r t Anno 2010_Numero 141

rapporti tecnici INGV

Wi-Fi Mesh Network: integrazione dell'infrastruttura telematica della rete sismica e geodetica nazionale

141

Istituto Nazionale di Geofisica e Vulcanologia

Anno 2010_Numero 141

rapporti tecnici

INGV

WI-FI MESH NETWORK: INTEGRAZIONE DELL'INFRASTRUTTURA TELEMATICA DELLA RETE SISMICA E GEODETICA NAZIONALE

Vincenzo Cardinale, Angelo Castagnozzi, Ciriaco D'Ambrosio, Luigi Falco, Antonino Memmolo, Felice Minichiello

INGV (Istituto Nazionale di Geofisica e Vulcanologia, Centro Nazionale Terremoti)

141

Indice

Introduzione

L'INGV (Istituto Nazionale di Geofisica e Vulcanologia) utilizza differenti sistemi di telecomunicazione per l'acquisizione dei dati sismici e gps dalle stazioni remote. L'eterogeneità di questi collegamenti assicura robustezza e ridondanza al servizio di sorveglianza sismica del territorio nazionale.

I Circuiti Diretti Numerici (CDN) ed i Circuiti Diretti Analogici (CDA) hanno costituito per decine di anni gli unici strumenti di connessione permanente delle reti ed a tutt'oggi sono ancora utilizzati per i collegamenti "punto a punto" che permettono l'interconnessione di sistemi, o di LAN, al fine di realizzare le reti private.

Allo stato attuale quasi tutte le stazioni sismiche e gps remote utilizzano un collegamento IP per la trasmissione dati. L'accesso sempre più semplificato a questo tipo di collegamento, ormai maturo ed affidabile, è reso possibile grazie alle evoluzioni che negli ultimi anni si sono avute nel campo delle telecomunicazioni. L'implementazione di un collegamento IP, infatti, è possibile utilizzando le già esistenti e dense reti telefoniche analogiche (adsl), attraverso la realizzazione di reti ad hoc per lo scambio dati come avvenuto con RUPA (Rete Unificata per la Pubblica Amministrazione), grazie all'evoluzione della telefonia mobile (GPRS/EDGE/UMTS/HSDPA), oppure grazie ai recenti collegamenti di tipo satellitare ricorrendo a fornitori come SatLink, Tooway o gestendo in loco, come nel caso dell'INGV, un vero e proprio hub satellitare (Nanometrics Libra Vsat).

La rete wireless mesh della quale si propone la descrizione in questo rapporto tecnico integra l'insieme dei sistemi di trasmissione attualmente utilizzati presso l'INGV riferendosi ancora una volta all'ormai collaudato Internet Protocol (IP).

1. Le reti wireless Wi-Fi e la normativa italiana

Le reti wireless Wi-Fi utilizzano la tecnologia senza fili (wireless), ovvero le onde radio come vettori delle informazioni altrimenti scambiate sui tradizionali cavi in rame, in analogia a quanto avvenuto in passato con l'avvento delle comunicazioni cellulari, rispetto al telefono fisso. Ciò è stato possibile grazie alla disponibilità di nuove bande di frequenza, nonché la maturazione di questa tecnologia, con la conseguente riduzione dei prezzi dei dispositivi.

Wi-Fi, abbreviazione di *Wireless Fidelity*, è un termine che indica dispositivi che possono collegarsi a reti locali senza fili (WLAN) basate sulle specifiche IEEE 802.11. Un dispositivo, anche se conforme a queste specifiche, non può utilizzare il logo ufficiale Wi-Fi se non ha superato le procedure di certificazione stabilite dal consorzio Wi-Fi Alliance (Wireless Ethernet Compatibility Alliance), che testa e certifica la compatibilità dei componenti wireless con gli standard 802.11x (della famiglia 802.11). La presenza del marchio Wi-Fi su di un dispositivo dovrebbe quindi garantirne l'interoperabilità con gli altri dispositivi certificati, anche se prodotti da aziende differenti.

IEEE 802.11 definisce uno standard per le reti WLAN sviluppato dal gruppo 11 dell'IEEE 802, in particolare in livello fisico e MAC del modello ISO/OSI. Questo termine viene usualmente utilizzato per definire la prima serie di apparecchiature 802.11 sebbene si debba preferire il termine "802.11 legacy".

La famiglia 802.11 consta di tre protocolli dedicati alla trasmissione delle informazioni (a, b, g), la sicurezza è stata inclusa in uno standard a parte, 802.11i. Gli altri standard della famiglia (c, d, e, f, h, …) riguardano estensioni dei servizi base e miglioramenti di servizi già disponibili. Il primo protocollo largamente diffuso è stato il b; in seguito si sono diffusi il protocollo a e soprattutto il protocollo g.

L'802.11b e 802.11g utilizzano lo spettro di frequenze (banda ISM) nell'intorno dei 2,4 GHz. Si tratta di una banda di frequenze regolarmente assegnata dal piano di ripartizione nazionale (ed internazionale) ad altro servizio, e lasciato di libero impiego **solo** per le applicazioni che prevedono potenze EIRP (Massima Potenza Equivalente Irradiata da antenna Isotropica) di non più di 20 dBm ed utilizzate **all'interno di una proprietà privata** (no attraversamento suolo pubblico). Trovandosi così ad operare in bande di frequenze ove già lavorano altri apparecchi, i dispositivi b e g possono essere influenzati da telefoni cordless, ripetitori audio/video per distribuire programmi televisivi satellitari od altri apparecchi all'interno di un appartamento che utilizzano quella banda di frequenze.

L'802.11a utilizza la banda ISM dei 5,4 GHz. Tuttavia non risponde alla normativa europea ETSI EN 301 893 che prevede DFS (Dynamic Frequency Selection), TPC (Transmit Power Control) e radar meteorologici; tale normativa di armonizzazione europea è valida in Italia su indicazione del Minitero delle Comunicazioni con il decreto ministeriale del 10 gennaio 2005.

Per ovviare al problema in Europa è stato introdotto nel 2004 il protocollo *802.11h*, che risponde ai requisiti richiesti. Un apparato WiFi per trasmettere su suolo pubblico in Italia a 5.4GHz deve quindi utilizzare questo standard.

Dal punto di vista normativo occorre fare riferimento alle direttive nazionali che si rifanno alle norme europee.

Il piano nazionale di ripartizione delle frequenze (decreto ministeriale 20 febbraio 2003) destina ad uso delle wireless-lan le seguenti frequenze:

- 2.400-2.483,5 MHz
- 5.150-5.350 MHz (all'interno di edifici)
- 5.470-5.725 Mhz (in campo aperto)

La trasmissione in questi intervalli di frequenze è regolamentata dalla normativa ETSI.

Il quadro normativo (ETSI EN 301 893 V1.4.1 (2007-07)) è piuttosto complesso; in riferimento alla nostra tipologia di rete e per gli apparati utilizzati, i punti da rispettare sono i seguenti:

- viene definito un limite massimo nella potenza di trasmissione
  - 20 dBm EIRP sui 2.400-2.483,5 Mhz
  - 23 dBm EIRP sui 5.150-5.350 Mhz
  - 30 dBm EIRP sui 5.470-5.725 Mhz

- è reso obbligatorio l'utilizzo di un sistema di controllo di potenza che assicuri un fattore di mitigazione di almeno 3 dB (TPC)
- è richiesta la selezione dinamica della frequenza che assicuri una distribuzione uniforme del carico sui 255 MHz della banda in questione (DFS)
- è richiesto un meccanismo che controlli l'assenza di attività radar nei canali selezionabili per la trasmissione

MikrotikOS (ambiente operativo installato sugli apprati radio utilizzati e descritto nei successivi paragrafi) può rispondere completamente ai requisiti richiesti delle norme italiane utilizzando le seguenti configurazioni:

- Frequency Mode = regulatory domain

- Country = Italy
- Antenna Gain = (guadagno dell'antenna - perdita dei cavi) in db
- DFS mode = radar detect

In base alla normativa vigente, quindi, tali apparati possono emettere una potenza massima, comprensiva del guadagno dell'antenna utilizzata, in termini di EIRP (Equivalent Isotropically Radiated Power) di 1 W (paragonabile alla potenza di un tipico telefono cellulare) per le reti a 5 GHz e di 0,1 W per le reti a 2,4 GHz.

Oltre alle su citate normative, nazionali e comunitarie, tali apparati devono soddisfare anche le normative in materia di limiti di esposizione della popolazione ai campi elettromagnetici (D.M. 10 settembre 1998, n. 381 Regolamento recante norme per la determinazione dei tetti di radiofrequenza compatibili con la salute umana) e sono soggette a controlli da parte dell'ARPA.

L'installazione e l'esercizio di tali apparati sono soggetti agli stessi vincoli a cui sono sottoposte le SRB per telefonia mobile in materia di inquinamento elettromagnetico (come indicato nel titolo VIII, capo IV e nel comma 3 dell'articolo 306 del decreto legislativo 9 aprile 2008, n. 81.), per cui è possibile la verifica preventiva del progetto ed i controlli dei campi elettromagnetici, laddove necessari, da parte dell'ARPA.

L'imposizione della potenza massima, comprensiva del guadagno dell'antenna utilizzata, ad 1 W fa si che le distanze massime ottenibili siano difficilmente superiori a 35 km.

2. Le reti Mesh e nozioni di internetworking

La tecnologia mesh non è una novità dal punto di vista tecnico, ma solo oggi sta incontrando grande approvazione. Le reti mesh usano la stessa tecnologia del Wi-Fi ma con una topologia diversa.

Nel sistema tradizionale, basato su hot-spot, l'architettura è ad albero, poiché ogni access point deve essere collegato alla rete fissa. Un approccio che può risultare troppo complesso e costoso in alcune situazioni, soprattutto quando le aree da coprire sono ampie.

Per questo, le reti mesh hanno un'architettura magliata, con un funzionamento analogo a quello di Internet: gli access point sono in grado di dialogare tra loro e hanno tutti funzioni di routing, cioè sono in grado di inoltrare i pacchetti verso un altro nodo; è sufficiente, quindi, che uno di questi sia connesso alla rete cablata per estendere la copertura.

Ulteriori access point collegati fisicamente alla rete possono essere aggiunti per aumentare l'affidabilità complessiva del sistema o per migliorare il throughput, riducendo il numero di salti (hop) necessari per raggiungere il punto di interconnessione.

2.1 Bridging vs Routing

Una delle decisioni ricorrenti nella progettazione di una rete è sicuramente la scelta di effettuare bridging o routing. Si elencano brevemente alcune differenze.

Il bridge è un dispositivo che connette reti differenti e opera attraverso i livelli uno e due del modello OSI, quello fisico e quello data link.

Un router opera attraverso i primi 3 livelli del modello OSI, aggiungendo il livello rete a quello fisico e data link. I bridge possono contattare i dispositivi connessi ad una rete attraverso i loro indirizzi MAC (media access control) ma non possono farlo attraverso protocolli del livello di rete come IP.

I router a differenza dei bridge calcolano i percorsi ottimali per raggiungere le reti mantenendo le informazioni nelle tabelle di routing.

In teoria l'uso del bridge consente l'interconnessione di reti dello stesso tipo (come tutte IP o tutte IPX) mentre il router consente la telecomunicazione tra reti differenti (ad esempio è possibile collegare reti IP a reti IPX). Da un punto di vista pratico conviene sempre implementare il routing, se possibile, perché più efficiente. Il bridge è necessario quando non è possibile subnettare la propria rete IP o quando si ha la necessità di usare protocolli non-routabili come Netbios o DECnet.

Nel complesso il bridge è molto semplice da configurare e consente l'interconnessione ad una rete in maniera trasparente ma tutto questo lo si paga con le performance. Questo perché: Tipicamente un bridge è munito di porte con cui è collegato a diversi segmenti della rete. Quando riceve un frame su una porta, cerca di capire se il destinatario si trova nello stesso segmento del mittente oppure no. Nel primo caso evita di inoltrare la trama, in quanto presumibilmente il destinatario l'ha già ricevuta. Nel secondo caso, invece, il bridge inoltra la trama verso il segmento in cui si trova il destinatario. Se non sa su quale segmento si trova il destinatario, il bridge inoltra la trama su tutte le porte tranne quella da cui l'ha ricevuta. Queste operazioni sono definite operazioni di **filtraggio** e **inoltro**. Il bridge quindi comporta spesso un inutile dispendio di risorse dovuto alle frequenti trasmissioni broadcast impattando quindi sulle prestazioni.

In alternativa, il router, operando sul terzo strato del modello OSI, è in grado di prendere decisioni più intelligenti circa l'invio di un pacchetto attraverso la rete esaminando gli indirizzi mittente e destinazione di ciascun pacchetto. Esso inoltra solo i pacchetti destinati ad una rete remota. Questo elimina il traffico inutile e consente un'allocazione di banda più efficiente.

Per la rete mesh di acquisizione dati sismici e gps è stato implementato il routing.

2.2 Routing

Il termine Routing indica generalmente attività degli apparati di rete volte a determinare il percorso lungo il quale inoltrare i pacchetti. Nel campo dell'internetworking esistono tre tecniche fondamentali per guidare il routing.

Routing by network address (instradamento basato sull'indirizzo di rete): l'intestazione di ogni pacchetto contiene l'indirizzo di livello rete del destinatario. Quando riceve un pacchetto, l'apparato decide su quale delle sue interfacce esso debba essere trasmesso in base all'indirizzo della destinazione. La decisione viene presa mediante l'uso di una tabella che, nell'eccezione più semplice, contiene una riga per ogni destinazione che il router sa raggiungere; l'apparato trova la riga che si riferisce all'indirizzo del destinatario del pacchetto e in essa reperisce le informazioni necessarie all'inoltro. Questa tabella è chiamata forwarding table (tabella di inoltro) o routing table (tabella di routing). La tecnica routing by network address viene utilizzata, tra gli altri, dai protocolli IEEE 802.1D, IPv4, IPv6, IPX, Decnet Fase IV, ISO CLNP.

Label swapping (scambio di etichetta): l'intestazione di ogni pacchetto contiene un'etichetta usata dal router per trovare la riga della tabella di routing contenente le informazioni per l'instradamento del pacchetto. Normalmente tale riga contiene anche una nuova etichetta, che l'apparato sostituisce a quella presente nell'intestazione del pacchetto prima di ritrasmetterlo. Ciò, sebbene rappresenti un'elaborazione ulteriore che l'apparato deve fare su ogni pacchetto, rende locale a ogni collegamento la validità delle etichette e, di conseguenza, ne semplifica l'assegnazione. La tecnica del label swapping è normalmente impiegata in reti che forniscono servizi orientati alla connessione (connection oriented): a ogni connessione è associata un'etichetta su ogni collegamento attraversato. La tecnica è utilizzata nei protocolli ATM, Frame Relay, X.25, APPN.

