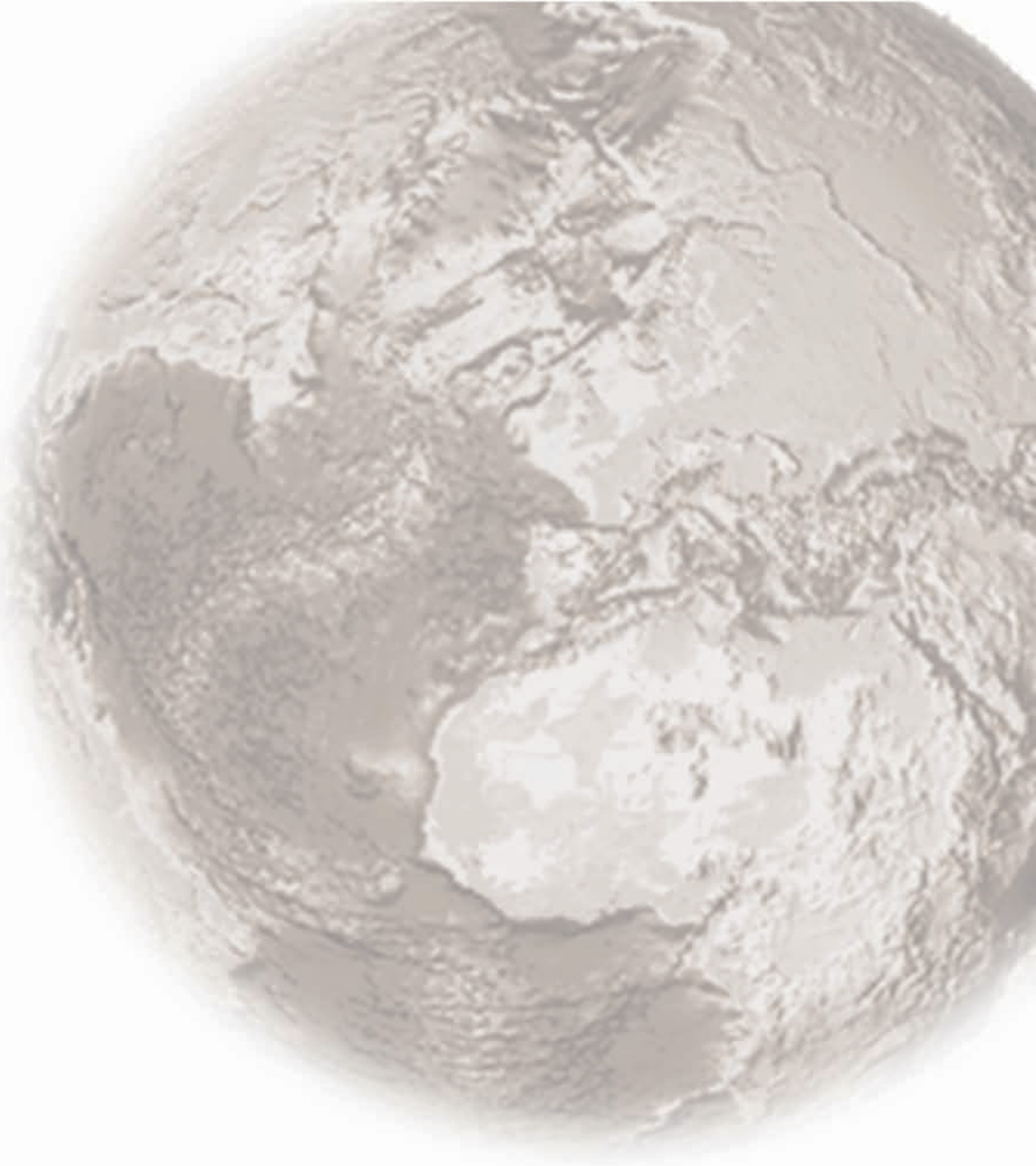
Rapporti Tecnici INGV



2008

Rete sismologica basata su stazioni GAIA

Leonardo Salvaterra,
Stefano Pintore e Lucio Badiali

n. 68

Istituto Nazionale di Geofisica e Vulcanologia
Via di Vigna Murata 605 - 00143 Roma
tel 06518601 • fax 065041181
www.ingv.it

Direttore
Enzo Boschi

Editorial Board
Raffaele Azzaro (CT)
Sara Barsotti (PI)
Mario Castellano (NA)
Viviana Castelli (BO)
Anna Grazia Chiodetti (AC)
Rosa Anna Corsaro (CT)
Luigi Cucci (RM1)
Mauro Di Vito (NA)
Marcello Liotta (PA)
Lucia Margheriti (CNT)
Simona Masina (BO)
Nicola Pagliuca (RM1)
Salvatore Stramondo (CNT)
Andrea Tertulliani - coordinatore (RM1)
Aldo Winkler (RM2)
Gaetano Zonno (MI)

Segreteria di Redazione
Francesca Di Stefano (coordinatore)
Tel. +39 06 51860068
Fax +39 06 36915617
Rossella Celi
Tel. +39 06 51860055
Fax +39 06 36915617
redazionecen@ingv.it

RETE SISMOLOGICA BASATA SU STAZIONI GAIA

Leonardo Salvaterra, Stefano Pintore e Lucio Badiali

Istituto Nazionale di Geofisica e Vulcanologia, Sezione CNT

Introduzione

Lo sviluppo della rete sismometrica nazionale digitale per mezzo degli acquisitori progettati nei laboratori dell'Istituto Nazionale di Geofisica, parte a febbraio 1998 con il primo test di collegamento numerico (CDN) della stazione MNS (Montasola). Il tutto era composto da un modulo acquisitore AGDF1, un modulo GPS1 di sincronizzazione tramite il segnale del tempo del sistema GPS e un modulo alimentatore ALIM1. La stazione trasmetteva in modo asincrono con baud rate 19200 e 10 bit tramite un modem digitale DCE-3. Aumentarono i collegamenti, ma ben presto i numerosi problemi causati dai disturbi sulle linee che inficiavano i dati non dotati di correzione di errore portarono a ripensare al protocollo di comunicazione.

L'evoluzione naturale fu quella di adottare un collegamento con protocollo TCP-IP, per il quale si pensò all'infrastruttura RUPA (Rete Unitaria delle Pubbliche Amministrazioni) alla quale si sono aggiunti, in seguito, dei collegamenti tramite vettore satellitare e su internet. In contemporanea nasce il progetto GAIA (Geophisical All Inclusive Aquisitor) che previde lo sviluppo di un ulteriore modulo da affiancare agli esistenti, denominato Transmission Node 1 (TN-1 – 2002), che si occupasse della connessione. Il passaggio a RUPA, dopo un anno di test, si è reso pressoché indispensabile vista la quasi totale assenza di errori (garanzia data anche dal protocollo TCP-IP) e dato il costo inferiore del collegamento rispetto ai CDN. L'installazione delle stazioni sulla rete RUPA è iniziata nel 2003 sempre con la stazione di Montasola (RI), su internet e satellite a fine 2006.

Alla data di pubblicazione è già pronta e funzionante la nuova stazione digitale denominata GAIA2 che aggiunge ulteriori funzionalità (come l'adozione del SNMP per i setup, ecc.), ma non è compito di questa stesura entrare nei suoi dettagli.

La rete Nazionale basata su GAIA vede attualmente (Maggio 2008) installate circa 60 stazioni, sparse in tutta Italia (vedi appendice A) e ben presto ne saranno installate altre per migliorare la copertura.

In questo documento verranno seguite le seguenti convenzioni tipografiche:

- *corsivo* per i nomi di programmi
- **grassetto** per la specifica di linee di comando
- Font Arial per file di configurazione di programmi.

1. La Rete Unitaria delle Pubbliche Amministrazioni

Nel 1995 l'AIPA portò a termine lo studio di fattibilità in merito alla realizzazione della rete RUPA. RUPA doveva diventare l'unico strumento di telecomunicazioni utilizzato dalla Pubblica Amministrazione per operare all'interno dello stesso dominio interamministrazione e per accedere a servizi di interoperabilità tra domini. P.A.thNet (TELECOM) si aggiudicò nel 1997 la gara per la realizzazione della rete di trasporto. EDS vinse invece la gara per la realizzazione dei servizi interdominio. In RUPA ogni Amministrazione costituisce un Dominio. L'Amministrazione gestisce il proprio dominio tramite un proprio centro di gestione dell'amministrazione: CG-Amm. Le connessioni fra Domini sono gestite dal Fornitore dei servizi per l'interoperabilità (CGI). La Rupa è costituita da diverse infrastrutture, una condivisa per i servizi CTN (usa i CDN), una dedicata per fornire i servizi IP permanente, Frame Relay e X.25 e una mista per il servizio IP commutato. Oltre a queste è dotata di due sistemi gestionali: Il Centro di Gestione dell'Interoperabilità (CGI) e il Centro di Gestione del Trasporto (CGT).

