domanda destinazioni per evento per la destinazione j
per ogni evento esplicito le richieste/Vettore d [Demand] //
d=[14,12,17,30,12,16,10,10,10,26,31,9,9,9,15,20,9,15,15,25,
25,20,16,21,21,20,25,20,16,27,15,14,19,22,13,14,18,17,21,25];
//Vettore w [Penalty]//
w = [ 100,800,100,500];
//Vettore costi fissi f //
f = [28000, 40000, 12000, 22000, 48000];
#######    FINE FILE .dat   #######
```

Di seguito le soluzioni restituite dal solver CPLEX:

```
#######    INIZIO SOLUTIONS   #######
/ // solution (optimal) with objective 306074
// Quality Incumbent solution:
// MILP objective                3.0607400000e+005
// MILP solution norm |x| (Total, Max)
2.74933e+005 2.74300e+005
// MILP solution error (Ax=b) (Total, Max)
0.00000e+000 0.00000e+000
// MILP x bound error (Total, Max)
0.00000e+000 0.00000e+000
// MILP x integrality error (Total, Max)
3.75255e-014 3.55271e-014
// MILP slack bound error (Total, Max)
3.55271e-014 3.55271e-014
x = [5 12 13 30 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 19
20 16 20 0 0 0 0 0 0 0 0 13 17 17 25 0 0 0 0 8 16 6 10 10
26 31 9 0 0 0 0 7 15 14 25 21 20 15 21 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 7 9 13 20 0 0 0 0 0
0 0 0 0 0 0 0 7 27 11 14 16 22 9 14 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
y = [1 1 1 0 0];
#######    FINE SOLUTIONS   #######
```

8 Glossario

- **CFLP** Capacitated Facility Location Problem
- **CPLEX** Solver scritto in C che prende il nome del simplesso. Risolve problemi di programmazione lineare intera, problemi di programmazione lineare e problemi di programmazione mista
- **DSS** Decision Support System
- **OPL** Optimization Programming Language (Linguaggio proprietario ILOG / IBM)
- **MILP** - Mixed Integer Linear Programming
- **SIGMA** Sistema Integrato di sensori In ambiente cloud per la Gestione Multirischio Avanzata
- **SITR** Sistema Informativo Territoriale Regionale
- **UFLP** Uncapacitated Facility Location Problem

Riferimenti

1 J.-B. Sheu, Challenges of emergency logistics management, Transportation Research Part E: Logistics and Transportation Review 43 (6) (2007) 655 – 659. doi:https://doi.org/10.1016/j.tre.2007.01.001.

2 D. Menerba, «Ingegneria - Università di Brescia», 2010. Online.

3 IBM ILOG CPLEX Optimization Studio [online] (http://www-03.ibm.com/software/products/it/it/ibmilogcpleoptistud/).

4 Gurobi [online] (http://www.gurobi.com/).

5 F. Filippi, Pianificazione e gestione dell'emergenza, La Sapienza, Roma, 2002.

6 Regione Sicilia, Sistema Informativo Territoriale Regionale (S.I.T.R.), [Online]. (http://www.sitr.regione.sicilia.it.).