Source routing (routing controllato dal mittente): il mittente scrive nell'intestazione del pacchetto il percorso da seguire in terminini di router intermedi (ed eventualmente collegamenti) da attraversare. Questa tecnica di inoltro non richiede la presenza di tabelle di routing all'interno dei nodi ed è utilizzata dai bridge per reti Token Ring, detti bridge source route, nei protocolli IPv4, IPv6, HPR.

Le prime due tecniche di routing sono di gran lunga le più diffuse; in questo rapporto tecnico si è fatto riferimento alla tecnica di Routing by network address.

2.2.1 La tabella di routing

Il funzionamento del routing by network address è strettamente legato all'organizzazione della tabella di routing. Il contenuto specifico di ogni riga della tabella dipende dal particolare protocollo. In linea generale, senza approfondire ulteriormente l'argomento, possiamo assumere che ogni riga della tabella di routing di un apparato di internetworking, che realizza routing by network address, oltre all'indirizzo della destinazione contiene l'interfaccia su cui inoltrare i pacchetti per tale destinazione e il costo per raggiungere la destinazione sul percorso che comincia dall'interfaccia indicata. Il costo consente al router di scegliere tra eventuali percorsi alternativi; l'unità di misura di questo costo dipende dal protocollo utilizzato.

Quando il router deve inoltrare un pacchetto, scorre la tabella per individuare la riga corrispondente al destinatario del pacchetto. Il numero medio di passi richiesti da tale operazione, detta table lookup (ricerca in tabella), è pari alla metà del numero di righe. Considerando che l'operazione è fatta per ogni pacchetto da inoltrare, la sua complessità è un aspetto molto critico per le prestazioni di un apparato; per questo i costruttori investono notevoli risorse per ridurre il tempo necessario alla ricerca in tabella, progettando algoritmi sempre più efficienti. Nella maggior parte dei protocolli che usano la tecnica routing by network address l'inoltro non è basato sull'intero indirizzo del destinatario, ma su un prefisso, molto speso di lunghezza variabile. Quindi, il dispositivo non deve "semplicemente" cercare la riga che contiene l'indirizzo della destinazione, ma quella che contiene il più lungo prefisso comune all'indirizzo del destinatario. Questa operazione, chiamata long est prefix matching (corrispondenza del prefisso più lungo), è di complessità superiore alla semplice ricerca di una riga che contenga un certo indirizzo.

2.2.2 On-line e off-line routing

Come già descritto il termine routing indica genericamente le attività dei dispositivi di internetworking volte a determinare il percorso lungo il quale inoltrare i pacchetti. Nel caso in cui l'inoltro sia basato su una tabella di routing, il percorso seguito dai pacchetti dipende dalle tabelle dei vari apparati, quindi la loro costruzione è parte integrante del routing. Dunque il routing nelle reti a commutazione di pacchetto ha due componenti tra di loro complementari ed entrambe indispensabili per il corretto funzionamento della rete.

On-line routing (instradamento in linea) è una funzione del piano dati degli apparati in quanto, agisce su ogni singola unità dati che l'apparato inoltra.

Off-line routing (instradamento fuori linea) è una funzione del piano di controllo degli apparati, cioè di quell'insieme di funzionalità volte a controllare il funzionamento dell'apparato. Pur essendo essenziali, queste funzionalità non sono parte integrante dell'inoltro di ogni singola unità dati; infatti, come indica il nome, l'off-line routing viene realizzato in modo indipendente rispetto all'inoltro dei pacchetti – per esempio, normalmente la scelta del percorso verso una destinazione è assolutamente slegata dal fatto che sulla rete sia effettivamente presente traffico verso quella destinazione.

La suddivisione del routing nelle due componenti sopra elencate è essenziale se si tiene conto della sua natura quasi contraddittoria. Da un lato il routing deve essere molto sofisticato per consentire un recapito delle informazioni che sia il più possibile certo, veloce e robusto. D'altro lato la decisione di routing sul singolo pacchetto deve essere presa molto velocemente per consentire all'apparato per internetworking di

inoltrare un numero elevato di pacchetti. Di qui la suddivisione del routing nelle due componenti: l'off-line routing può applicare algoritmi sofisticati e relativamente lenti per decidere i percorsi; questi vengono tradotti in strutture dati (le tabelle di routing) semplici e veloci da utilizzare da parte dell'on-line routing per far si che i pacchetti inoltrati seguano effettivamente le strade scelte.

Affinché i pacchetti arrivino a destinazione è indispensabile che le tabelle nei vari router siano coerenti, altrimenti i pacchetti vengono inoltrati lungo percorsi ciclici (routing loop). In tal caso essi non raggiungono la destinazione, ma girano per sempre a vuoto nella rete, oltretutto consumando inutilmente risorse computazionali e trasmissive.

Dal percorso lungo cui un pacchetto viene inoltrato dipendono il ritardo che esso subisce, la probabilità che sia scartato a causa della congestione dei router intermedi e il fatto che esso raggiunga o no la destinazione. Inoltre, se la rete contiene maglie, come nel caso della rete mesh descritta in questo rapporto tecnico, una destinazione può essere raggiunta attraverso più percorsi alternativi; in presenza di guasti, la scelta di un percorso che eviti nodi o collegamenti non funzionanti consente alla rete di continuare a recapitare dati. Dunque la scelta dei percorsi, cioè l'off-line routing, è un fattore chiave per il buon funzionamento di un internetwork e per la sua robustezza ai guasti (fault-tolerance). L'off-line routing può essere operato in modo statico o dinamico.

2.2.3 Routing statico

Il routing statico (static routing) prevede che i percorsi d'inoltro dei pacchetti siano determinati ed eventualmente cambiati dall'amministratore della rete tramite la configurazione degli apparati di internetworking. In altre parole, l'amministratore di rete ha la responsabilità di inserire o modificare righe della tabella di routing. Il principale svantaggio del routing statico è l'impossibilità di reagire automaticamente ai cambiamenti topolgici, cioè di adattare i percorsi alle variazioni nello stato di funzionamento di nodi e collegamenti.

In realtà, quando si utilizza il routing statico si ottiene una limitata reattività ai guasti introducendo, nelle tabelle di routing, route alternative per la stessa destinazione come mostrato nell'esempio della **fig. 1** per le destinazioni X e Y. La rotta detta primaria presenta un costo minore per raggiungere la destinazione (attraverso l'interfaccia 3 per raggiungere X e attraverso l'interfaccia 1 per raggiungere Y) e viene utilizzata per l'inoltro dei pacchetti in condizioni normali. Il costo associato a una route (rotta) è associato dal gestore della rete in base a criteri topologici o amministrativi; per questo motivo non ha un particolare unità di misura o un significato generalmente riconosciuto.

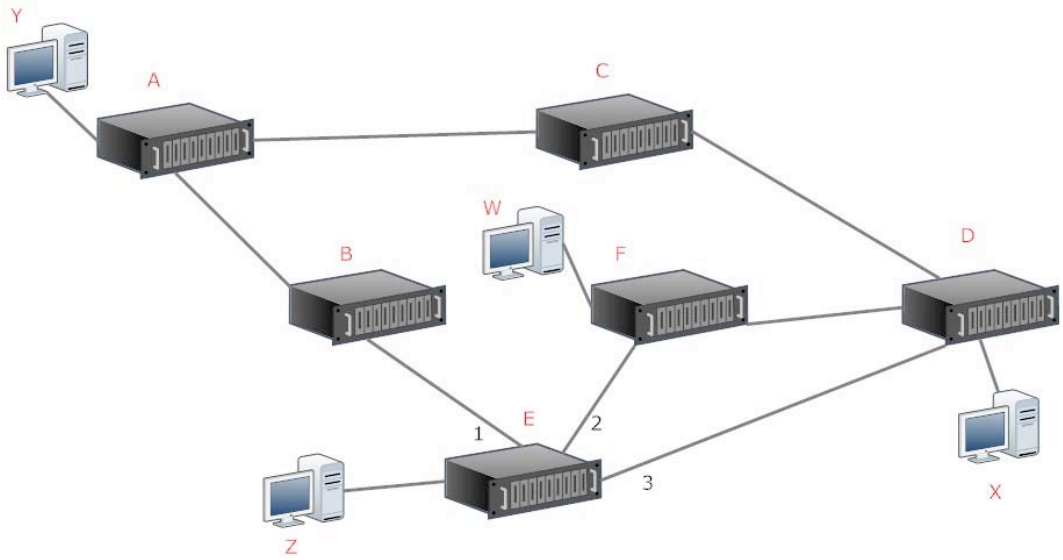


Figura 1. Esempio topologia di rete.

Se a causa di un malfunzionamento l'interfaccia 3 non fosse utilizzabile, l'apparato ignorerebbe tutte le route che fanno uso di tale interfaccia. Quindi, i pacchetti per la destinazione X sarebbero inoltrati secondo quanto specificato dalla route secondaria che, sebbene presenti un costo più elevato, è la più conveniente quando l'interfaccia 3 non funziona. Discorso analogo vale per i pacchetti destinati a Y; essi sono normalmente inoltrati attraverso l'interfaccia 1, ma in caso di malfunzionamento di quest'ultima vengono inviati attraverso l'interfaccia 3.

L'uso delle route alternative non rende comunque la rete sufficientemente robusta. Infatti, nel caso del malfunzionamento del collegamento tra A e B, il router E continuerà ad utilizzare la sua route primaria verso Y mandando a B i pacchetti e B sarà costretto a scartarli perché impossibilitato a inoltrarli verso A. Il routing statico presenta, quindi, limitata robustezza ai guasti dell'internetwork; in effetti, la rete potrebbe funzionare correttamente se E fosse in grado di reagire al malfunzionamento del collegamento tra A e B, inoltrando i pacchetti per Y sulla sua interfaccia 3. L'uso del routing dinamico permette di ottenere questo.

2.2.4 Routing dinamico

Il routing dinamico (dynamic routing) consente ai router di ricalcolare automaticamente le loro tabelle di routing, in modo da reagire a cambiamenti della topologia della rete dovuti al mutare dello stato di funzionamento degli apparati e dei collegamenti.

Il routing dinamico può essere realizzato secondo tre paradigmi fondamentali.

Routing centralizzato: l'off-line routing è operato da un centro di calcolo che si occupa di compilare le tabelle di routing per tutti i router della rete e poi di installarle su ognuno di essi. La centralizzazione del routing elimina la possibilità che diversi apparati compiano scelte tra loro incoerenti. Tuttavia, dal momento che il centro di calcolo del routing necessita di informazioni sullo stato della rete che gli devono essere inviate dai vari apparati, il traffico nella zona della rete circostante può rilevarsi troppo elevato.

Routing isolato: ogni router costruisce la propria tabella di routing autonomamente e senza interagire con gli altri. Il più popolare algoritmo che segue tale paradigma è chiamato backward learning e viene utilizzato dai bridge IEEE 802.1d. Il routing isolato è particolarmente semplice, ma presenta un'efficacia limitata.

Routing distribuito: prevede che i router scambino informazioni sulla topologia della rete per compilare la propria tabella di routing. Le decisioni di routing vengono prese indipendentemente da ogni apparato, ma sono basate su informazioni ottenute cooperando con gli altri apparati. Questo paradigma di routing è applicabile a reti di dimensione arbitraria ed è di gran lunga il più utilizzato sulle reti moderne.

A ogni collegamento della rete è associato un costo di attraversamento che è normalmente detto metrica. Per scegliere tra percorsi alternativi in modo coerente, i router compongono le metriche di tutti i collegamenti che costituiscono il percorso e scelgono quello che ha il minimo costo totale. A seconda della semantica della metrica (ritardo di attraversamento, banda, carico del collegamento, intereferenze radio nel caso della rete wifi oggetto di questo rapporto) la composizione può consistere nella somma, oppure nella scelta del valore massimo o in altri tipi di operazione. Il costo per il raggiungimento degli apparati vicini è un parametro che viene fornito dall'amministratore di rete in fase di configurazione degli apparati e non deve necessariamente essere simmetrico nelle due direzioni di un collegamento. Questo può riflettere effettive differenze nelle caratteristiche del collegamento nelle due direzioni (per esempio diversa capacità trasmissiva o livello medio di carico), oppure decisioni di tipo amministrativo volte a invitare i router intermedi a usare un collegamento in un senso e non in quello opposto.

Lo scambio di informazioni e il calcolo della tabella di routing avvengono dunque secondo un algoritmo di routing. Due sono gli algoritmi di routing più utilizzati nel routing distribuito: distance vector e link state. La descrizione dettagliata degli algoritmi esula da questo rapporto tecnico pertanto saranno affrontati in modo superficiale.

2.2.5 Distance Vector

L'algoritmo distance vector prevede che il router invii su tutte le proprie interfacce l'elenco delle destinazioni che è in grado di raggiungere e la loro distanza da sé. Tale elenco è chiamato appunto "distance vector" (vettore delle distanze); la destinazione è espressa da un indirizzo e la distanza è il minimo costo associato a una route verso la destinazione.

D'altro canto un apparato riceve un distance vector da ognuno dei suoi vicini e lo memorizza dopo aver sommato alle distanze annunciate la distanza tra sé e il vicino che ha inviato il distance vector. I distance vector costituiscono la conoscenza a disposizione dei router per la raggiungibilità delle destinazioni della rete. A partire da tale conoscenza l'apparato costruisce la propria tabella di routing con una semplice operazione di fusione (merge) dei distance vector. All'atto della fusione avviene la scelta del percorso lungo cui raggiungere una destinazione che sia contenuta in più di un distance vector: i pacchetti per tale destinazione saranno inviati sull'interfaccia da cui è stato ricevuto il distance vector contenente la distanza minima associata alla destinazione. La fusione dei distance vector deve essere ripetuta ogni volta che viene ricevuto un nuovo distance vector. Se la tabella di routing viene modificata durante l'operazione di fusione, il router invia un distance vector su tutte le proprie interfacce, in modo che i vicini aggiornino la copia che mantengono memorizzata e ricalcolino di conseguenza la propria tabella.

2.2.6 Link state

L'algoritmo Link state, sebbene più difficile da realizzare, è più semplice e intuitivo da comprendere di quello distance vector. Esso è basato sul principio che ogni router descrive la topologia della rete intorno a sé, cioè lo stato dei suoi collegamenti (link state); quindi diffonde questa descrizione in tutta la rete trasmettendola all'interno di pacchetti detti LSP (Link State Packet). Per ogni collegamento è specificata l'identità del nodo all'altro capo e la metrica associata, cioè il costo di attraversamento di tale collegamento. D'altro canto, ogni router riceve da tutti gli altri una descrizione dei loro collegamenti e può comporre le varie descrizioni locali come tessere di un mosaico per produrre una mappa dell'intera rete. A questo punto l'apparato sceglie sulla mappa il percorso migliore per raggiungere ogni destinazione, costruendo il più basso

albero (shortest path tree) che ha se stesso come radice e ognuna delle destinazioni come foglie. La distanza dalla radice a un altro nodo è data dalla composizione dei costi associati ai singoli collegamenti (rami) che portano al nodo. L'albero è costruito utilizzando l'algoritmo di Dijkstra, detto anche algoritmo SPF (Shortest Path First) per il modo in cui opera. A partire dallo shortest path tree un router costruisce la tabella di routing associando a ogni destinazione l'interfaccia dell'apparato da cui parte il sottoalbero che contiene la destinazione, e un costo di raggiungibilità pari alla distanza dalla radice.