1.1. L'hardware di RUPA

La rete è costituita essenzialmente da due livelli: Il livello 1 costituisce la dorsale interregionale, il livello 2 costituisce la rete di raccolta del traffico regionale verso il livello 1. La dorsale interregionale è costituita da nodi Magellan Passport di Nortel, connessi con flussi da 2 a 34 Mbit/s. In particolare l'anello di Roma è costituito da 6 nodi connessi a 34 Mbit/s. I collegamenti tra nodi sono realizzati in fibra ottica.

1.2. L'interfaccia tra INGV e RUPA

Il servizio RUPA che noi utilizziamo è quello di IP permanente, dal nostro punto di vista possiamo pensare alla rete RUPA come a un'estensione della rete locale sul territorio nazionale. Presso le stazioni sismiche collegate esiste un router di accesso con un indirizzo IP assegnato, che instrada i pacchetti su una sottorete. Tale sottorete contiene generalmente una sola scheda GAIA. Il router è collegato alle infrastrutture P.A.thNet tramite un DCE (Data Communication Equipment), equivalente digitale del modem ed insieme costituiscono il Punto di Accesso al Servizio (PAS). La banda disponibile, in termini di velocità del collegamento, è pari a 32 Kbit/s garantiti. Il traffico può occasionalmente superare questa velocità, fino ad un massimo di 64 kbit/s, ma non è assicurata la consegna da parte della rete di trasporto di traffico eccedente la banda garantita. L'equivalente gestionale del nostro CED al quale fare riferimento per eventuali problemi è il CGT. Nella Sala macchine attigua alla Sala Sismica è presente il PAS della Sede INGV, costituito da 2 coppie di DCE e router per ridondanza. L'unica differenza con le sedi remote è logicamente nella disponibilità di banda superiore.

La stazione remota ha una piccola LAN (Local Area Netwok) che ha a disposizione 8 indirizzi IP (di questi quelli effettivamente utilizzabili dall'INGV sono 5): il primo è relativo alla rete, il secondo è per il router, l'ultimo è il broadcast.

Nella tabella 1 si vede la configurazione della stazione di Montasola:

Rete	10.136.0.0
Subnet Mask	255.255.255.248
Primo IP	10.136.0.1
Ultimo IP	10.136.0.6
Broadcast	10.136.0.7
Router remoto:	IP 10.136.0.1

Tabella 1: Configurazione interfaccia ethernet della stazione di Montasola.

La stazione tipo prevede una sola scheda TN-1 collegata al Router, per cui un unico indirizzo IP utilizzato; nel caso di più schede collegate (ad es. presenza di un apparato GPS) è necessario uno switch.

2. Satellite

Le altre tipologie adottate per il collegamento con le GAIA sono satellitari e Internet. Per la prima si è instaurato un rapporto commerciale con la società Base3 s.r.l. che fornisce collegamenti satellitari attraverso SATLink.

SATLink nasce come brand di Base3 s.r.l. (settore ITT) dedicato ai servizi satellitari in larga banda, configurandosi come punto di riferimento per strutture aziendali di varia natura.

La soluzione Satlink si basa su tecnologia iDirect. L'architettura di rete della soluzione proposta consta di tre principali componenti:

1. un equipaggiamento presso la sede remota;

2. il link satellitare;

3. l'Internet Data Center (IDC) con accesso diretto al backbone pubblico di internet, l'hub satellitare e il Network Operations Center (NOC).

2.1. Equipaggiamento della sede periferica

L'equipaggiamento localizzato presso la sede periferica (fig. 1) è composto di tre componenti principali:

1. Outdoor Unit (ODU), formato da antenna, staffe di montaggio, trasmettitore (BUC Block Up Converter), ricevitore (LNB Low Noise Block), guida d'onda, cavi;

2. Indoor Unit (IDU), comunemente denominato modem satellitare.

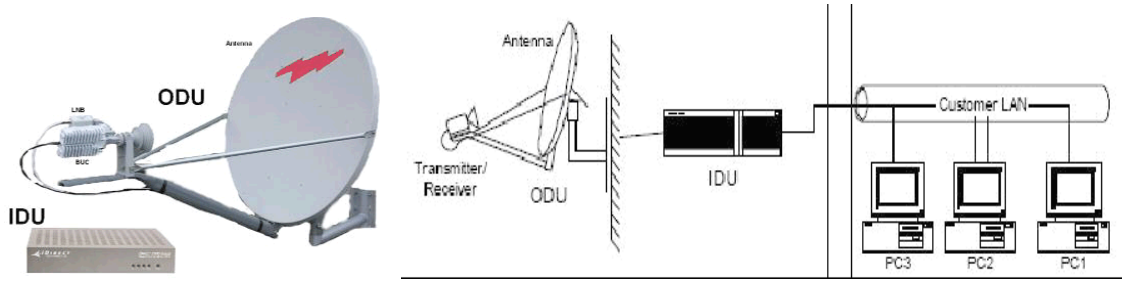


Figura 1: Equipaggiamento da installare presso la sede periferica e schema di installazione.

2.2. Satellite

Il servizio è offerto sul satellite HELLAS SAT 2. HELLAS SAT (www.hellas-sat.net) è una joint venture tra la Grecia e Cipro, ed è controllata da OTE (Hellenic Telecommunications Organization) che è il più importante operatore di telecomunicazioni del sud Europa.

Il satellite è dotato di 30 transponder in banda Ku distribuiti su due beam fissi posizionati sull'Europa e due steerable beams che possono essere puntati in qualunque direzione della porzione di Terra visibile. Il satellite è controllato attraverso due stazioni di monitoraggio e controllo (TT&C) localizzate in Grecia e Cipro rispettivamente, che assicurano un elevato livello della qualità dei segnali trasmessi.

In Tabella 2 le specifiche tecniche del satellite HELLAS SAT 2:

Satellite HELLAS SAT 2
Produttore ASTRIUM (75% EADS, European Aeronautic Defence and Space Company and 25% BAE SYSTEMS)
Frequenze downlink: 10.95-11.20 GHz, 11.45 -11.70 GHz 12.50-12.75 GHz
Banda dei transponders: 36 MHz
Massa 3250 kg
Potenza 7500 W
Ciclo di vita > 15 anni
Posizione orbitale Geostationary 39 ° E
N° transponder operativi 30

Tabella 2: Informazioni sul satellite Express-AM1.

Anche per il collegamento satellitare vale quanto detto per RUPA e, cioè, la stazione remota ha una piccola LAN, ma con 127 indirizzi IP disponibili. Nella tabella 3si vede la configurazione della stazione di Campotto Po (FE):

Rete	172.24.179.
Subnet Mask	255.255.255.128
Primo IP	172.24.179.1
Ultimo IP	172.24.179.126
Broadcast	172.24.176.127
Router remoto:	172.24.179.1

Tabella 3: Configurazione interfaccia ethernet della stazione di Campotto.

Presso la sede di Roma dell'INGV è installato un equipaggiamento completo, come per una stazione, chiaramente il flusso dati è principalmente in ricezione al contrario delle stazioni.

3. Internet

Per quanto riguarda la rete Internet è l'ormai enorme diffusione dell'infrastruttura con costi relativamente bassi e buona affidabilità, ad averne giustificato l'utilizzo per la trasmissione dei dati sismici in particolari circostanze. Chiaramente non è compito di questo testo fornirne una descrizione, l'unica indicazione riguarda l'utilizzo e le richieste per un collegamento per dati sismici in tempo "quasi reale": occupazione di banda non elevata, fondamentale necessità per la GAIA di un indirizzo IP statico. L'estrema diffusione di internet permette l'instaurarsi di convenzioni con vari soggetti (università, osservatori, scuole, comuni, ecc.) che in cambio dell'ospitalità vengono dotati di un apparato per la rilevazione sismica all'avanguardia senza costi aggiuntivi. Attualmente si hanno tre stazioni GAIA collegate tramite internet e ospitate presso l'università di Modena, il museo "Bendandi" di Faenza e l'osservatorio di Gibilmanna. Quest'ultimo, parte integrante dell'INGV, è stato il capostipite dei collegamenti internet e ha permesso di sviluppare il progetto ed effettuare i test. A breve verranno realizzati altri collegamenti con l'università di Parma e l'osservatorio astronomico di Monteporzio Catone (RM).