2.2.7 Confronto tra i due algoritmi

La complessità computazionale dell'algoritmo distance vector è dell'ordine di N^2 oppure di N^3 a seconda della complessità topologica della rete, mentre quella dell'algoritmo link state è C log N. Dunque, dal punto di vista della complessità computazionale, il secondo è sempre preferibile.

A seguito di un cambiamento topologico, l'algoritmo distance vector fa scattare una reazione a catena di trasmissioni di distance vector che comincia nella zona in cui è avvenuto tale cambiamento, si propaga fino alla periferia della rete, quindi nuovamente indietro, e così via per un certo numero di volte.

L'algoritmo link state prevede la propagazione di uno o più LSP dalla zona in cui è avvenuto il cambiamento fino alla periferia.

Quindi, nel primo caso, prima che tutti gli apparati abbiano aggiornato le informazioni di routing, è necessario che l'onda di reazione si propaghi più volte su tutta la rete; nel secondo caso è sufficiente un'unica propagazione.

L'algoritmo distance vector può portare poi, non di rado, all'instaurazione di routing loop perché i router non operano su una rappresentazione topologica della rete, ma su semplici informazioni di distanza. Con l'algoritmo link state ciò non accade perché gli apparati operano su una mappa della rete; i routing loop sono possibili solo quando gli apparati non dispongono tutti della stessa mappa, cioè durante la (breve) fase di propagazione delle informazioni di routing dopo un cambiamento topologico.

Analizziamo, infine, come ultimo termine di paragone, il traffico dovuto allo scambio di informazioni di routing generato dai due algoritmi a seguito di un cambiamento topologico. L'algoritmo distance vector richiede ai nodi situati ai capi di un collegamento che cessa di funzionare di modificare la loro tabella di routing per riflettere il cambiamento di stato del collegamento e generare il distance vector risultante che contiene la distanza di tutte le destinazioni ancora raggiungibili sulla rete. Ciò può eventualmente spingere i vicini a modificare le tabelle di routing e a inviare il loro distance vector, e così via.

Dunque, un cambiamento topologico richiede che parecchi router (eventualmente tutti) generino un distance vector che, su una rete con molte destinazioni, è una struttura dati di grandi dimensioni. L'algoritmo link state richiede invece che i due router ai capi del collegamento che ha subito il cambiamento di stato generino un pacchetto contenente informazioni sui propri collegamenti, cioè una tabella di poche righe (il link state, appunto). Tale tabella viene trasmessa su tutti i collegamenti della rete in modo che raggiunga tutti gli altri router.

Quindi, in generale, l'algoritmo link state richiede di generare una minore quantità di traffico di routing rispetto all'algoritmo distance vector: anche sotto queto punto di vista l'algoritmo link state appare migliore di quello distance vector.

2.2.8 RIP e OSPF

RIP (Routing Information Protocol) e OSPF (Open Shortest path first) sono i protocolli di routing che implementano rispettivamente l'algoritmo distance vector (RIP) e link state (OSPF). Abbiamo scelto per la

rete mesh descritta in questo rapporto tecnico il protocollo OSPF considerati i vantaggi descritti nel paragrafo precedente.

3. Obbiettivi del progetto

Lo scopo di questo lavoro è stato realizzare un'infrastruttura telematica di acquisizione dati sismici e gps perfettamente integrata nei vari sistemi di trasmissione dati utilizzati presso l'INGV. L'infrastruttura doveva essere affidabile, robusta e garantire una banda minima sufficiente anche per applicazioni future ad alto troughput come un elevato campionamento accellerometrico o gps.

Prerogativa ambiziosa di questo progetto è stata la volontà di non affidare la progettazione, realizzazione e gestione della rete Wi-Fi a società esterne, preferendo avere pieno controllo dell'infrastruttura telematica realizzata (dall'installazione e configurazione degli apparati radio all'acquisizione dei dati sismici e gps). Incentivati, poi, dal successo del sistema di trasmissione dati satellitare Libra VSAT di Nanometrics, nel quale la gestione, manutenzione e distribuzione dati è affidata direttamente a personale INGV altamente qualificato, abbiamo intrapreso un percorso di studio approfondito delle reti mesh Wifi che ha portato parte del personale di questo rapporto tecnico al conseguimento della certificazione "*MikroTik Certified Wireless Engineer*".

4. Rete MESH INGV

Di seguito è descritto il layout di rete, la strumentazione hardware e software utilizzata, il piano di indirizzamento, i protocolli di rete implementati e le politiche di sicurezza adottate.

4.1 Hardware

Per la realizzazione della rete ci siamo rivolti principalmente a prodotti di casa Mikrotik.

MikrotikLS, conosciuta anche come Mikrotik, è una produttrice lettone di apparati di networking, in particolare router e apparati wireless con sede a Riga. La compagnia è stata fondata nel 1995 con l'intento di emergere nel mercato wireless. La produzione di hardware è costituita dalla linea di prodotti RouterBOARD, schede modulari con funzioni di router o apparato wireless. Il prodotto software principale, ovvero RouterOS (basato su Linux), permette agli utenti di trasformate un normale PC in un router avanzato con caratteristiche come firewall, VPN server e client, bandwidth shaper, punto d'accesso wireless e molte altre caratteristiche. Il sistema operativo è licenziato con diversi livelli, che permettono diversi utilizzi del sistema. È utilizzato in tutto il mondo da moltissimi wireless internet service provider per connettere utenti in banda non licenziata. Oltre al sistema operativo, punto chiave è la produzione di hardware, le RouterBOARD, che permettono, a basso costo, di implementare soluzioni di rete.

4.1.1 RouterBoard

Abbiamo utilizzato prevalentemente la RouterBOARD 433 (**fig.2**), ma talvolta anche la RouterBOARD433AH (**fig.3**), la RouterBOARD 600 (**fig.4**) e la RouterBOARD 450G (**fig.5**) .

Riportiamo di seguito alcune loro caratteristiche principali:

RouterBOARD 433

The rb433 is a high speed AP/router.

Much faster than it's predecessors the rb433 is replacing not only the low priced rb133, but also the powerful rb333.

The heart of this device is the new Atheros CPU which makes this tiny device a quick one. Tests show that this device is faster than any other low cost product by mikrotik, making the rb400 series fit right behind rb600 and rb1000.

rb433 includes RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router/firewall or bandwidth manager.

One small device - with all the power of RouterOS. At a very special price.

CPU	Atheros AR7130 300MHz network processor
Memory	64MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip
Ethernet	Three 10/100 Mbit/s Fast Ethernet ports with Auto-MDI/X
miniPCI	Three MiniPCI Type IIIA/IIIB slots
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC
Dimensions	10.5 cm x 15 cm, 137 grams
Power consumption	~3W without extension cards, maximum - 25 W
Operating System	MikroTik RouterOS v3, Level4 license

Figura 2. Datasheet RouterBoard 433.

RouterBOARD 433AH

The RB433AH is a more powerful version of the standard RB433. The 128MB DDR will be capable of supporting new RouterOS features coming. The microSD slot supports an additional memory card that can be used for a Dude database and other features.

The 680MHz Atheros MIPs 24K CPU with a 64KB/32KB instruction/data cache is probably the fastest CPU used in low cost wireless access points.

The three Ethernets and mpci slots give you ample data interfaces to put the big CPU power to work.

CPU	Atheros AR7161 680MHz network processor
Memory	128MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip and microSD
Ethernet	Three 10/100 Mbit/s Ethernet ports with Auto-MDI/X
miniPCI	Three MiniPCI Type IIIA/IIIB slots
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC. Voltage monitor.
Dimensions	10.5 cm x 15 cm, 137 grams
Power consumption	~3W without extension cards, maximum - 25 W, 16W output to cards
Operating System	MikroTik RouterOS v3, Level5 license

Figura 3. Datasheet RouterBoard 433AH.

RouterBOARD 600

The high performance wireless platform. It has four miniPCI slots and three gigabit ethernet ports and it is the fastest wireless board that MikroTik has ever made.

The heart of this device is the new state of the art PowerPC networking processor which makes the RB600 faster than any other MikroTik product, introducing a whole new class to the RouterBOARD brand.

Two Compactflash slots for webproxy cache and configuration backups of the User Manager database or The Dude server.

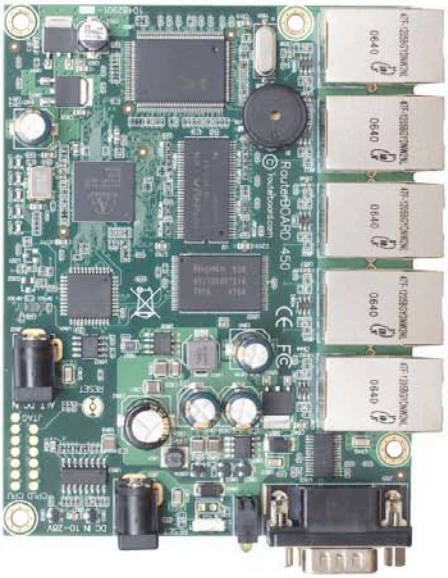
RB600 includes RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router/firewall/bandwidth manager or hotspot.

And all this power - at a very affordable price.

CPU	MPC8343E 266/400MHz network processor
Memory	64MB DDR SDRAM onboard memory
Boot loader	RouterBOOT, 1Mbit Flash chip
Data storage	64MB onboard NAND memory chip
Ethernet	Three 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X
miniPCI	Four MiniPCI Type IIIA/IIIB slots
Expansion	Daughterboard support, including RB500 daughterboards
Compact Flash	Two independent CompactFlash slots (TrueIDE Microdrive supported)
Serial port	One DB9 RS232C asynchronous serial port
Speaker	Mini PC-Speaker
Power options	IEEE802.3af PoE: 38..56V DC including over datalines. Power jack: 10..56V DC
Fan control	Two 5V DC fan power output headers with rotation sensor and automatic fan switching (maximum output current - 300mA total)
Dimensions	14 cm x 20 cm (5.51 in x 7.87 in), 227 g (8 oz)
Power consumption	~9W without extension cards, maximum - 35+ W
Operating System	MikroTik RouterOS v3, Level4 license

Figura 4. Datasheet RouterBoard 600.

RouterBOARD 450



The rb450 is a five port ethernet router. The rb450 is replacing rb150, but introduces at least three times better thoughput.

The heart of this device is the new Atheros CPU which makes this tiny device a quick one. Tests show that the rb400 series is faster than any other low cost product by mikrotik, making the rb400 series fit right behind rb600 and rb1000.

rb450 includes RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router/ firewall or bandwidth manager.

One small device - with all the power of RouterOS. At a very special price.

CPU	Atheros AR7130 300MHz network processor
Memory	32MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip
Ethernet	Five 10/100 Mbit/s Fast Ethernet ports with Auto-MDI/X
miniPCI	none
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC
Dimensions	9 cm x 11.5 cm, 105 grams
Power consumption	~3W without extension cards, maximum – 12 W
Operating System	MikroTik RouterOS v3, Level4 license

Figura 5. Datasheet RouterBoard 450.

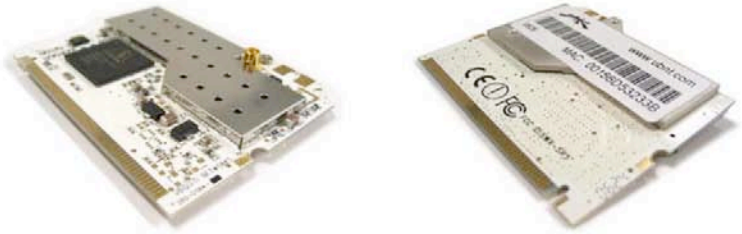
4.1.2 Radio

Le radio utilizzate nella rete mesh sono state: Ubiquiti Super Range 5 (**fig.6)**, Ubiquiti UB-5 (**fig.7**) e Compex WLM54AG (**fig.8**). La scelta del modello è funzione della distanza da coprire, del tipo di antenna utilizzata e relativo cavo.

UBIQUITI NETWORKS

SUPER RANGE 5

Powerful Range and Throughput Performance for 5GHz Networks



CARD INFORMATION	
Chipset	Atheros, 4th Generation, AR5213
Radio Operation	IEEE 802.11a, 5GHz
Interface	32-bit mini-PCI Type IIIA
Operation Voltage	3.3VDC
Antenna Ports	Single MMCX
Temperature Range	-40C to +80C
Security	WPA, WPA2, AES-CCM & TKIP Encryption, 802.1x, 64/128/152bit WEP
Data Rates	6Mbps, 9Mbps, 12Mbps, 24Mbps, 36Mbps, 48Mbps. 54Mbps
TX Channel Width Support	5MHz / 10MHz / 20MHz / 40MHz
RoHS Compliance	YES

REGULATORY INFORMATION	
Wireless Modular Approvals	FCC Part 15.247, CE

RADIO OPERATING FREQUENCY 5.20-5.825GHz

TX SPECIFICATIONS				RX SPECIFICATIONS			
	DataRate	Avg.Power	Tolerance		DataRate	Sensitivity	Tolerance
802.11a OFDM	6Mbps	26 dBm	+/-1.5dB	802.11a OFDM	6Mbps	-94 dBm	+/-1.5dB
	9Mbps	26 dBm	+/-1.5dB		9Mbps	-93 dBm	+/-1.5dB
	12Mbps	26 dBm	+/-1.5dB		12Mbps	-91 dBm	+/-1.5dB
	18Mbps	26 dBm	+/-1.5dB		18Mbps	-90 dBm	+/-1.5dB
	24Mbps	26 dBm	+/-1.5dB		24Mbps	-86 dBm	+/-1.5dB
	36Mbps	24 dBm	+/-1.5dB		36Mbps	-83 dBm	+/-1.5dB
	48Mbps	22 dBm	+/-1.5dB		48Mbps	-77 dBm	+/-1.5dB
	54Mbps	21 dBm	+/-1.5dB		54Mbps	-74 dBm	+/-1.5dB

ADJUSTABLE CHANNEL SIZE SUPPORT (Increase Channel Capacity or Increase Throughput)			
5MHz	10MHz	20MHz	40MHz (Turbo)

CURRENT CONSUMPTION INFORMATION

TX CURRENT CONSUMPTION				RX CURRENT CONSUMPTION			
	DataRate	Current	Tolerance		DataRate	Current	Tolerance
802.11a OFDM	6Mbps	1.30 A	+/-100 mA	802.11a OFDM	6Mbps	350 mA	+/-100 mA
	9Mbps	1.30 A	+/-100 mA		9Mbps	350 mA	+/-100 mA
	12Mbps	1.30 A	+/-100 mA		12Mbps	350 mA	+/-100 mA
	18Mbps	1.30 A	+/-100 mA		18Mbps	350 mA	+/-100 mA
	24Mbps	1.30 A	+/-100 mA		24Mbps	350 mA	+/-100 mA
	36Mbps	1.00 A	+/-100 mA		36Mbps	350 mA	+/-100 mA
	48Mbps	0.90 A	+/-100 mA		48Mbps	350 mA	+/-100 mA
	54Mbps	0.80 A	+/-100 mA		54Mbps	350 mA	+/-100 mA

RANGE PERFORMANCE	
Indoor (Antenna Dependent):	Up to 150meters
Outdoor (Antenna Dependent):	Over 50km

DRIVER INFORMATION	
Operating System Support	Linux MADWIFI, WindowsXP, Windows2000
Advanced Mobility / QuickHandoff	WindowsXP/2000 Utility with Enhanced Mobility Driver from Ubiquiti
Cisco Support	CCX 4.0 Supported Driver/Utility also available from Ubiquiti

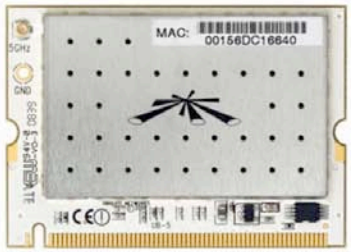
For help with MADWIFI or other Special Driver Support, Please e-mail support@ubnt.com

Figura 6. Datasheet Ubiquiti Super Range 5.