4. Point-to-Point Protocol

L'ultima tipologia di collegamento, di cui è dotata la GAIA, è quella che utilizza il protocollo PPP (TCP/IP su seriale). La configurazione di questo collegamento è simile alla precedente perché il protocollo è sempre TCP-IP anche se si passa su una linea seriale. Il collegamento PPP sulla porta seriale di un pc configurato opportunamente per questo protocollo, è simile al collegamento con il router del collegamento RUPA. L'interfaccia su cui lavora PPP necessita di un indirizzo IP, come una qualunque scheda di rete, sia lato TN sia lato PC. Quest'ultimo, per la TN, si comporta a tutti gli effetti come un router e sarà proprio il suo indirizzo IP-PPP ad essere utilizzato come gateway (vedi tabella 1 del funzionamento RUPA).

Il protocollo PPP (Point to Point Protocol) fornisce un metodo standard per il trasporto di diversi tipi di protocollo su una connessione punto a punto. Uno dei motivi per cui PPP è stato sviluppato è di facilitare il collegamento tra apparati di rete eterogenei (per ulteriori informazioni vedi Appendice B).

Attualmente è la sola stazione RDP, ubicata presso il Museo Geofisico di Rocca di Papa (RM) ad essere collegata tramite un collegamento che sfrutta il PPP. Tra la stazione e la sede di Roma dell'INGV c'è un ponte radio digitale a 9600 b/s con frequenza di 442.4 MHz e potenza in trasmissione pari a 200mW Nella sede INGV il ponte radio digitale è collegato tramite un collegamento seriale ad un server, NARA, che fa da router verso la rete interna. Tale server è un PowerEdge 1850 Xeon 2.8Ghz della DELL, con 1GB di RAM e hard disk SCSI da 72 GB in raid 1, sistema operativo Linux (distribuzione Big Box del CASPUR basata su Red Hat Enterprise).

Il file di configurazione del PPP su NARA è **/etc/ppp/options.** Nella stessa directory è presente lo script contenente la riga di comando per lanciare il demone *pppd*:

pppd 192.168.0.3: 192.168.0.1 /dev/ttyS3 9600

dove il primo indirizzo IP è quello del PC-router, il secondo è della TN.

5. Architettura software della TN-1

Il compito della scheda TN-1, all'interno del progetto GAIA, è stato ampliato in fasi successive fino ad assumere, nella sua configurazione finale, una struttura complessa.

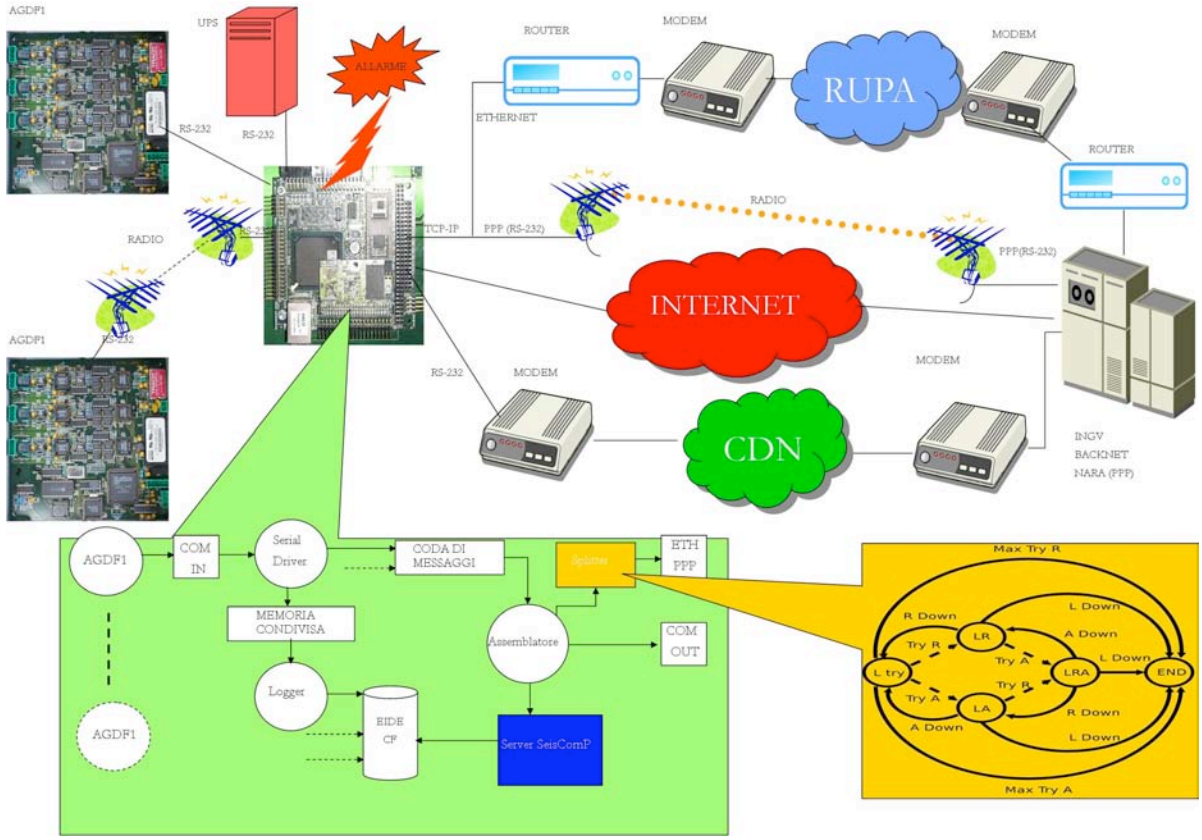


Figura 2: Schema di collegamento INGV – stazione remota con GAIA1 e architettura software.

La scheda TN-1 svolge attualmente i seguenti compiti (fig. 2):

1. raccoglie uno o più flussi di ingresso provenienti da schede AGDF attraverso collegamenti seriali (tramite cavo e/o ponte radio);
2. convoglia i flussi di input su: una linea seriale di uscita; un socket tcp remoto, dialogando con il sistema di acquisizione *SisMux*; un socket tcp remoto su seriale grazie all'uso del protocollo PPP;
3. gestisce l'aggiornamento della scheda AGDF tramite terminale seriale, anche remotamente attraverso la rete IP;
4. monitora i flussi di input per eventuali anomalie dovute ad errori nel collegamento con l'AGDF, che possono verificarsi ad esempio in presenza di collegamenti in ponte radio e corregge se possibile tali errori di trasmissione;
5. monitora i flussi di input per riconoscere i possibili problemi di perdita di sincronismo dovuti a irregolarità nel funzionamento del modulo GPS connesso alle schede AGDF;
6. monitora le informazioni provenienti dal sistema di alimentazione UPS;
7. invia al sistema di controllo messaggi di allarme di stato in base ai parametri monitorati;
8. se equipaggiata di scheda Compact-Flash (CF) opzionale, consente la memorizzazione locale dei dati sismici;

in più, essendo la scheda TN-1 a tutti gli effetti un PC dotato di sistema operativo Linux:

9. consente, tramite protocolli di comunicazione “sicuri”, la comunicazione con stazioni di controllo remote;
10. consente l'aggiornamento dei software applicativi da parte della stazione di controllo remota, senza necessità di intervento di personale tecnico alla stazione sismica;
11. consente l'aggiornamento dello stesso sistema operativo, se necessario anche dalla stazione di controllo remota.

Un’altra caratteristica del sistema un’improvvisa mancanza di alimentazione non causa problemi al sistema operativo perché dotato di un file system journaled che ripristina in automatico la configurazione originale. Inoltre al riavvio l’applicativo riparte in automatico. In ultimo, come già detto, vi è la possibilità dell’archiviazione dei pacchetti in arrivo delle varie AGDF nel formato del sistema di acquisizione dell’INGV e miniSeed essendo in funzione nella TN-1, un server Seedlink.

L’installazione della scheda TN-1 in stazione consiste, quindi, nel metterla in comunicazione con il server Sismux che gira nel computer Luna della sala sismica. A tal fine è stato sviluppato un programma apposito, *splitter*, che gestisce la comunicazione. In questo modo tutto ciò che riguarda i problemi di collegamento remoto ha causa o effetto all'interno del software *splitter*, senza effetti collaterali propagati ad altre funzionalità. Poiché il programma di comunicazione IP è stato concepito, quando il programma *backnet* (stessa architettura di *Sismux*) era già funzionante assieme al programma *frontnet* per i collegamenti seriali CDN, ci si è adattati alle sue specifiche di comunicazione. Queste prevedevano che *backnet* si comporti da server e che i client che vogliano comunicare dati sismici richiedano l’apertura di porte TCP sul server *backnet* stesso. Inoltre non si utilizza alcun protocollo di negoziazione della comunicazione a livello applicativo, quindi il server accetta connessioni e legge il contenuto inviatogli dal client, riservandosi un’analisi sintattica e semantica a livello di pacchetti WF. Seguendo tale schema di collegamento, il software *splitter* risulta lui responsabile di mantenere la comunicazione con il server *SisMux* riaprendo la connessione in caso di problemi alla stessa.