UBIQUITI NETWORKS

UB-5

HI-Reliability, Low-Cost 5GHz mini-PCI Radio



ENHANCED RF ESD/EMP PROTECTION AND SOLID PERFORMANCE

CARD INFORMATION	
Chipset	Atheros, 6th Generation, AR5414 with SuperA/Turbo Support
Radio Operation	IEEE 802.11a, 5GHz
Interface	32-bit mini-PCI Type IIIB
Operation Voltage	3.3VDC
Antenna Ports	Single u.fl
Temperature Range	-30C to +70C
Security	WPA, WPA2, AES-CCM & TKIP Encryption, 802.1x, 64/128/152bit WEP
Data Rates	6Mbps, 9Mbps, 12Mbps, 24Mbps, 36Mbps, 48Mbps. 54Mbps
TX Channel Width Support	5MHz / 10MHz / 20MHz / 40MHz
RoHS Compliance	YES

REGULATORY INFORMATION	
Wireless Modular Approvals	CE

RADIO OPERATING FREQUENCY 5.20-5.825GHz

TX SPECIFICATIONS					RX SPECIFICATIONS			
	DataRate	Avg.Power	Tolerance			DataRate	Sensitivity	Tolerance
802.11a OFDM	6Mbps	23 dBm	+/-1.5dB		802.11a OFDM	6Mbps	-94 dBm	+/-1.5dB
	9Mbps	23 dBm	+/-1.5dB			9Mbps	-93 dBm	+/-1.5dB
	12Mbps	23 dBm	+/-1.5dB			12Mbps	-91 dBm	+/-1.5dB
	18Mbps	23 dBm	+/-1.5dB			18Mbps	-90 dBm	+/-1.5dB
	24Mbps	23 dBm	+/-1.5dB			24Mbps	-86 dBm	+/-1.5dB
	36Mbps	21 dBm	+/-1.5dB			36Mbps	-83 dBm	+/-1.5dB
	48Mbps	19 dBm	+/-1.5dB			48Mbps	-77 dBm	+/-1.5dB
	54Mbps	18 dBm	+/-1.5dB			54Mbps	-74 dBm	+/-1.5dB

ADJUSTABLE CHANNEL SIZE SUPPORT (Increase Channel Capacity or Increase Throughput)			
5MHz	10MHz	20MHz	40MHz (Turbo)

CURRENT CONSUMPTION INFORMATION

TX CURRENT CONSUMPTION					RX CURRENT CONSUMPTION			
	DataRate	Current	Tolerance			DataRate	Current	Tolerance
802.11a OFDM	6Mbps	0.80 A	+/-100 mA		802.11a OFDM	6Mbps	300 mA	+/-100 mA
	9Mbps	0.80 A	+/-100 mA			9Mbps	300 mA	+/-100 mA
	12Mbps	0.80 A	+/-100 mA			12Mbps	300 mA	+/-100 mA
	18Mbps	0.80 A	+/-100 mA			18Mbps	300 mA	+/-100 mA
	24Mbps	0.80 A	+/-100 mA			24Mbps	300 mA	+/-100 mA
	36Mbps	0.70 A	+/-100 mA			36Mbps	300 mA	+/-100 mA
	48Mbps	0.60 A	+/-100 mA			48Mbps	300 mA	+/-100 mA
	54Mbps	0.50 A	+/-100 mA			54Mbps	300 mA	+/-100 mA

RANGE PERFORMANCE	
Indoor (Antenna Dependent):	Up to 150meters
Outdoor (Antenna Dependent):	Over 50km

DRIVER INFORMATION	
Operating System Support	Linux MADWIFI, WindowsXP, Windows2000
Advanced Mobility / QuickHandoff	WindowsXP/2000 Utility with Enhanced Mobility Driver from Ubiquiti
Cisco Support	CCX 4.0 Supported Driver/Utility also available from Ubiquiti
For help with MADWIFI or other Special Driver Support, Please e-mail support@ubnt.com	

Figura 7. Datasheet Ubiquiti UB-5.

WLM54AG 6A MINIPCI TECHNICAL SPECIFICATIONS

MODEL	WLM54AG (Wireless-AG)
CHIPSET	AR5413
SPEED (max)	54Mbps
OUTPUT POWER	
802.11a	6-24Mbps 20dBm 36Mbps 17dBm 48Mbps 16dBm 54Mbps - 13dBm
802.11b	1-11Mbps 20dBm
802.11g	6-24Mbps 20dBm 36Mbps 18dBm 48Mbps 17dBm 54Mbps 15dBm
POWER CONSUMPTION	
	1.8W
STANDARDS	
IEEE 802.11a:	54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps
IEEE 802.11b:	11Mbps, 5.5Mbps, 2Mbps, 1Mbps
IEEE 802.11g:	54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps, automatically fallback to 5.5Mbps, 2Mbps, 1Mbps
FREQUENCY RANGE	
IEEE 802.11b/g	2.412GHz ~ 2.462GHz (US & Canada) 2.412GHz ~ 2.472GHz (Europe) 2.412GHz ~ 2.484GHz (Japan)
IEEE 802.11a	5.15~5.35GHz, 5.725~5.850GHz (US & Canada) 5.15~5.35GHz, 5.47~5.725GHz (Europe) 4.90~5.00GHz, 5.03~5.091GHz, 5.15~5.25GHz (Japan)
NETWORK INTERFACE	
PCI interface v2.3 (Type III-B Mini PCI form factor)	
ANTENNA CONNECTOR	
Two antenna connectors (U.FL)	
MODULATION TECHNIQUES	
OFDM and DSSS OFDM: BPSK, QPSK, 16 QAM, 64QAM DSSS: DBPSK, DQPSK, CCK	
RECEIVER SENSITIVITY	
802.11a -90 dBm @ 6Mbps, -70 dBm @ 54Mbps 802.11b -92 dBm @ 1Mbps, -87 dBm @ 11Mbps 802.11g -90 dBm @ 6Mbps, -70 dBm @ 54Mbps	
OPERATING CHANNELS	
US and Canada	11 Channels
Europe	13 Channels
Japan	14 Channels
SECURITY	
64/128 Bit WEP, WPA/WPA2 , IEE802.1X Authentication	
CERTIFICATE	
FCC, CE	
RoHS COMPLIANCE	
Yes	
ENVIRONMENTAL SPECIFICATIONS	
Temperature	Operating -20℃ to 70℃ Storage -65℃ to 100℃
Humidity	Operating 5% to 95% (non-condensing)
DIMENSIONS & WEIGHT	
Dimensions	6.0cm x 4.5cm (L x B)
Weight	20 grams

Figura 8. Datasheet Compex WLM54AG.

4.1.3 Antenne

A seconda della tratta radio da realizzare, abbiamo utilizzato antenne patch da 23 dbi (**fig. 9**), parabole o grid da 29 dbi (**fig. 10** e **fig. 11**).

Si elencano le relative specifiche tecniche.

Frequency Range	5150-5850 MHz
Gain	23 dBi
Horizontal Beamwidth	10 °
Vertical Beamwidth	10 °
Mounting	Diameter 30-50 mm
VSWR	1 to 1,4
Impedance	50 ohm
Polarization	Horizontal or vertical
Output connector	NFemale type
Weight	1,8 kg
Overall dimensions (W x L)	390 x 430 mm

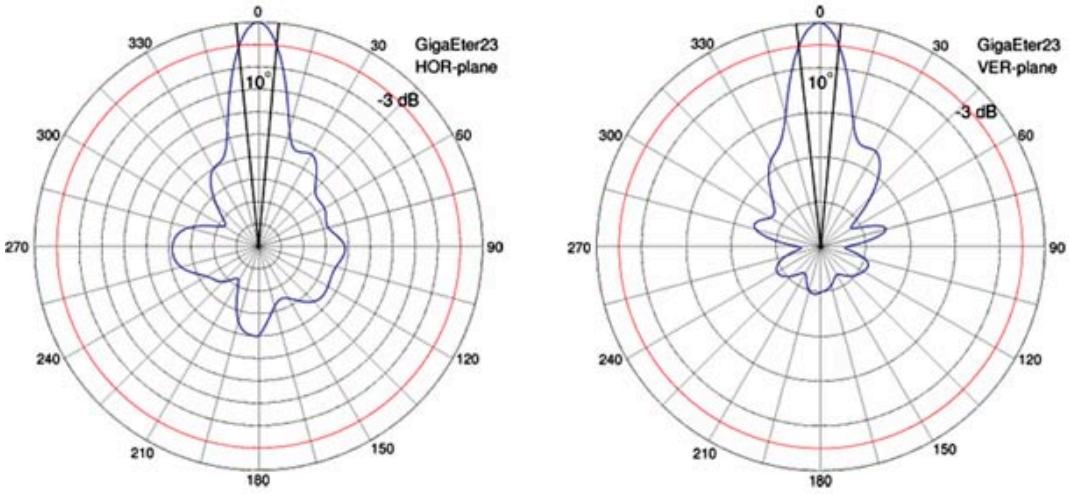


Figura 9. Datasheet antenna patch 23 dbi.

Frequency Range	5470-5725 MHz
Gain	29,5 dBi
Beamwidth	V:6 ° / H:4°
Wind loading	90 m/s
Mounting	40-60 mm
VSWR	<= 1,5
Impedance	50 ohm
Polarization	Horizontal and Vertical
Output connector	NFemale Type
Weight	4,5 kg (without bracket)
Dimensions	600 x 900 mm

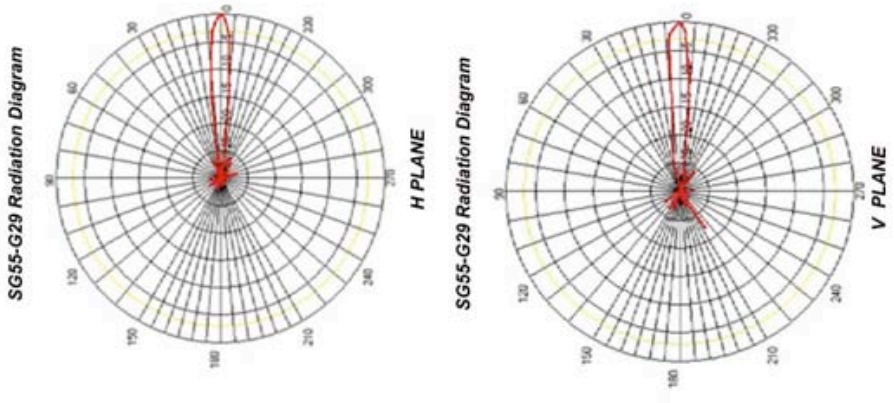


Figura 10. Datasheet antenna grid 29 dbi.

Frequency Range	5450-5900 MHz
Gain	29,5 dBi
Beamwidth	V:5.8 ° / H:5.8°
Polarization	Horizontal and Vertical
Mounting	40-60 mm
VSWR	1 to 1,5
Impedance	50 ohm
Mounting Diameter	38-51 mm
Output connector	NFemale Type
Weight	7,8 kg
Dimensions	750 x 735 x 285 mm

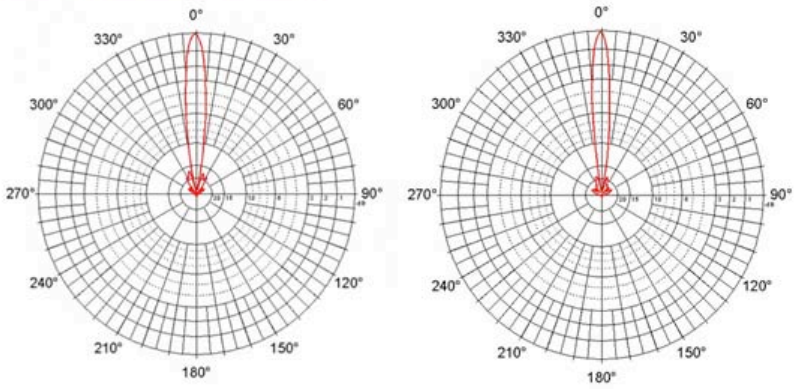


Figura 11. Datasheet parabola 29 dbi.

4.2 Software RouterOS

Mikrotik RouterOS è il sistema operativo delle RouterBoard Mikrotik.Come già detto, può essere installato su un pc trasformandolo in un router con tutte le funzionalità necessarie – routing, firewall, bandwidth management, wireless access point, backhaul link, hotspot gateway, VPN server e molto altro.

RouterOS è un sistema operativo stand-alone basato sul kernel Linux 2.6, e lo scopo di Mikrotik è quello di fornire tutte queste funzionalità attraverso una semplice e veloce installazione ed una facile interfaccia utente.

RouterOS supporta computer multi-core e multi-CPU e può funzionare anche sulle schede madri di ultima generazione basate su processori multicore. Può essere installato su dispositivi di storage IDE, SATA, USB e quindi HDD, CF, SD e SDD. Necessita di almeno 64 MB di spazio disco.

RouterOS supporta inoltre molteplici interfacce di rete comprese le ultime interfacce ethernet a 10 Gbit, wireless card 802.11/a/b/g/n e modem 3G.

RouterOS supporta diversi metodi di configurazione : accesso locale con tastiera e monitor, console seriale, Telnet, uno strumento personalizzato di configurazione GUI chiamato Winbox (**fig. 12**), una semplice interfaccia web o tramite accesso sicuro SSH (**fig.13**).