Il programma *splitter* prende in input fino a tre coppie IP-PORT, una di sorgente e due di destinazione. All'avvio apre un socket su un server sorgente e tenta di aprire e mantenere connessi altri due socket di destinazione. Prende i dati dal socket sorgente e li replica su entrambi i socket di destinazione. Le due destinazioni vengono trattate in modo simmetrico in caso di caduta della connessione. Quando una connessione remota cade, il software cerca di riaprirla, mentre continua a scrivere sull'altro socket. Se entrambe cadono cerca di riaprirle entrambe un numero limitato di volte. Se non riesce a stabilire almeno una connessione remota il programma si chiude. Lo stesso accade se cade la connessione locale [Pintore e Salvaterra, 2007].

6. Sistema d'acquisizione GAIA

Il sistema di acquisizione dei dati delle GAIA è composto di vari livelli (fig. 3). Il primo, identificato col computer Luna (fig. 4), è dotato del server *Sismux* configurato, a sua volta, in due livelli: vi è un *MasterMux*, cui tutte le stazioni si collegano, che spedisce i dati ricevuti ad una serie di *SlaveMux* (attualmente quattro: TokyoMux, KyotoMux, GeoMux e GibMux).

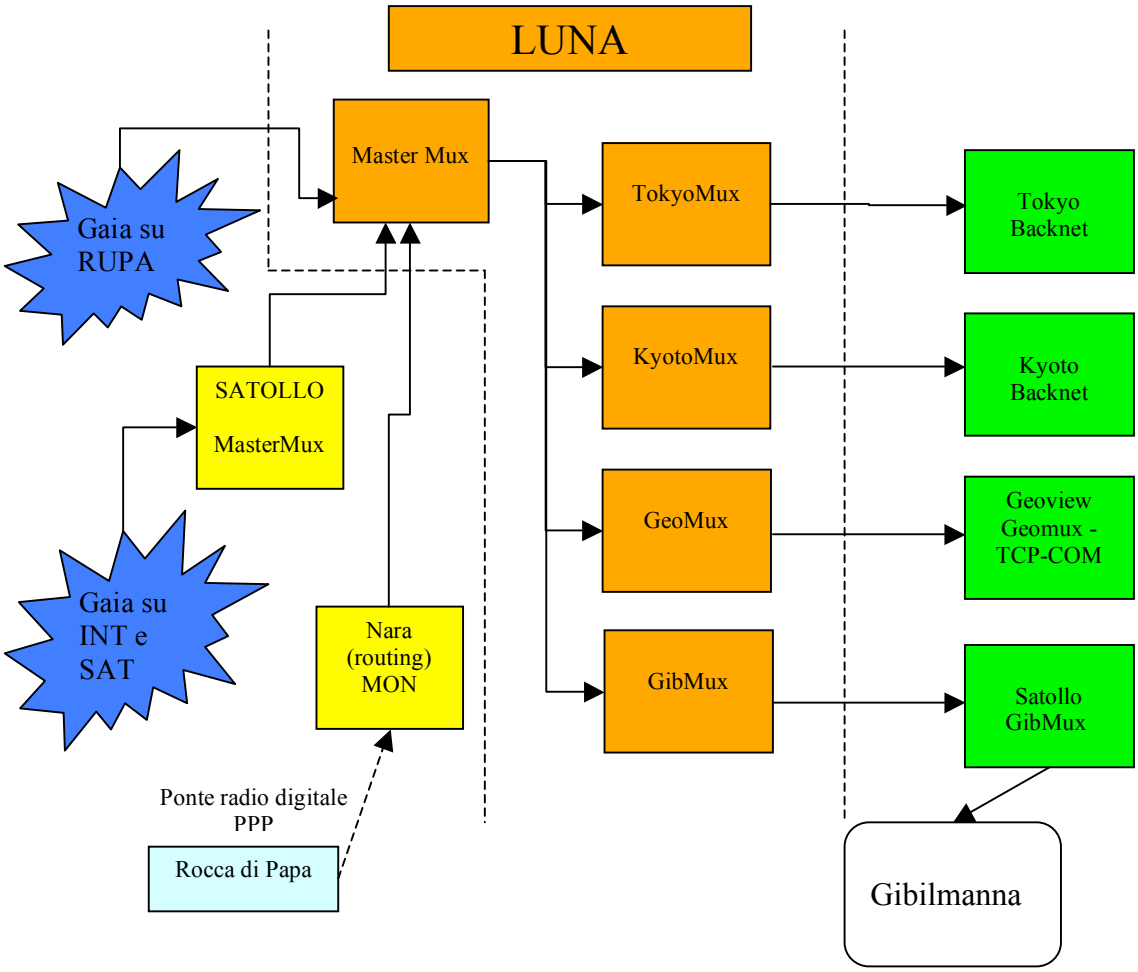


Figura 3: schema a blocchi del sistema di acquisizione.

MasterMux riceve dati dalle GAIA su RUPA e dai server Satollo e Nara. Gli slave spediscono, a loro volta, i dati ai computer Tokyo e Kyoto (2° secondo livello) con i server Backnet di acquisizione vera e propria, a GeoView per la visualizzazione e a Satollo per l'invio a Gibilmanna delle stazioni GAIA su RUPA siciliane. Si noti l'eccezione del collegamento PPP della stazione RDP descritto in precedenza.

Per quanto riguarda le GAIA che arrivano da Internet e Satellite, sul server preposto alla prima ricezione dei dati, Satollo (fig. 4), gira un *MasterMux* che "rimbalza" i dati a Luna. La presenza di questo server si è resa necessaria per ragioni di sicurezza, infatti Satollo è configurato in rete esterna verde, mentre Luna, oltre che in rete interna, sta in rete esterna blu e comunicano con queste reti attraverso un firewall e con l'indicazione di rotte statiche (fig. 5). Su Satollo gira anche *GibMux*, che ricevendo i dati da Luna delle stazioni siciliane, li "rimbalza" a Gibilmanna.

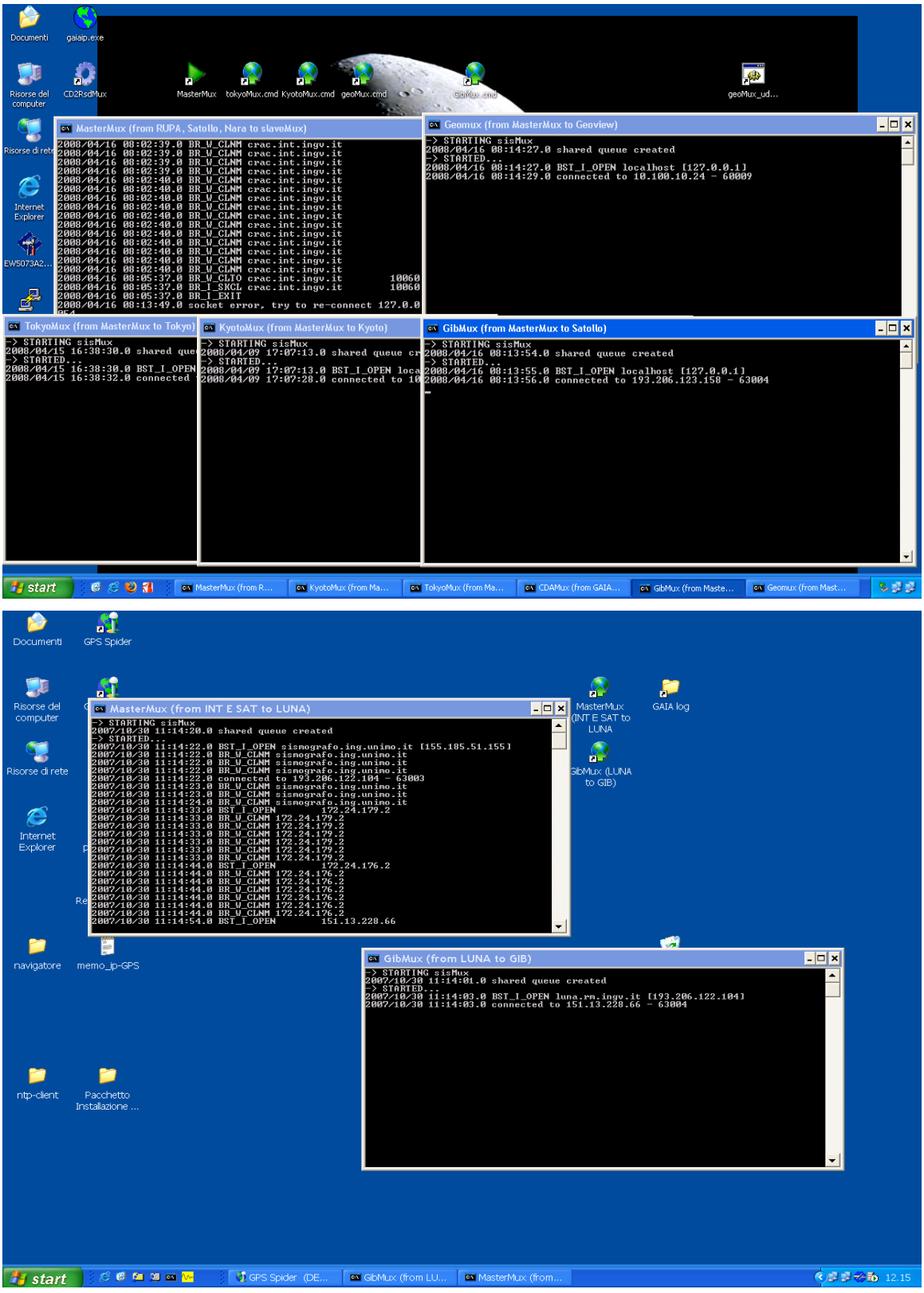


Figura 4: screenshot del desktop di LUNA (in alto) e Satollo (in basso) con i processi SisMux attivi.

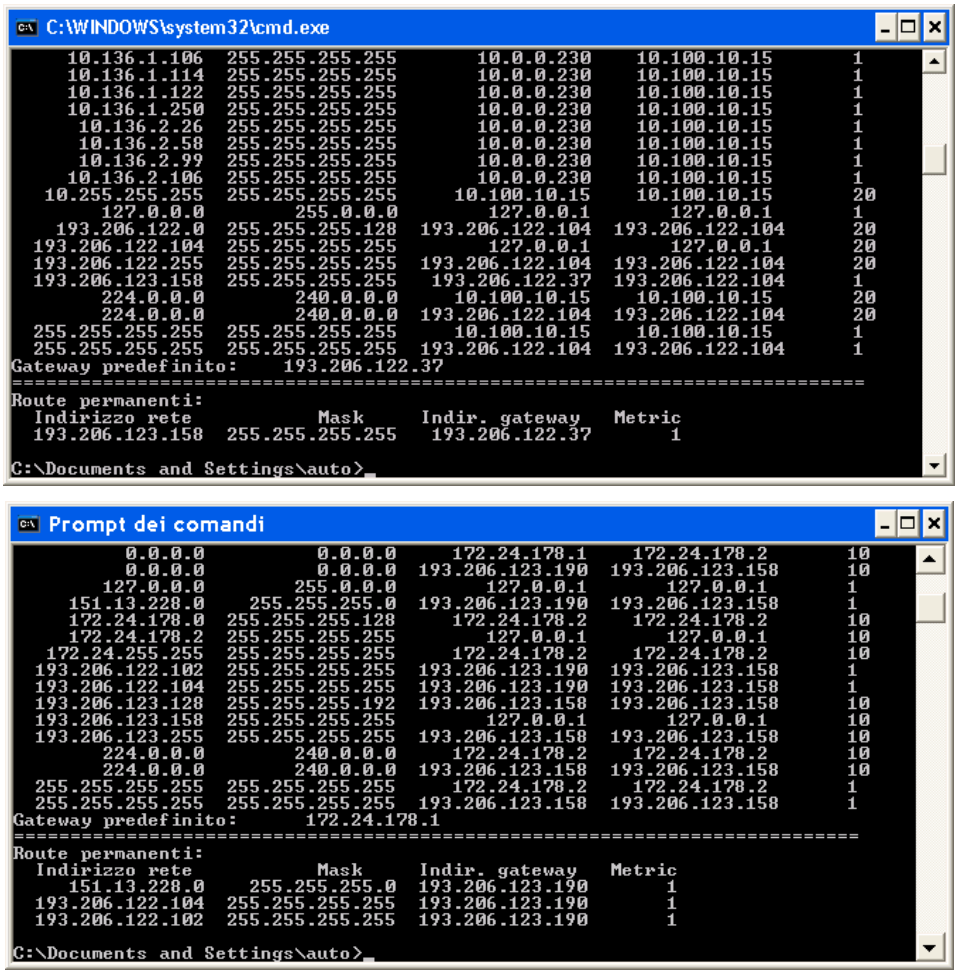


Figura 5: screenshot delle rotte statiche di LUNA (in alto) e Satollo (in basso).

Per la visualizzazione dei dati, su Geoview gira un *GeoMux* associato ad un programma, *TCP-COM*, che, creando delle porte seriali virtuali, consente l'utilizzo del software di analisi e visualizzazione dei dati sismici *GeoView*. Il protocollo di comunicazione è chiaramente TCP/IP per la sua affidabilità. C'è da notare, inoltre, che la parte di dati relativa ai segnali GPS presente nel pacchetto di dati viene spedita solo al computer GeoView e non a Tokyo e Kyoto.

6.1. Descrizione SisMux

Il programma applicativo *SisMux* ha come scopo di acquisire centralmente un flusso di pacchetti nativi Gaia e di ridistribuirli secondo una lista di indirizzi. I destinatari possono essere a loro volta dei *SisMux* o dei *backnet*.

Il programma è sviluppato in C++ ed è dotato di un insieme di classi sviluppate ad hoc.

Il *SisMux* usa la tecnica multithreading. Il programma genera le risorse comuni usate da tutti i vari moduli tra cui una coda condivisa, riconosciuta da un nome logico, ed i meccanismi di sincronizzazione. Un modulo si preoccupa di gestire le connessioni di rete ed acquisisce i dati che ripone nella coda condivisa. Esiste un modulo di spedizione per ogni indirizzo di destinazione.

Ognuno dei moduli preleva i dati dalla coda condivisa, accessibile in lettura e scrittura, e si occupa di spedire il dato sulla rete.

Tutti i moduli contenuti nel programma girano indipendentemente accodando l'operazione solo in caso di una collisione dovuta ad un evento di sincronizzazione, riprendendo subito dopo la collisione. Il *SisMux* può ricevere comandi in modo asincrono da console tra cui il fine programma o la rilettura forzata del file di stazioni, operazione questa che comunque esegue periodicamente.

Il sistema può essere passivo rispetto al nome di stazione e quindi far passare ogni pacchetto oppure filtrare sul nome decidendo se il pacchetto deve o non essere rispedito. Una versione specifica di *SisMux* può anche cambiare on the fly i nomi di stazione e canale se necessario.

Il modulo principale del *Sismux* ha un comportamento simile al seguente pseudo-codice:

```
init(configuration_files);
create_shared_queue();
async_receiver();
async_sender();
while(wait_for_event());
   process_event();
```

La sintassi del programma è la seguente:

sisMux.exe IP_PORT config_file

Il config_file riporta i parametri di connessione per la spedizione dei dati: IP e porta IP di destinazione, codec (spedizione o meno dei dati GPS), protocollo (TCP-IP o UDP), file di filtro dei dati.

es.

```
# Configuration file for SisMux:
# 1st row -> to bn_rupa
# 2nd row -> to geoview
# hints:
# ipAddr, ipPort, codec, protocol,filter file
#
#

# to local server
127.0.0.1,63004,1,tcp,c:\none #(senza filtro)

# to remote server
# 10.100.60.47,63004,1,tcp,c:\sisMux\rupa.txt

# to data viewer
10.100.10.24,62000,0,tcp,c:\sisMux\rupa.txt
```

Oltre il config_file sono presenti altri due file che condizionano il funzionamento di *SisMux*:

- Set.up che imposta i parametri per le code di memoria

```
# sisMux core information
# do not alter
# hints:
# code_name, element size, element number
#
```

SISMUX001, 1024, 10240

- Filter_file che filtra quali canali ricevuti devono essere inviati ai server e se devono essere rinominati.

```
# key file for SisMux
#
# hints:
# orig name, orig chann [; dest name, dest chann]
#
#
#

ARVD, EHZ
ARVD, EHN
ARVD, EHE
CDAGE, 1HZ ; FIN, SHZ
CDAGE, 2HZ ; IMI, SHZ
CDAGE, 3HZ ; ORX, SHZ
CDAGE, 4HZ ; PZZ, SHZ
```

6.2. Controllo e riavvio processi

Come si nota dalla struttura descritta, il sistema è modulare per cui in caso di problemi, per i quali è necessario il riavvio di uno o più processi, è sufficiente il riavvio di quelli bloccati. In particolare per chiudere i processi SisMux bisogna digitare nella finestra DOS relativa, la stringa "quit" e attenderne la chiusura, mentre per riavviarli è sufficiente fare doppio click sull'icona relativa posta sul desktop di Luna. Un unico inconveniente che "disturba" la modularità è TCP/COM del computer *GeoView*. Quest'ultimo programma sfrutta molto le risorse del computer, in particolare all'avvio, per cui è necessario, in caso di riavvio, che *GeoMux* (sia quello di Luna, sia quello locale) non stia funzionando, altrimenti si rischia il blocco del software. Per chiudere TCP/COM, bisogna fare click col tasto destro sull'icona che si trova nel system tray (fig. 6), selezionare "open TCP/COM" e chiudere la finestra che si apre, dal menù file o dal pulsante di chiusura delle finestre di Windows.