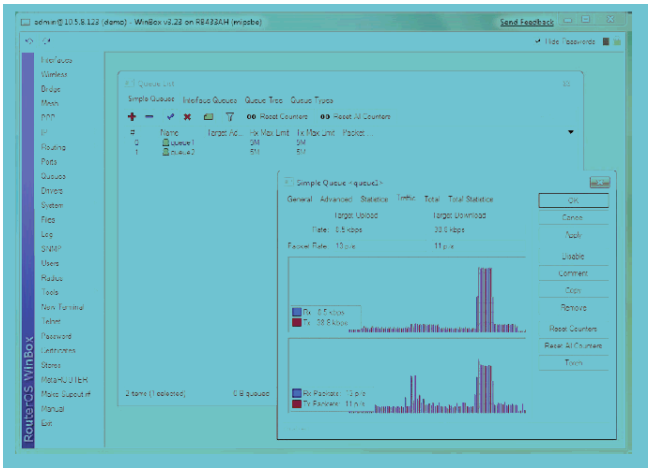


Figura 12. Finestra Winbox di configurazione degli apparati.

Nel caso in cui non vi è l'accesso locale, e vi è un problema con le comunicazioni a livello IP, RouterOS supporta anche un livello di connessione basata su MAC.

RouterOS dispone di una potente ma facile interfaccia di configurazione a riga di comando con capacità di script integrato.

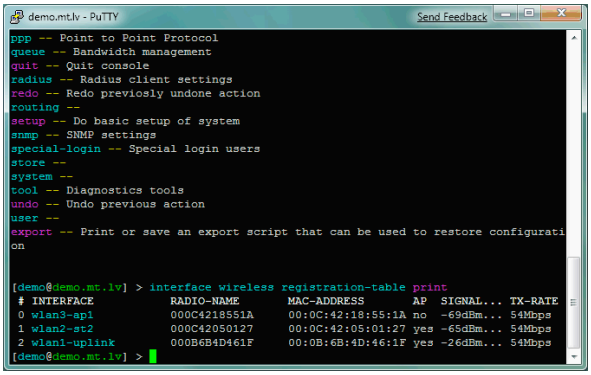


Figura 13. Terminale di configurazione apparati.

Il firewall (**fig.14**) implementato in RouterOS realizza il filtraggio dei pacchetti e quindi fornisce funzioni di sicurezza, che vengono utilizzati per gestire il flusso dati da e attraverso il router. Insieme con il Network Address Translation consente di prevenire l'accesso non autorizzato alle reti direttamente connesse. RouterOS dispone di un firewall stateful, il che significa che esegue stateful packet inspection e tiene traccia dello stato delle connessioni che lo attraversano.

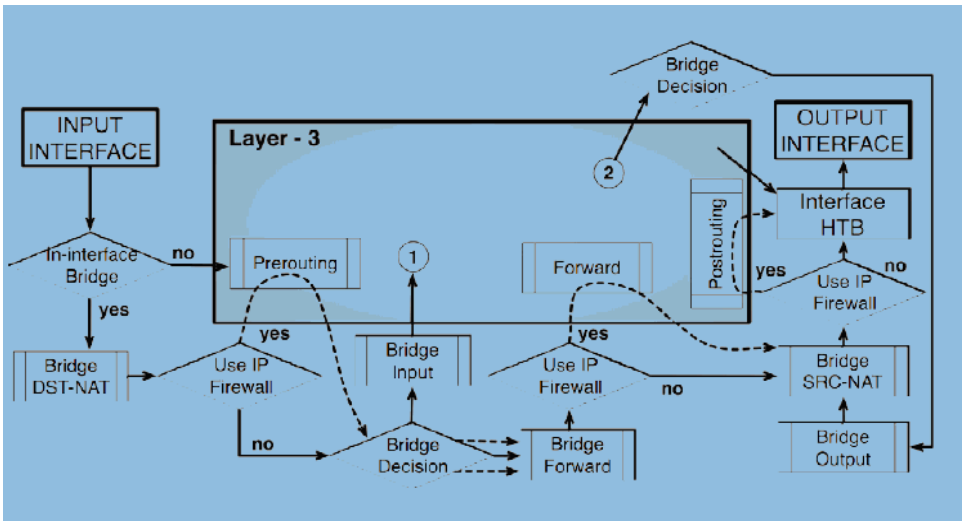


Figura 14. Schema a blocchi NAT/firewall/Routing RouterOS.

RouterOs supporta il routing statico e una moltitudine di protocolli di routing dinamico (**fig. 15**):

Per IPv4 supporta RIP v1 e v2, OSPF v2, BGP v4
Per IPv6 supporta RIPng, OSPF v3 e BGP

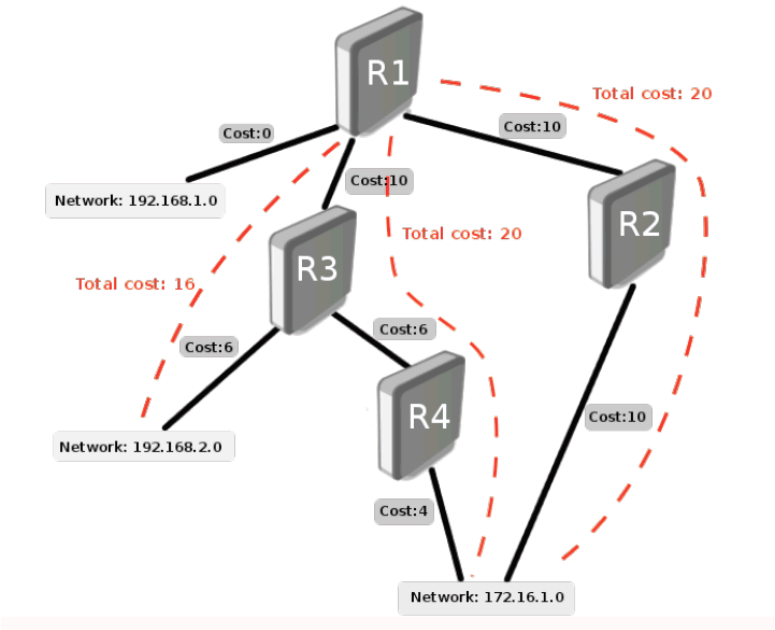


Figura 15. Mappa di rete con relativi costi dei collegamenti.

Per stabilire connessioni sicure attraverso reti aperte o internet, oppure per connettere postazioni remote con link crittografati, RouterOs supporta vari protocolli che realizzano tunnel VPN (**fig. 16**):

- Ipsec – tunnel and transport mode, certificate or PSK, AH and ESP security protocols
- Point to point tunneling (OpenVPN, PPTP, PPPoE, L2TP)
- Advanced PPP features (MLPPP, BCP)
- Simple tunnels (IPIP, EoIP)
- 6to4 tunnel support (IPv6 over IPv4 network)
- VLAN – IEEE802.1q Virtual LAN support, Q-in-Q support

• MPLS based VPNs

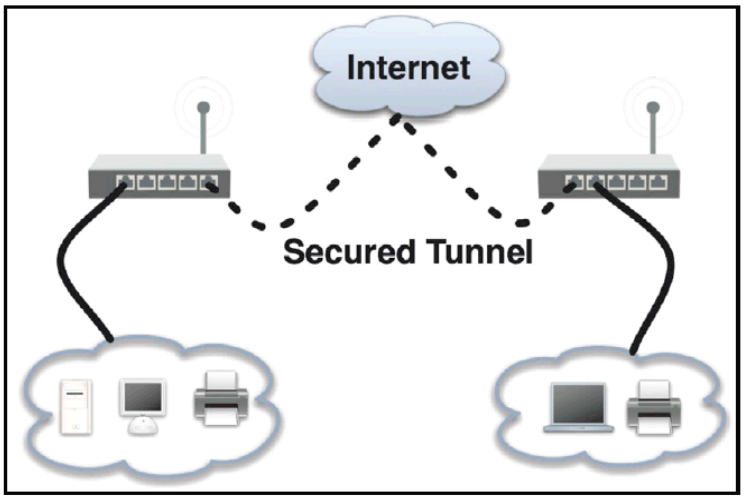


Figura 16. Schema di un tunnel VPN.

RouterOs supporta una varietà di tecnologie wireless che vanno dalla capacità di estendere una copertura Wifi in un'abitazione fino alla realizzazione di reti mesh che possono coprire diversi centri abitati. Alcune tecnologie supportate sono:

• IEEE802.11a/b/g/n wireless client and access point
• Nstreme and Nstreme2 proprietary protocols
• Client polling
• RTS/CTS
• Wireless Distribution System (WDS)
• Virtual AP
• WEP, WPA, WPA2 encryption
• Access control list
• Wireless client roaming
• WMM
• MME wireless routing protocol
• HWMP+ Wireless MESH protocol.

In ultimo, RouterOs supporta il Quality of Service (QoS). Ciò significa che il router può priorizzate il traffico di rete limitando ad esempio il data rate per certi indirizzi ip, subnets, protocolli, porte e altri parametri; assegnare priorità al flusso di determinate pacchetti piuttosto che altri; condividere il traffico disponibile egualmente tra più utenti (**fig. 17**) o a seconda del carico del canale.

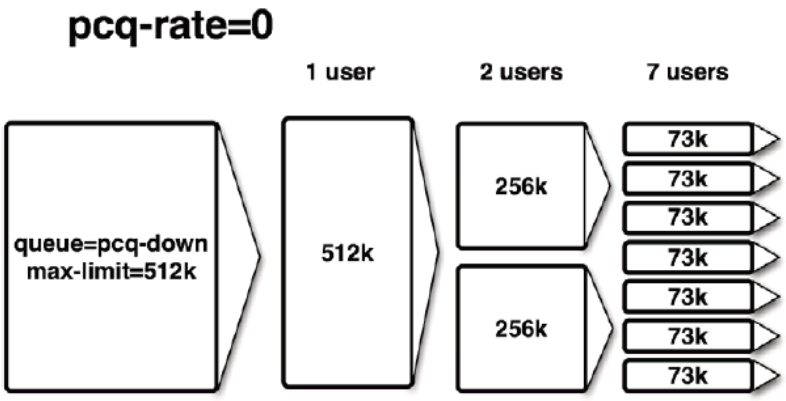


Figura 17. Esempio ripartizione banda con QoS.

5. Layout di rete

Il progetto di rete realizzato è quello mostrato in **fig.18**. Ogni nodo della rete, contraddistinto dalla sigla "STxx", rappresenta un router remoto ciascuno equipaggiato con uno o più apparati radio per consentirgli l'interconnessione con i siti adiacenti ed una eventuale ridondanza del link radio.

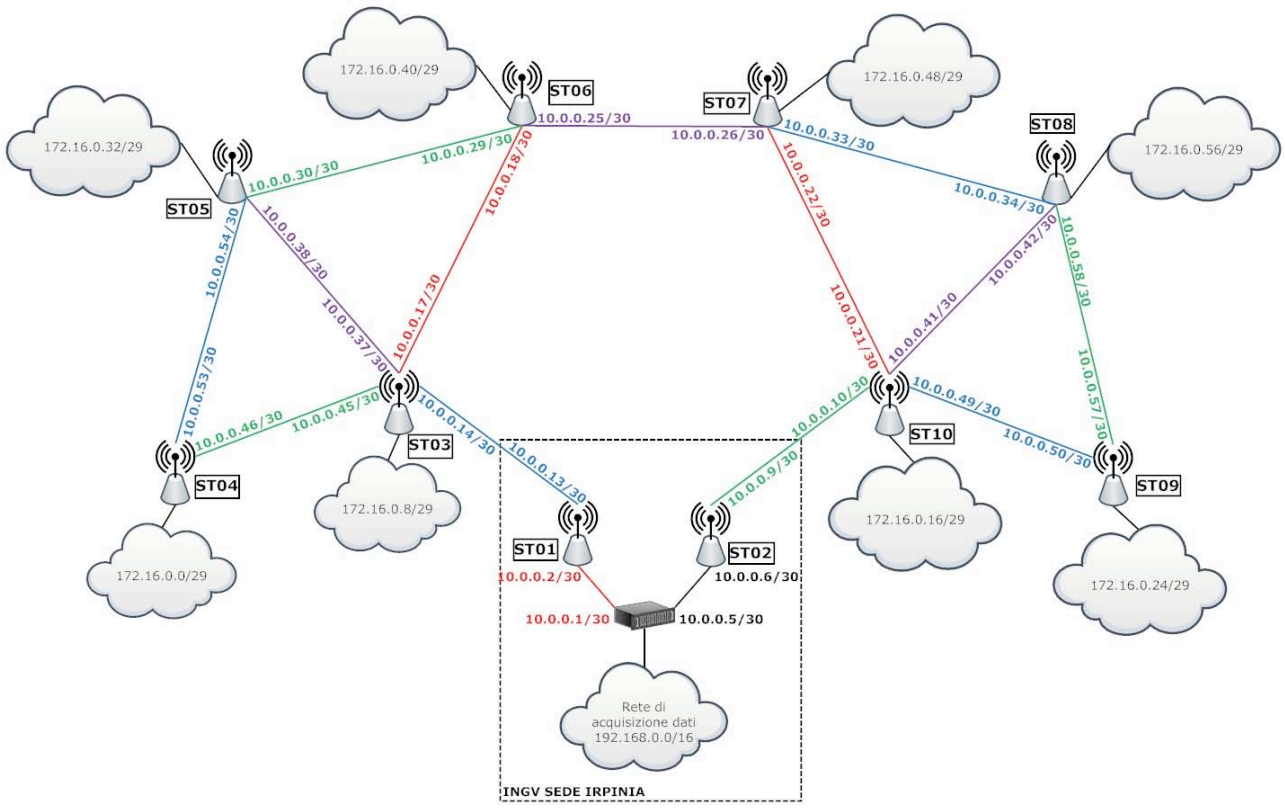


Figura 18. Progetto di rete mesh wi-fi realizzato per l'acquisizione dei dati sismici e gps.

5.1 Piano di indirizzamento

La rete mesh wireless è stata realizzata con un piano di indirizzamento IP composto dalle seguenti sottoreti:

- Collegamenti dorsali Wi-Fi punto-punto realizzate mediante reti private classless **10.x.x.x/30**
- Rete privata **192.168.0.0/16** che ospita i server di acquisizione dati NaqsServer, Seedlink Server, Earthworm Server, Spider Server presso la Sede Irpinia dell'INGV
- Reti private classless **172.16.x.x/29** che interconnettono presso il sito remoto acquisitore sismico (GAIA2), gps (Leica 1200) ed eventuali altri dispositivi.

5.2 Sicurezza collegamenti wireless

Le onde elettromagnetiche hanno intrinsecamente una grande capacità di diffondersi in tutte le direzioni con una portata relativamente grande. È quindi molto difficile arrivare a confinare le emissioni di onde radio in un perimetro limitato. La conseguenza principale di questa "propagazione selvaggia" delle onde radio è la facilità che può avere una persona non autorizzata di ascoltare la rete.

Per la messa in sicurezza della rete mesh realizzata abbiamo utilizzato i seguenti accorgimenti:

- **Filtraggio mac address**: solo i dispositivi conosciuti possono connettersi agli Access Point
- Autenticazione e crittografia dei dati mediante protocollo **WPA2-PSK AES**
- **Firewall** per la protezione della rete di acquisizione dati 192.168.0.0/16 e dei singoli Access Point

6. Pianificazione e fattibilità dei link radio

La realizzazione di un collegamento wi-fi necessita di un'attenta analisi dei siti nei quali installare gli apparati.