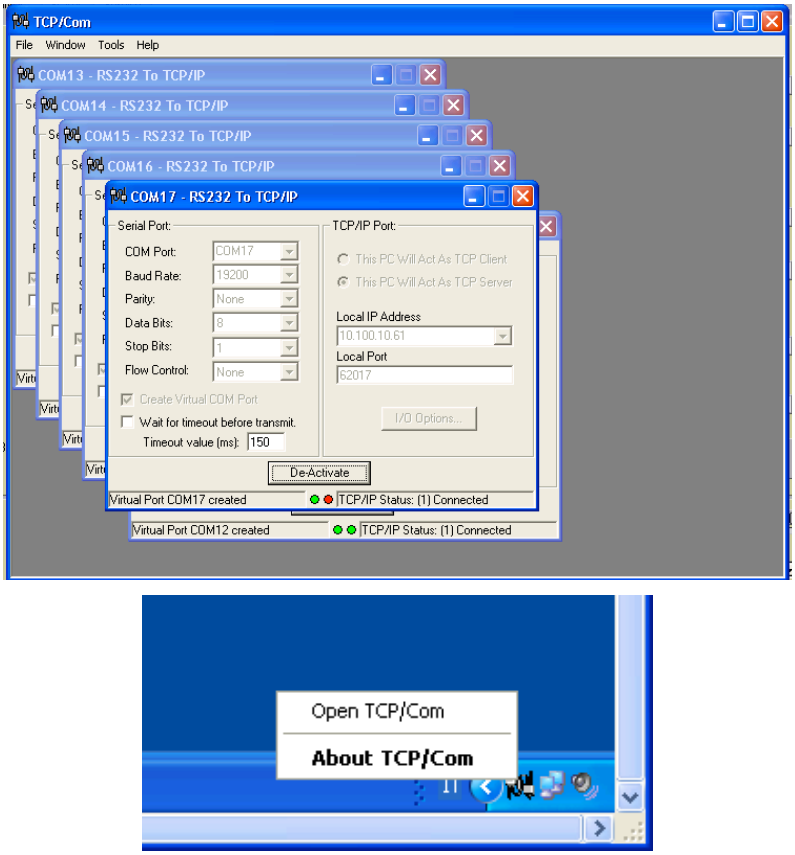


Figura 6: screenshot del programma TCP/COM.

7. Monitoraggio delle stazioni

Per controllare automaticamente lo stato dei collegamenti è stato modificato ed installato sul server NARA, un applicativo di monitoraggio open source, MON. Tale applicativo è raggiungibile da qualsiasi computer attraverso la sua interfaccia web (quindi basta un qualunque browser web). MON è un programma che consente di monitorare risorse connesse in rete IP. È costituito da un programma server a cui si può accedere tramite varie interfacce.

MON è stato sviluppato sotto Linux, ma funziona anche con Solaris 2.5 e 2.6. Sia il server sia i client sono scritti completamente nel linguaggio Perl il che ne garantisce la portabilità. Le modalità di monitoraggio sono due: sincrona ed asincrona. Con la prima, MON schedula l'avvio di processi detti monitor, indipendenti rispetto a MON, che svolgono il monitoraggio di vari servizi, ad esempio **ping** e **telnet**, mentre con la seconda, MON è in grado di ricevere delle trap via UDP (allarmi) inviate in modo asincrono dalle risorse monitorate.

In seguito alla risposta ricevuta dai monitor o alle varie trap ricevute, MON è in grado di inviare degli allarmi (Alert) sotto varie forme, anche in tempi diversi: e-mail agli amministratori di sistema, variazione dello stato nell'interfaccia WEB (fig. 7), finestre Winpop-up. Il servizio "Alert" si basa su script che spediscono dei messaggi in caso di errori riscontrati da MON. Tali alerts, come i monitor, non fanno parte del server, per cui è facile aggiungerne di nuovi. Esiste anche il servizio "Upalerts" che avvisa della fine dell'errore.

I vari test sono effettuati in parallelo su diversi host o gruppi di host, per esempio effettuare un ping verso router e verso server WWW contemporaneamente. Non esistono code di attesa nella schedulazione dei test. In caso di allarmi ripetitivi, questi possono essere soppressi, ad esempio spedire un'e-mail solo se il guasto dura più di ora, inoltre si può ignorare l'errore se esso dura poco.

É possibile far dipendere un test dall'esito di un altro. Per esempio, se un router prima di un server WWW è giù, il servizio HTTP chiaramente non funziona, ma è comodo avere solo l'allarme sul guasto del router. Questo servizio serve per prevenire l'invio di tantissimi allarmi causati da un problema ad una qualche risorsa critica. Le dipendenze possono essere interpretate in forma gerarchica ad albero, e quando un errore accade, l'albero viene attraversato all'indietro fino al nodo che non ha dipendenze a monte.

I file di configurazione sono molto flessibili e permettono di raggruppare gli host da monitorare in gruppi e ad essi associare molteplici servizi da testare.

Gli allarmi possono essere bloccati fino a che il problema non viene risolto tramite autenticazione, inoltre allarmi di host, gruppi o servizi possono essere temporaneamente disattivati e riattivati senza fermare e far ripartire MON. Questa funzionalità è comoda quando per esempio si vuole aggiornare un server, si disabilita il suo controllo per ripristinarlo appena terminato il lavoro.

Dai vari link della pagina web si accede ad ulteriori informazioni sugli allarmi, sui sistemi monitorati, oltre a statistiche e log.

La configurazione INGV di MON fornisce molte informazioni tra le quali la raggiungibilità o meno delle singole stazioni (attualmente tutte le GAIA e tutte le MEDNET sia su RUPA sia su WIND), dei router remoti, dei server in istituto e il funzionamento dei processi di acquisizione. Per le stazioni GAIA è monitorato (tramite il servizio **syslog**) il numero dei satelliti visibili, la presenza dell'alimentazione e, così come per le Mednet, il funzionamento del server Seedlink (servizio **SLchk**).