La fattibilità del collegamento Wi-Fi richiede l'analisi dei seguenti parametri:

- Coordinate GPS dei punti in cui andranno installati gli apparati radio;
- Visibilità ottica tra i punti da interconnettere;
- Analisi dell'orografia del terreno (eventuali ostacoli lungo la tratta potrebbero inficiare la bontà del segnale);
- Caratteristiche tecniche apparati radio (Rx Sesitivity, tx power …);
- Caratteristiche tecniche delle antenne da installare (gain, diagramma di irradiazione, polarizzazione);
- Attenuazioni dovute a componenti passivi (cavi, connettori, pig-tail);
- Elevazione delle antenne dal suolo.

Per la simulazione del link è stato utilizzato "Radiomobile", un software elaborato da un radioamatore francese che utilizza un modello predittivo di propagazione noto come Longley-Rice model e sviluppato presso US Institute for Telecommunications Science (ITS). Tale software ci ha permesso di predire le prestazioni del sistema radio ed effettuare la simulazione della propagazione del segnale, consentendoci a priori di scegliere la giusta combinazione radio-antenna da utilizzare.

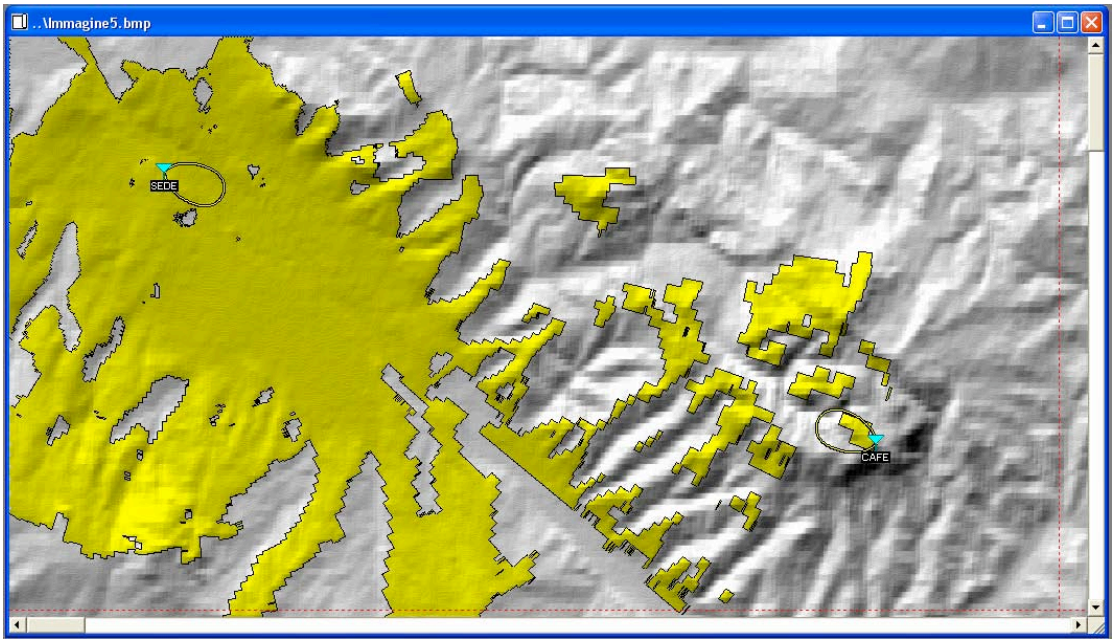


Figura 19. Analisi di visibilità.

Il software utilizza dati altimetrici della superficie terrestre rilevati dallo spazio e rilasciati dalla NASA; i tipi di dati che possono essere caricati sono GTOPO30, GLOBE e DTED livello 0 a 30 arcosecondi, SRTM e DTED level 1 a 3 arcosecondi, DTED livello 2 e SRTM a 1 arcosecondo, e BIL ad ogni risoluzione.

Attraverso il software è possibile avere una stima della visibilità, come mostrato nella **fig. 19,** in cui viene evidenziato in giallo ciò che un osservatore, situato nel punto SEDE ad un'altezza di 25m, può vedere.

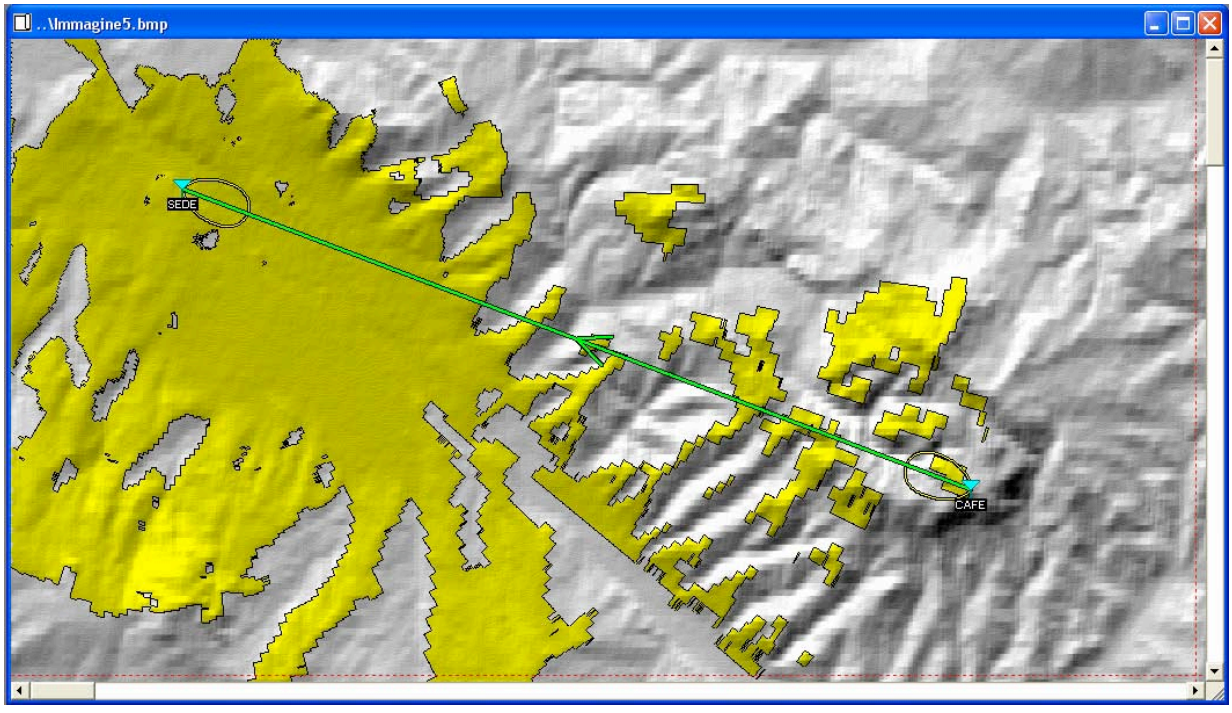


Figura 20. Link radio fattibile.

Dopo aver inserito i dati degli apparati si otterrà la simulazione della propagazione del segnale, con i risultati mostrati nella **fig. 20** in cui è evidente che il link è fattibile in quanto il collegamento tra le due stazioni è di colore verde; in caso contrario avremmo avuto il link di colore rosso (**fig. 21**)

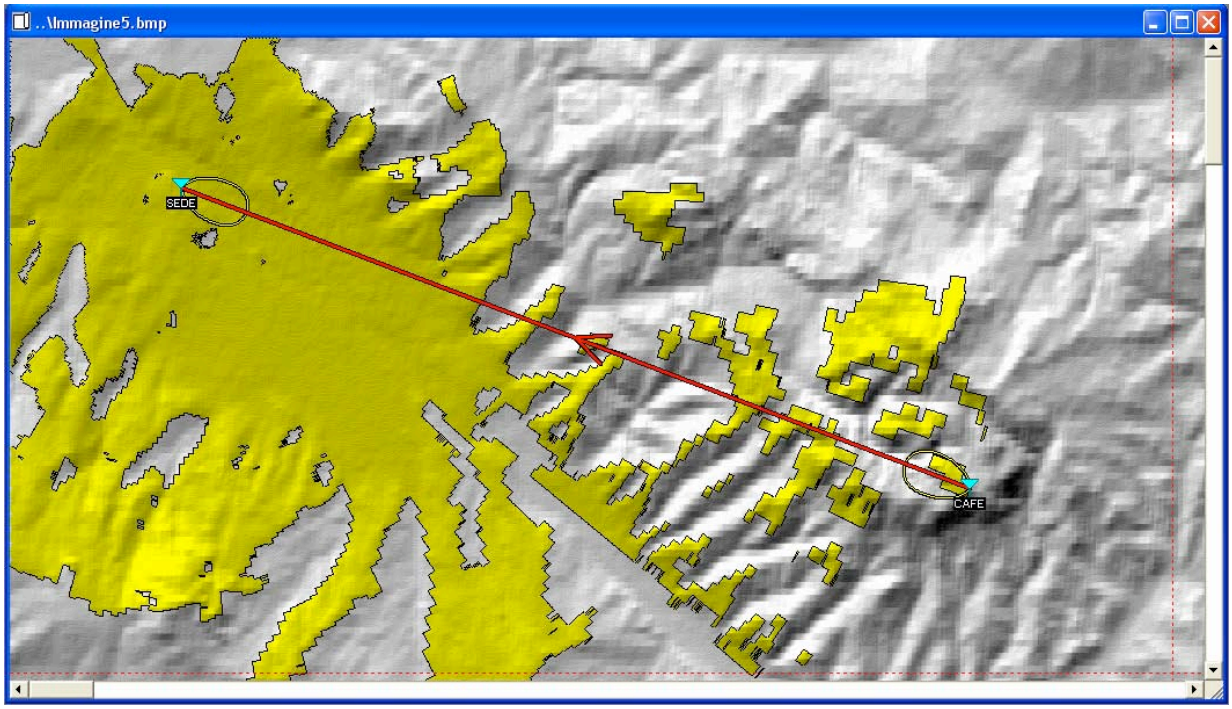


Figura 21. Link radio non realizzabile.

Il software permette di visualizzare la tratta andando a costruire un profilo della stessa come mostrato in **fig. 22**.

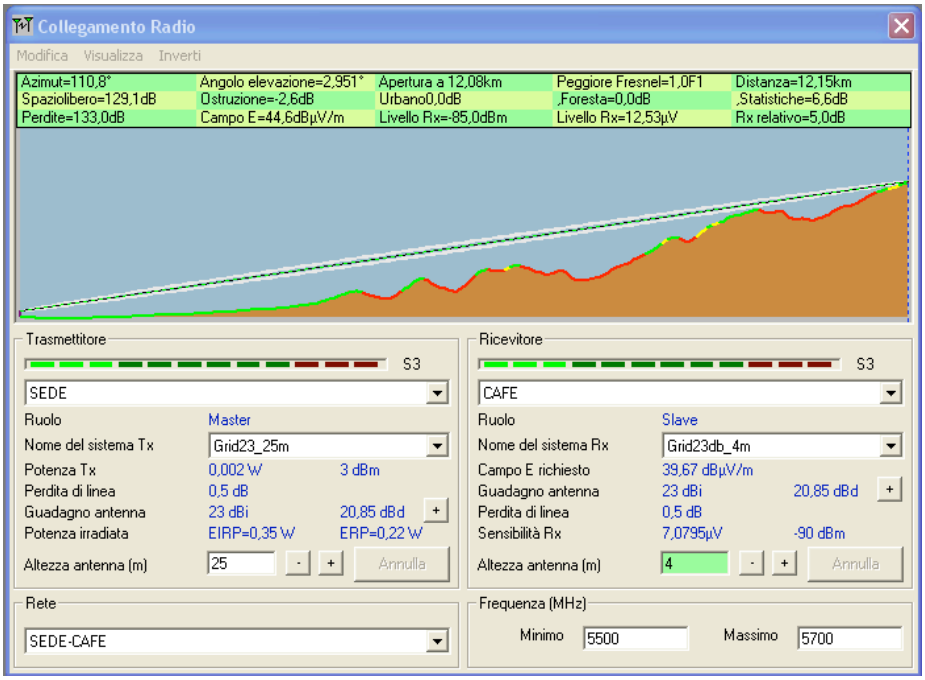


Figura 22. Profilo della tratta SEDE-CAFE (Carife).

Inoltre è possibile visualizzare i risultati in forma testuale in cui viene evidenziato l'orientamento che devono avere le antenne per effettuare il link (**fig. 23**).

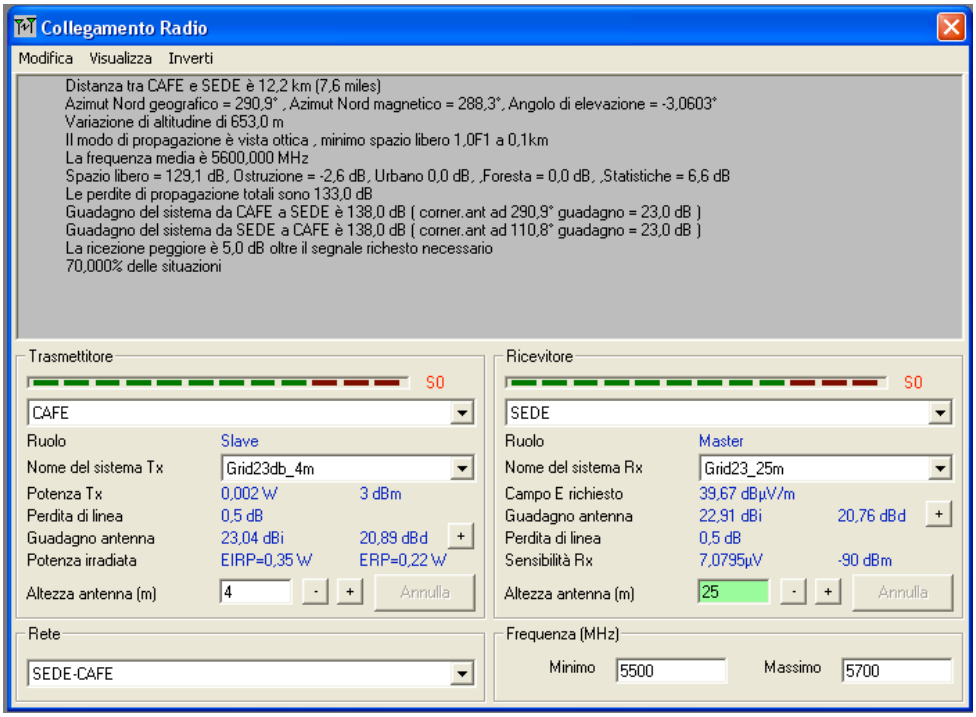


Figura 23. Risultato testuale della simulazione del link radio.

Infine è possibile esportare i dati della tratta da eseguire su Google-earth per effettuare un ulteriore controllo sull'orografia della superficie terrestre come mostrato in **fig. 24**.