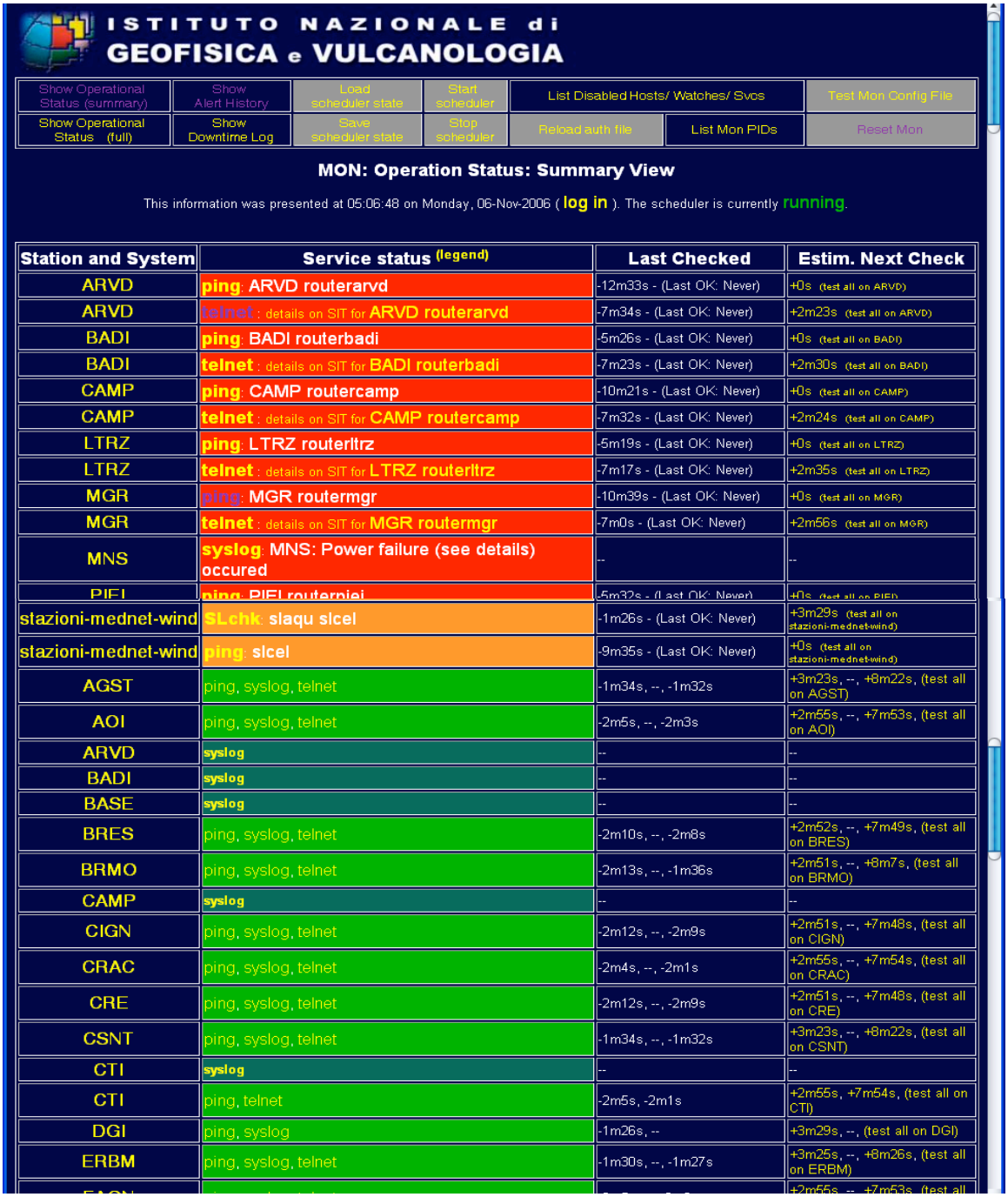


Figura 7: interfaccia web di MON, l'indirizzo attuale è http://nara.int.ingv.it/cgi-bin/mon.cgi.

Analizzando l'interfaccia di MON (fig. 7), nella prima colonna ci sono i gruppi controllati: le singole stazioni GAIA (per comodità, il singolo gruppo è composto da TN e router), le stazioni Mednet distinte in base al collegamento (WIND e RUPA), i router Mednet, i computer di acquisizione e quelli con *SisMux*, i router sia WIND sia RUPA presenti in sede a Roma.

Nella seconda colonna (Service Status) c'è il riepilogo degli esiti dei test effettuati sui vari gruppi: **ping**, **telnet**, **Seedlink check** e ricezione trap (**syslog**) per le GAIA, **ping** e **Seedlink check** per le Mednet, **ping** per tutti i router, **ping** per i computer di acquisizione e SisMux e test di funzionalità dei processi Backnet. In caso di guasto MON porta in cima la il relativo gruppo, cambia il colore da verde (test passato) a rosso (test in errore) del servizio e dà una prima informazione sul guasto. Cliccando sul servizio errorato (figg. 8 e 9), si hanno ulteriori informazioni. Nella pagina cui si accede esiste un altro link (List downtime log) che rimanda ad un riepilogo (durata e tipologia) del guasto del gruppo stesso.

Nella terza e quarta colonna vengono riportati tempi dell'ultimo controllo effettuato e il tempo rimanente per il successivo.

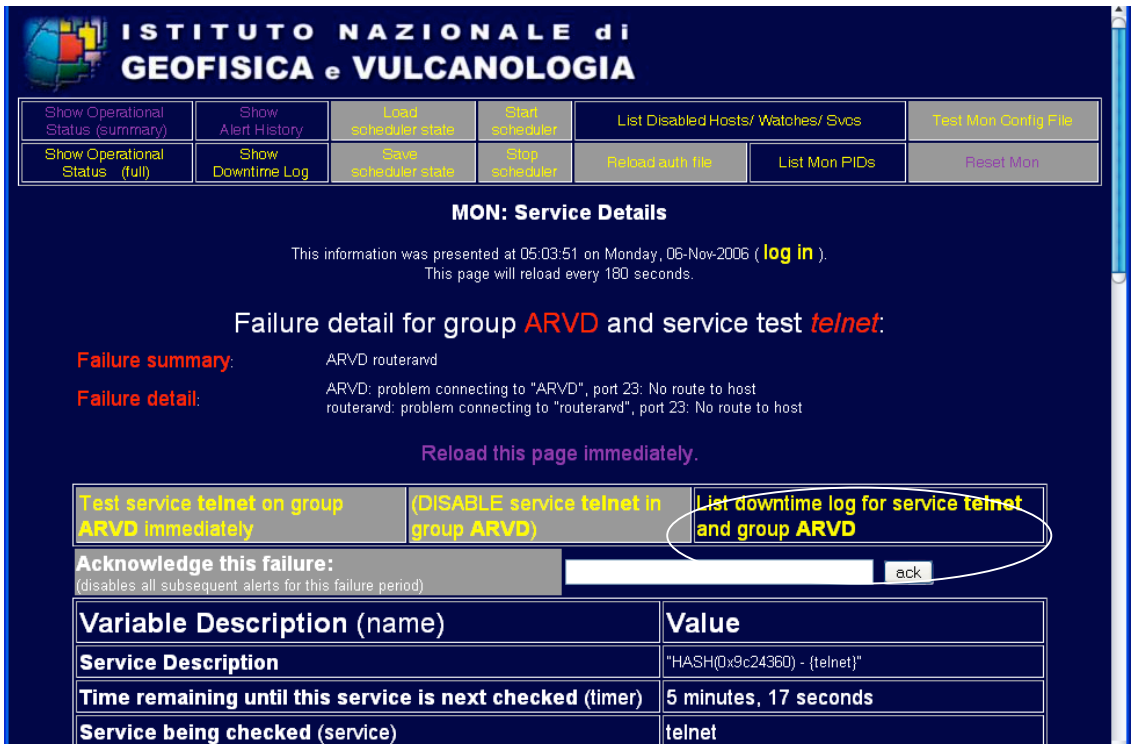


Figura 8: dettagli dell'errore del servizio telnet della stazione ARVD.

Figura 9: dettagli dell'errore del servizio syslog della stazione MNS.

Cliccando sul nome di un gruppo si accede ad una pagina (fig. 10) nella quale è possibile disabilitare/abilitare i servizi da controllare per il gruppo e i membri del gruppo stesso (in questa pagina c'è il link List downtime log che dà il riassunto di tutti gli errori del gruppo (fig. 11).

Figura 10: pagina di abilitazione/disabilitazione del gruppo BADI.

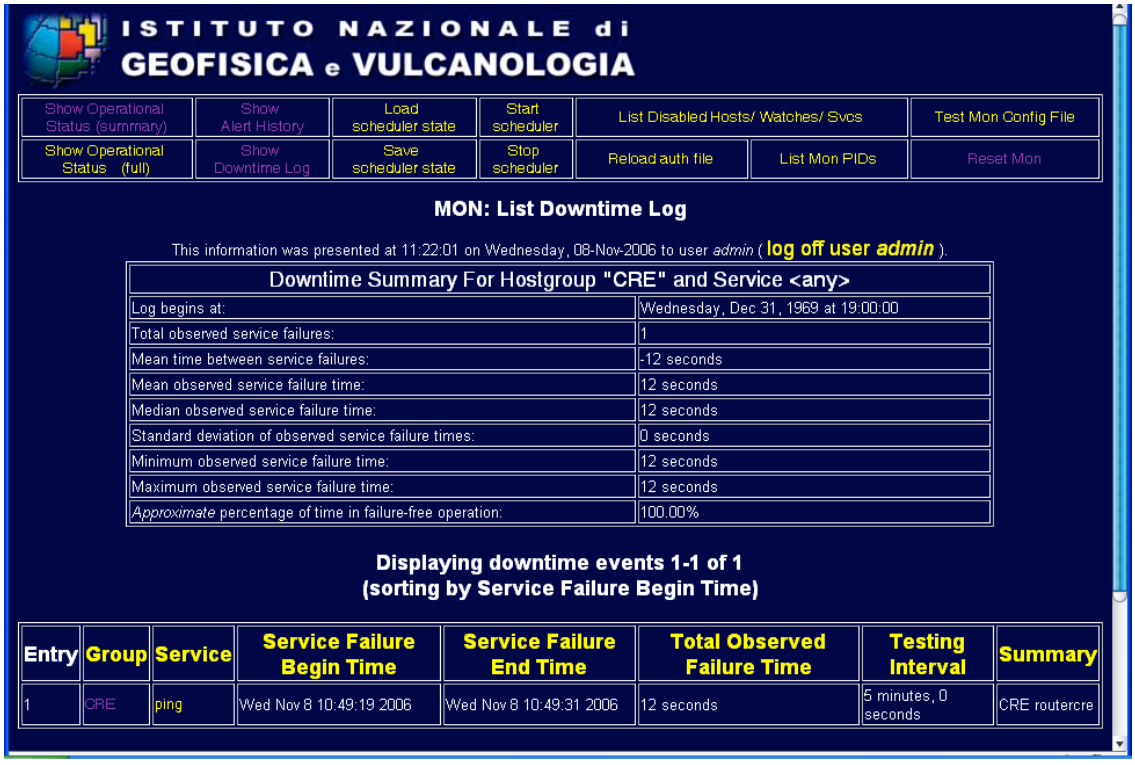


Figura 11: list downtime log del gruppo CRE.