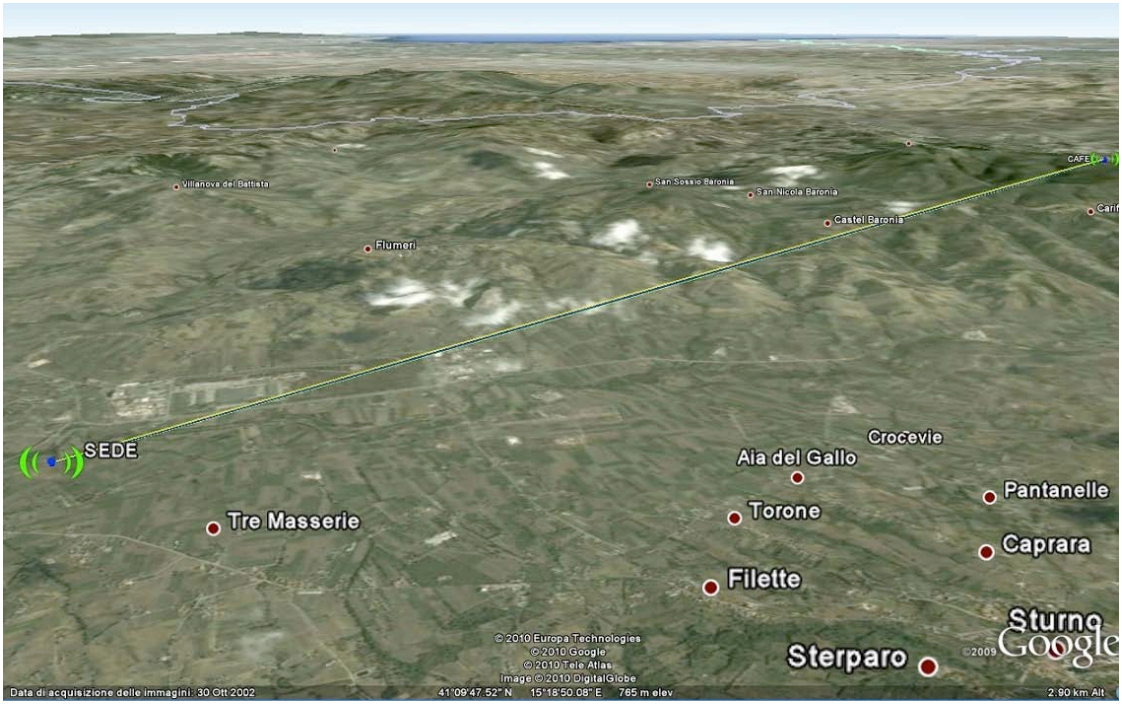


Figura 24. Simulazione della tratta radio su Google Earth.

7. Alimentazione siti e stima dei consumi

7.1 Alimentazione RouterBoard e strumentazione presso sito remoto

Le RouterBoard utilizzate per la realizzazione della rete sono alimentate tramite tecnologia Power over Ethernet (PoE) utilizzando come mezzo conduttore il cavo ethernet.

L'alimentazione degli apparati utilizza cavi UTP Cat. 5 (10-100 BaseT) in cui due coppie forniscono tensione mentre le restanti sono utilizzate per la trasmissione e la ricezione dei dati. Per evitare cadute di tensione elevate si utilizzano 2 coppie in modo da aumentare la sezione dei conduttori.

L'alimentazione tramite tecnologia PoE prevede l'utilizzo di un particolare dispositivo, chiamato "injector", che immette tensione sulle due coppie di cavi libere. L'injector (**fig. 25**) ha un collegamento alla rete elettrica e due prese ethernet di cui una connessa alla rete LAN e l'altra all'apparato PoE.

Figura 25. Vari di PoE injector.

Nel caso di alimentazione da rete pubblica si dovrà predisporre un quadro di bassa tensione (realizzato in laboratorio) per la trasformazione della tensione da alternata 230V a continua 12V e un quadro di bassissima tensione.

Il quadro di bassa tensione sarà assemblato con i seguenti dispositivi:

- Interruttore magnetotermico differenziale 2x10A – 4,5kA – Idiff=0,03A – immune alle correnti da fulmine;
- Blocco per autoripristino dell'interruttore magnetotermico-differenziale in caso di scatto intempestivo dello stesso;
- Alimentatore switching per trasformare e raddrizzare la tensione che poi verrà utilizzata per alimentare gli apparati;
- Scaricatori di sovratensione;

Ai fini della sicurezza degli operatori è di fondamentale importanza accertarsi che il valore della corrente di intervento dell'interruttore differenziale sia coordinato con il valore della resistenza di terra dell'impianto realizzato in loco.

Il quadro di alimentazione in bassissima tensione (**fig. 26**) dovrà essere realizzato con i seguenti componenti:

- Regolatore di carica, per il corretto controllo di carica e scarica delle batterie;
- Batterie, per avere una riserva di energia in caso di black-out;
- Injector, per alimentare gli apparati di trasmissione;

- Morsettiera di alimentazione, per i dispositivi presenti sulla stazione (GAIA/GAIA2, Ricevitore GPS, PoE etc….).

Figura 26. Quadro di bassissima tensione.

Inoltre si dovrà verificare che ognuno dei dispositivi collegati all'alimentazione siano dotati di una protezione da sovracorrenti, in caso contrario si dovranno installare dei fusibili appropriati ove necessario.

7.2 Stima dei consumi

Per un corretto dimensionamento del sistema di alimentazione è necessario conoscere l'effettivo consumo di ogni singolo apparato da installare.

Di seguito si riportano i consumi dei dispositivi utilizzati:

- RouterBOARD 433 3W
- Modulo radio MiniPCI WLM54AG 2,5W
- Acquisitore GAIA2 5,4W
- Acquisitore GPS Leica GPS1200+ 4,6W
- Regolatore di carica Prostar PS30 (autoconsumo) 0,3W

La RouterBOARD 433 ha la capacità di gestire un numero massimo di tre radio; in caso ci sia la necessità di utilizzare più radio nella stessa installazione verranno impiegate più RouterBOARD 433.

In base ai dati esposti è possibile dedurre i consumi massimi che una stazione potrà avere:

- Stazione **tipo A** con n°1 radio, acquisitore GAIA2, GPS: 17,5W
- Stazione **tipo B** con n°2 radio, acquisitore GAIA2, GPS: 20W
- Stazione **tipo C** con n°3 radio, acquisitore GAIA2, GPS: 22,5W
- Stazione **tipo D** con n°4 radio, acquisitore GAIA2, GPS: 28W

7.2.1 Moduli fotovoltaici

I moduli fotovoltaici utilizzati saranno del tipo monocristallino:

- Corrente corto circuito (Isc) 8,65A
- Corrente di picco (Im) 7,9A
- Max syst volt 750V
- NOCT (Esti 503) 43°C
- Potenza max (Pm) 140W
- Tensione circuito aperto (Voc) 23V
- Tensione max (Vm) 17,73V
- Tipo HELIOS H1540
- Efficienza 11,9%

7.2.2 Accumulatori

Gli accumulatori più adatti per l'uso in impianti fotovoltaici stand-alone devono avere le seguenti caratteristiche:

- elevata efficienza;
- lunga durata;
- buona resistenza alle escursioni termiche;
- bassa manutenzione;
- basso livello di autoscarica.

La scelta ricade su batterie piombo acido del tipo regolate da valvola con elettrolito immobilizzato in forma gelatinosa.

Sono stati utilizzati questi tipi di accumulatori al fine di ridurre il rischio di fuoriuscita di elettrolita e quindi rischio di corrosione ed inalazione da parte dell'operatore.

In base ai consumi sopra citati viene indicato il dimensionamento dell'impianto (negli esempi di seguito si tiene conto dei dati climatici del centro Italia, quindi spostandosi da nord a sud il dimensionamento della stazione potrebbe variare ed è quindi opportuno rivalutare questo dato).

Nel caso di stazione con alimentazione da rete elettrica sarà utilizzato un numero di batterie inferiori rispetto alla stazione in isola, supponendo che un black-out causato dal servizio pubblico raramente supera le 24h.

TIPO STAZIONE	CAPACITÀ BATTERIE
Tipo A	90 Ah
Tipo B	100 Ah
Tipo C	110Ah
Tipo D	135Ah

Diverso invece il caso in cui le stazioni saranno del tipo in isola e quindi l'unica fonte di energia sarà data dal sole (fonte aleatoria); in questo caso bisogna cercare il giusto equilibrio tra giorni di autonomia della stazione e quantità di moduli fotovoltaici ed accumulatori da installare. In media verrà calcolata su ogni stazione un'autonomia in completa assenza di sole di circa 4 giorni.

TIPO STAZIONE	QUANTITÀ PANNELLI	CAPACITA' BATTERIE
Tipo A	3	350 Ah
Tipo B	3	390 Ah
Tipo C	3	440Ah
Tipo D	3	550Ah

In **fig. 27** e **fig. 28** sono riportati gli schemi dei quadri realizzati rispettivamente per una stazione con alimentazione da rete elettrica e una stazione in isola.

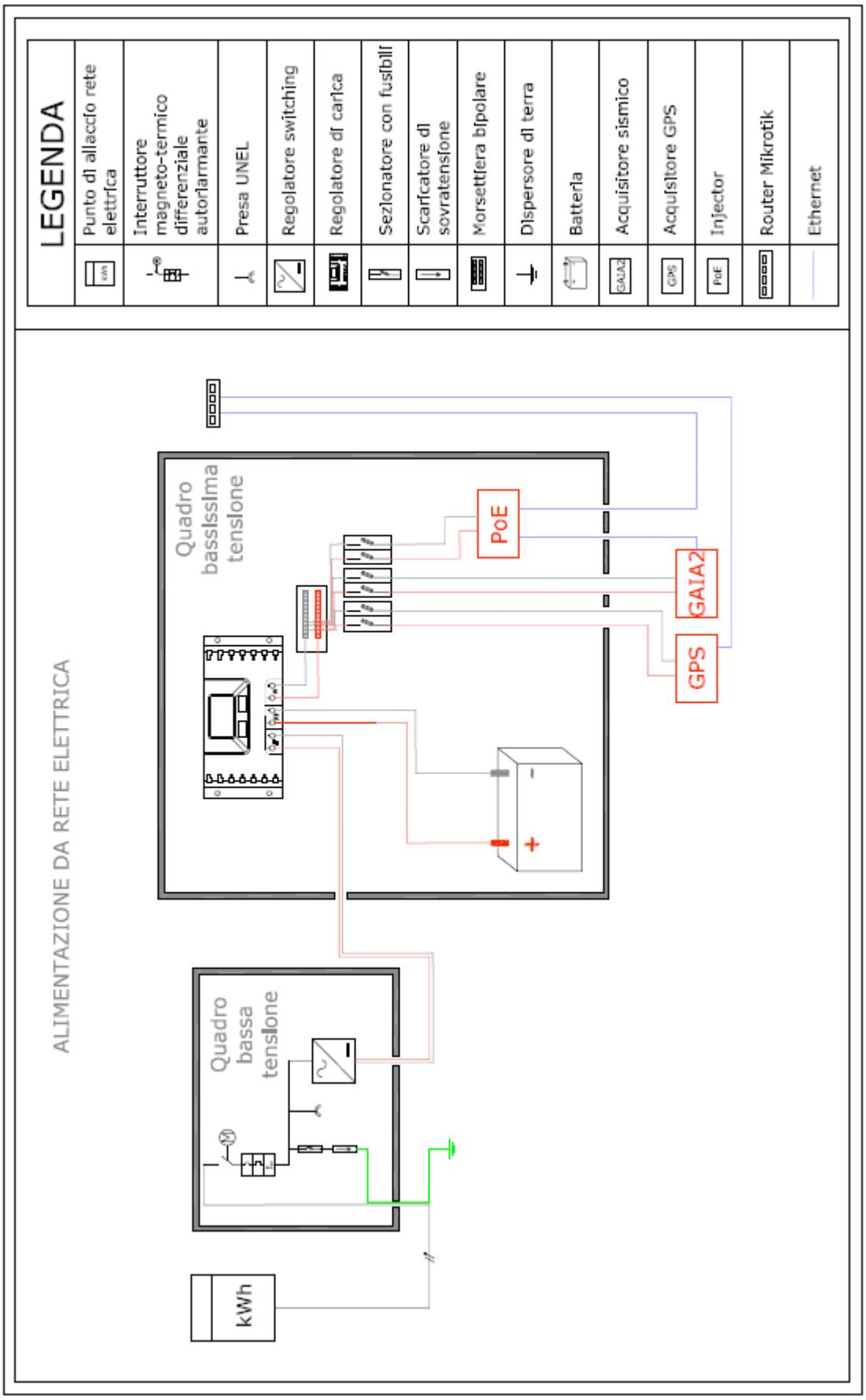


Figura 27. Schema alimentazione da rete elettrica.

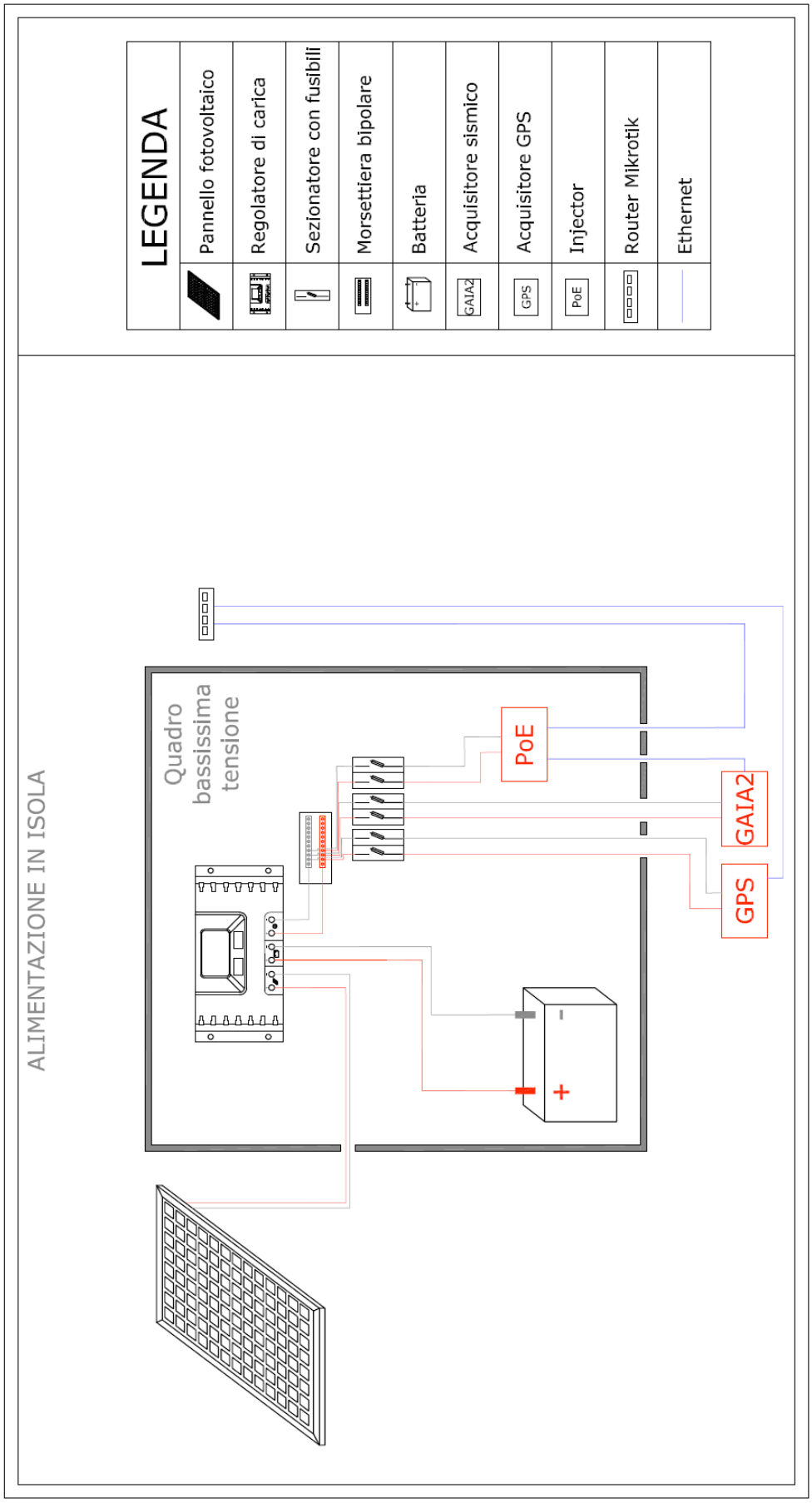


Figura 28. Schema di alimentazione in isola.