Quando vengono risolti gli errori, MON riporta nella posizione originaria il gruppo ricambiando il colore da rosso a verde del servizio. C'è da notare che qualche volta nel servizio syslog, rientrato il problema, MON non se ne accorge. Questo è dovuto al fatto che le trap inviate dalle stazioni vengono trasmesse col protocollo UDP che, come già visto, non garantisce la comunicazione.

8. Appendice A

Di seguito sono elencate le stazioni GAIA attualmente installate nel territorio italiano. Al nome della stazione, con la provincia, è associata la sigla e alcune note che danno informazioni su casi particolari, come la presenza di ponte radio, di un apparato geodetico (GPS), di acquisizione di più sensori (6CH) o tipologia del collegamento.

NOME	SIGLA	NOTE	NOME	SIGLA	NOTE
Augusta (SR)	AGST		Minerbio (BO)	FIU	
Ancona	AOI		Magasa (BR)	MAGA	GPS
Arcevia (AN)	ARVD		Morigerati (SA)	MGR	GAIA2
Appiano (BZ)	APPI	Ponte Radio	Milazzo	MILZ	GAIA2 GPS
Badiali (Città di Castello) (PG)	BADI		Montasola (RI)	MNS	GAIA2
Bressanone (BZ)	BRES	AGDF2	Montecelio (RM)	MTCE	
Bormio (SO)	BRMO		Novellara (RE)	NOVE	GAIA2
Campotosto (AQ)	CAMP		Oriolo (CS)	ORI	
Città di Castello	CDCA	GAIA2 6 ch	Oschiri	OSKI	GAIA2 sat
Sant'Elia a Pianisi (CB)	CIGN	GPS	Pesaro	PESA	GPS GAIA2
Cesi (MC)	CESI	satellite	Cagli (PU)	PIEI	GAIA2
Craco (MT)	CRAC	GPS	Patocco (UD)	PTCC	GAIA2 int
Caprese Michelangelo (AR)	CRE		Pietrapertosa (PT)	PTRP	GAIA2
Castellina in Chianti (SI)	CSNT		Ravarino (MO)	RAVA	
Castel Tesino (Pieve Tesino) (TN)	CTI	GAIA2	Rocca di Papa (RM)	RDP	Ponte Radio
Campotto Po (FE)	CMPO	GAIA2 sat	Repubblica di San Marino	RSM	GAIA2
Dorgali (NU)	DGI		San Benedetto Po (MN)	SBPO	GAIA2 GPS
Castelnovo ne'monti (RE)	ERBM		San Chirico Raparo (PT)	SCHR	GPS
Faenza (RA)	FAEN	GAIA2 int	Monte Rota (BZ)	SEST	Ponte radio
Fagnano Alto (AQ)	FAGN		Senigallia	SENI	GAIA2 P. R.
Fossombrone (PU)	FSSB		Santa Sofia (FO)	SFI	GAIA2
Forni a Voltri (UD)	FVI		S. Gregorio Matese (CE)	SGG	
Gibilmanna (PA)	GIB	GAIA2 int.	Sala Consilina (SA)	SLCN	Ponte radio
Giuliano di Roma (FR)	GIUL		Samo (RC)	SOI	
Girifalco (CZ)	GRI		Villa Celiera (PU)	VCEL	
Guarcino (FR)	GUAR	GAIA2 GPS	Ventotene (LT)	VENT	GPS
Leonessa (RI)	LNSS	GPS	Villavallelonga (AQ)	VVLD	GPS
Laterza (Casone S. Vito) (TA)	LTRZ	GAIA2	Zocca (MO)	ZCCA	GAIA2

9. Appendice B

Il Point to Point Protocol viene definito nella **RFC 1661**, va a sostituire il protocollo **SLIP** (Serial Line Internet Protocol) le cui caratteristiche erano troppo limitate per gestire l'incremento delle connessioni ad Internet. Le caratteristiche principali di PPP sono:

- supporto multiprotocollo;
- supporto all'autenticazione;
- riconoscimento errori;
- supporto all'indirizzamento IP dinamico.

I principali componenti del protocollo PPP sono tre:
- Un metodo di **incapsulamento** per i datagrammi di diversi protocolli;
- **LCP** (Link Control Protocol) per stabilire, configurare e mantenere sotto controllo la connessione;
- **NCP** (Network Control Protocol) per configurare i diversi protocolli a livello rete che vengono trasportati.

INCAPSULAMENTO

L'incapsulamento permette di trasportare simultaneamente più protocolli sullo stesso collegamento, questo processo è stato progettato in modo da garantire la compatibilità tra hardware di vendor differenti. Il formato dei frame PPP è simile a quello utilizzato da **HDLC** (*High-level Data Link Control*).

LINK CONTROL PROTOCOL

Il link control protocol permette di avere a disposizione un metodo per tenere sotto controllo e quindi gestire la connessione PPP. LCP oltre a stabilire e terminare la comunicazione si occupa anche dell'autenticazione dei sistemi che si mettono in comunicazione e del monitoraggio del suo corretto funzionamento.

NETWORK CONTROL PROTOCOL

Grazie a NCP è possibile avere un protocollo di controllo per ogni livello rete supportato. Ncp si occupa quindi di negoziare le opzioni del livello rete, come per esempio l'attribuzione dell'indirizzo IP utilizzato poi anche da altri protocolli TCP/IP trasportati.

PRINCIPALI FASI DI UNA CONNESSIONE PPP

Le fasi di una connessione PPP sono tipicamente 4:
FASE 1: Definizione della connessione (*Link Establishment Phase*);
FASE 2: Autenticazione (*Authentication Phase*);
FASE 3: Configurazione Protocollo di rete (*Network-Layer Protocol Phase*);
FASE 4: Terminazione della connessione (*Link Termination Phase*).

1 - Definizione della Connessione

La connessione viene stabilita dal Link Control Protocol il quale provvede a scambiare dei pacchetti di configurazione tra i due host che si mettono in contatto. La negoziazione avviene per i valori differenti da quelli predefiniti. I valori configurati sono:

- **MRU** (*Maximum Receive Unit*): Definisce la dimensione massima dei pacchetti trasmessi;
- **Authentication Protocol**: Seleziona il protocollo per l'autenticazione;
- **Quality of Link Protocol**: Determina se sono abilitate le funzioni di controllo della connessione;
- **Magic Number**: Individua se il collegamento si trova in uno stato di loop-back;
- **Protocol field compression**: Permette la compressione del campo protocollo PPP;
- **Address and Control Field compression**: Negozia la compressione dei campi indirizzi e controllo.

Terminata questa fase la connessione è stabilita.

2 - Autenticazione

In alcuni casi prima di scambiare pacchetti a livello rete, l'host che si connette deve essere autenticato. Per default l'autenticazione non è obbligatoria su una connessione PPP, ma se si decide di utilizzarla essa deve avvenire al più presto. Nessuno scambio a livello rete può avvenire prima che l'autenticazione sia completata. I protocolli comunemente utilizzati per l'autenticazione sono **PAP** (Password Authentication Protocol) e **CHAP** (Challange Handshake Autentication Protocol).

3 - Configurazione Protocollo di rete

In questa fase ogni protocollo di rete viene separatamente configurato tramite il proprio Network Control Protocol.

4 - Terminazione della connessione

La connessione PPP può terminare in qualsiasi momento per differenti motivi: caduta della portante, fallimento dell'autenticazione, decadimento della qualità della linea, scadenza del tempo di inattività (idle-time) o chiusura da parte di un amministratore.

Classico esempio di utilizzo del protocollo PPP è la connessione ad Internet tramite modem da parte di un PC. Questo protocollo è altresì utilizzato per connessioni router-router su linee dedicate.

10. Bibliografia

S.Pintore, S. e Salvaterra, L. (2007). Il Progetto TN-1. Rapporti Tecnici INGV, n° 40, 38 pp.

HELLAS- SAT 2 SATELLITE HANDBOOK (2004). www.hellas-sat.net, 87 pp.