8. Gestione e manutenzione della rete: the Dude

The Dude (**fig. 29**) è una applicazione sviluppata da MikroTik per migliorare la gestione della rete. In automatico The Dude fa la scansione di tutta la rete alla ricerca di tutti gli host connessi, disegna una mappa funzionale della stessa, alla quale è possibile sovrapporre una carta topografica reale del territorio, e monitorizza tutti i servizi attivi su quegli host (ping, web, mail, mysql, ssh, e tanto altro). Lasciato in esecuzione su di una macchina direttamente connessa all'infrastruttura di rete consente di monitorare velocemente lo stato della rete semplicemente osservando i colori delle icone dei vari apparati che in caso di interruzione di una tratta da verdi diventano gialli oppure rossi.

Consente, inoltre, di inviare un allarme nel caso in cui uno dei servizi monitorati non fosse disponibile.

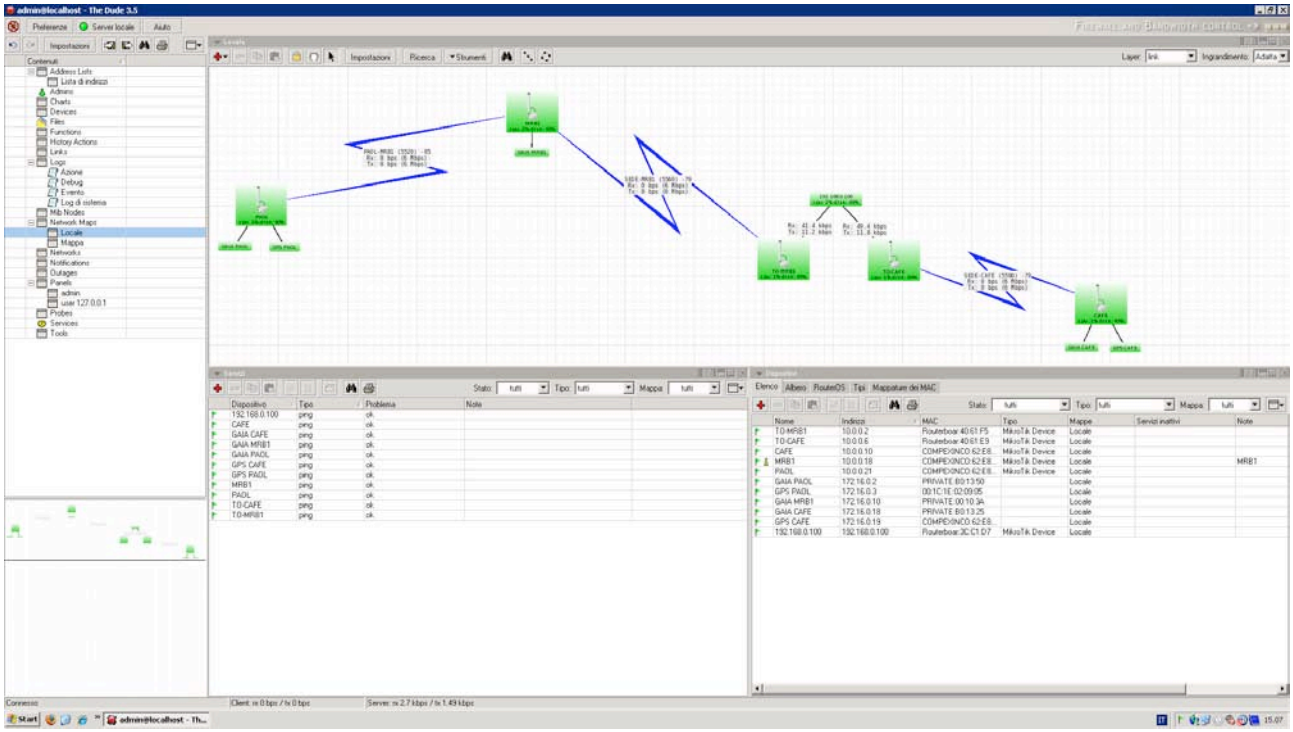


Figura 29. Screenshot del software di gestione "The Dude".

Alcune delle caratteristiche principali di The Dude comprendono:

- The Dude è assolutamente gratuito;
- Ricostruisce ogni tipologia e marca di host connesso;
- Monitorizza e notifica qualunque link e dispositivo;
- Permette l'uso di icone in formato SVG, e supporta icone personalizzate;
- Facilità di installazione e uso;
- Consente di disegnare la propria mappa aggiungendo i dispositivi che vogliamo;
- Supporta SNMP, ICMP, DNS e TCP;
- Controllo del carico e della banda passante dei link;
- Accesso diretto ai servizi degli host remoti, evitando quindi di dover memorizzare, su altri supporti, l'indirizzamento e le sottoreti di tutti i dispositivi interconnessi;
- Supporta altri The Dude server e client locali;

- È dotato di un web server integrato in grado di esportare sul web lo stato della rete in real time;
- Funziona sotto Windows, Linux (con Wine) e MacOS (con Darwine)
- Ha il miglior rapporto qualità prezzo comparato con i software concorrenti (è gratis!)

9. Vantaggi e svantaggi

Per quanto riguarda i vantaggi dell'utilizzo di tale tecnologia di trasmissione è subito evidente che estendere tale rete sul territorio porta all'abbattimento totale dei costi di connettività con forti ripercussioni economiche sul bilancio dell'Ente. La diffusione, legata alla sempre maggiore presenza di produttori, ha creato una notevole concorrenza abbassando di molto i prezzi iniziali di questa tecnologia. Attualmente il costo di un nuovo nodo di rete, completo di tutte le componenti necessarie (Routerboard, radio, antenna, cassetta connettori e cavi vari...) è di circa 250/300 €.

Altro non trascurabile vantaggio è legato alla capacità di banda che il sistema riesce a garantire, pari a 54 oppure 108 Mbit.

La possibilità di realizzare reti magliate, grazie all'utilizzo di particolari protocolli di instradamento dei pacchetti, fa si che non ci siano interruzioni di servizio anche a seguito di un link radio danneggiato.

La velocità di intervento in caso di guasto costituisce un ulteriore vantaggio: un repository raccoglie il file di configurazione di ogni singolo nodo della rete consentendo a qualunque operatore (anche inesperto) di essere in grado di sostituire l'apparato guasto ed importare, nel nuovo, la configurazione salvata.

Come qualsiasi altra tecnologia anche quella Wi-Fi è affetta da svantaggi.

Il link radio per estendersi a grandi distanze necessita che ci sia perfetta vista ottica tra gli apparati dei vari nodi della rete.

Il tempo di latenza delle schede wi-fi è leggermente superiore a quelle basate su cavo con una latenza massima nell'ordine di 1 - 3 ms (comunque questo particolare è trascurabile, a differenza delle connessioni GPRS/UMTS che hanno latenze nell'ordine di 200 - 400 ms).

Uno svantaggio delle connessioni wi-fi 802.11a può essere la stabilità del servizio legata a disturbi ed interferenze sul segnale. Nel nostro caso, vista la scelta dei siti, che generalmente ricade su zone molto distanti da centri densamente abitati e/o industrializzati, ciò difficilmente rappresenta un problema.

10. Conclusioni

La progettazione della rete mesh è stata avviata a fine dicembre 2009. Dal mese di Gennaio 2010 sono iniziati i lavori di predisposizione degli apparati presso la sede Irpinia dell'INGV (**fig. 30** e **31**); la fase successiva ci ha visti impegnati nell'installazione degli apparati radio presso i siti gps e sismici remoti (**fig. 32** e **33**).

Figura 30. Foto della sede Irpinia INGV e posizionamento apparati radio.

Figura 31. Palo di 25 metri posizionato nella sede Irpinia.

Figura 32. Tipica stazione remota – PAOL.

La **fig. 34** mostra lo stato della rete ad oggi; La copertura Wi-Fi è stata estesa a tutti i siti già presenti nell'area circostante la sede fatta eccezione per PAOL (Paolisi) che costituisce una nuova installazione.

L'infittimento della rete sismica e geodetica nazionale ci consentirà, in futuro, di disporre di ulteriori nodi Wi-Fi che contribuiranno alla realizzazione del progetto di rete magliata descritto nella **fig. 18**.

Nei primi due mesi di attività non abbiamo riscontrato alcuna interruzione di servizio riguardo i link radio neppure in concomitanza di eventi climatici avversi che più volte si sono verificati.

Nel complesso il sistema è molto robusto e affidabile.

Figura 33. Antenne installate presso il sito MRB1.

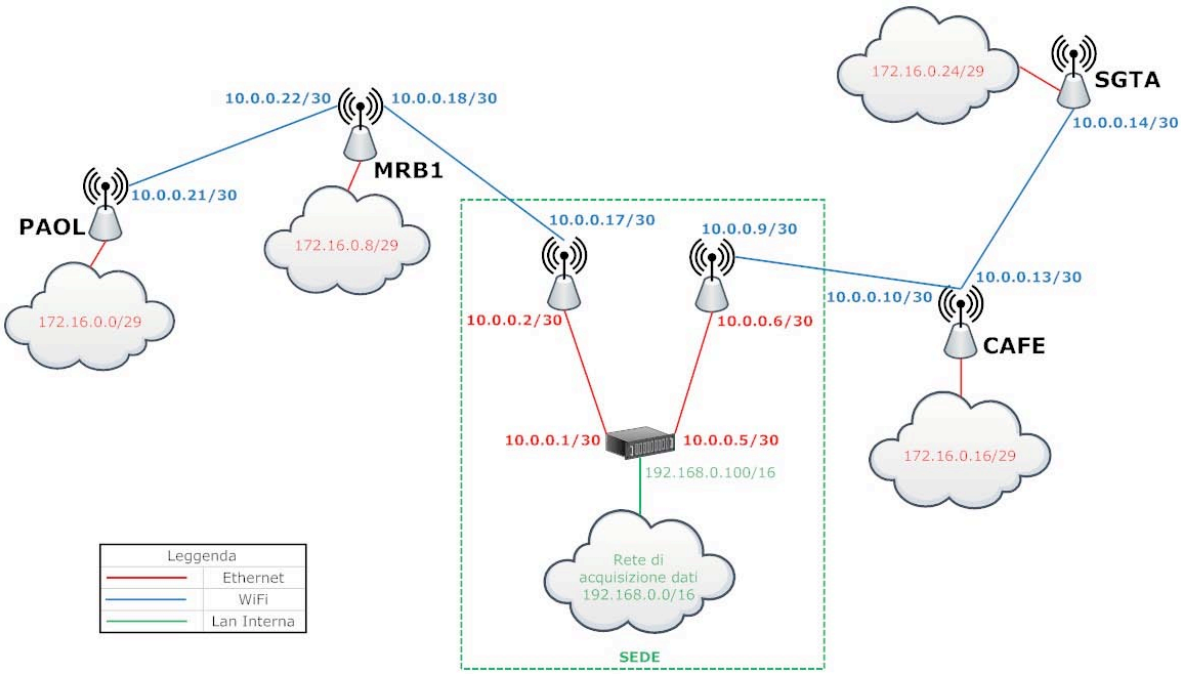


Figura 34. Stato attuale della rete.

Ringraziamenti

Gianpaolo Cecere – per aver creduto nel progetto Wi-Fi dandoci la possibilità di conseguire le certificazioni Mikrotik e per averci messo a disposizione le dovute risorse finanziarie

Raffaele Moschillo – per il supporto prestato alle analisi di visibilità dei siti remoti

Giovanni De Luca - per l'impegno profuso nell'inventariare tutte le componenti hardware della rete

Franco Migliari – per la minuziosa ricerca siti nell'ottica dei futuri sviluppi della rete

Bibliografia

Mario Baldi, Pietro Nicoletti. Internetworking

Gazzetta Ufficiale 69 del 20-7-2002- Suppl. Ordinario n.146. Piano Nazionale di Ripartizione delle

Frequenze Decreto 8 Luglio 2002 del Ministero delle Comunicazioni.

Gazzetta Ufficiale 273 del 21-11-2008 – Suppl. Ordinario n.255. Nuovo Piano Nazionale di Ripartizione delle Frequenze (PNRF).

Mikrotik on line documentation - http://wiki.mikrotik.com/wiki/Main_Page

Gazzetta Ufficiale N. 50 del 01 Marzo 2003 - DECRETO 20 febbraio 2003 Modifica del Piano nazionale di ripartizione delle frequenze.

G.U. n. 257 del 03 novembre 1998 - DECRETO 10 settembre 1998, n. 381 - Regolamento recante norme per la determinazione dei tetti di radiofrequenza compatibili con la salute umana.

Sandro Rao, Leonardo Salvaterra, Catello Acerra, (2010). SOFTWARE PER L'INSTALLAZIONE E LA CONFIGURAZIONE DELLA STAZIONE SISMICA GAIA2 Rapporti Tecnici INGV, n. 130

Coordinamento editoriale e impaginazione
Centro Editoriale Nazionale | INGV

Progetto grafico e redazionale
Laboratorio Grafica e Immagini | INGV Roma

Via di Vigna Murata, 605
00143 Roma
Tel. +39 06518601 Fax +39 065041181

http://www.ingv.it

Istituto Nazionale di Geofisica e Vulcanologia