ISSN 2039-7941
anno 2026 numero 528



RAPPORTI TECNICI INGV

Potenziamento della rete del Museo di Geoscienze INGV di Rocca di Papa: GARR e continuità operativa

ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA

528



Direttore Responsabile
Daniela VERSACE

Editor in Chief
Milena MORETTI

Editorial Board
Laura ALFONSI
Sofia BARANELLO
Carla BARNABA
Christian BIGNAMI
Simona CARANNANTE
Maria Grazia CIACCIO
Luca COCCHI
Luigi CUCCI
Lorenzo CUGLIARI
Elisabetta D'ANASTASIO
Alessia DI CAPRIO
Roberto DI MARTINO
Domenico DI MAURO
Domenico DORONZO
Filippo GRECO
Alessandro IAROCCI
Mario MATTIA
Daniele MELINI
Anna NARDI
Lucia NARDONE
Marco OLIVIERI
Arianna PESCI
Stefano PINTORE
Pierangelo ROMANO
Paola SBARRA
Davide SCAFIDI
Maurizio SOLDANI
Sara STOPPONI
Umberto TAMMARO
David ZULIANI

REGISTRAZIONE AL TRIBUNALE DI ROMA N.173 | 2014, 23 LUGLIO
© INGV Istituto Nazionale di Geofisica e Vulcanologia
Rappresentante legale: Presidente INGV
Sede: Via di Vigna Murata, 605 | Roma
Tutti i diritti riservati

www.ingv.it

ISTITUTO NAZIONALE **DI GEOFISICA E VULCANOLOGIA**

ISSN 2039-7941
anno 2026 numero 528

RAPPORTI TECNICI INGV

Potenziamento della rete del Museo di Geoscienze INGV di Rocca di Papa: GARR e continuità operativa

Network Infrastructure Enhancement for the INGV Geosciences Museum in Rocca di Papa: GARR Connectivity and Operational Continuity

Francesco Manzi[1,*], Pietro Ficeli[1], Alessandro Maiuri[1], Diego Sorrentino[2], Gianpaolo Sensale[1], Massimiliano Ascani[1]

[1]INGV | Istituto Nazionale di Geofisica e Vulcanologia, Amministrazione Centrale
[2]INGV | Istituto Nazionale di Geofisica e Vulcanologia, Sezione Roma 1

Corresponding author

Accettato 6 agosto 2026 | *Accepted 6 August 2026*
Come citare | *How to cite* F., Manzi, P., Ficeli, A., Maiuri, D., Sorrentino, G., Sensale, M., Ascani (2026). Potenziamento della rete del Museo di Geoscienze INGV di Rocca di Papa: GARR e continuità operativa. *Rapporti Tecnici INGV*, *528*, 22 pp. https://doi.org/10.13127/rpt/528

In copertina Vista del Museo di Geoscienze di Rocca di Papa (INGV) | *Cover View of the Rocca di Papa Geosciences Museum (INGV)*

528

INDICE

Riassunto 7

Abstract 7

Introduzione 7

1. Contesto operativo e motivazioni dell'intervento 8

2. Architettura hardware dell'infrastruttura di rete rinnovata 9
2.1 Dispositivi di interconnessione di rete 9
2.2 Server DNS/DHCP su Raspberry Pi 4 10

3. Connettività GARR in fibra ottica 11

4. Configurazione delle VLAN e segmentazione della rete informatica 12

5. Connessione satellitare Starlink come rete di backup 12
5.1 Dismissione della rete MPLS Fastweb 13

6. Cable management e riorganizzazione del rack di rete 14

7. Test di funzionamento e validazione del sistema 14
7.1 Stazione sismica di Rocca di Papa 15

8. Conclusioni 15

Ringraziamenti 15

Bibliografia 16

Sitografia 16

Glossario 17

Riassunto

Nel 2025, al fine di migliorare la resilienza dell'infrastruttura della rete informatica del Museo di Geoscienze di Rocca di Papa gestito dall'Istituto Nazionale di Geofisica e Vulcanologia (INGV), sono stati apportati diversi miglioramenti tecnologici. Gli interventi hanno incluso l'installazione di due dispositivi di sicurezza perimetrale Fortinet FortiGate 101F in configurazione di Alta Disponibilità attivo-passivo, di uno *switch* di tipo *Layer* 3 HPE Aruba 2930M con segmentazione della rete in *Virtual Local Area Network* (VLAN), e di un *server* DNS/DHCP basato su Raspberry Pi OS (Raspbian) con *Bind9* e *ISC-DHCP-Server* su piattaforma Raspberry Pi 4. È stata inoltre attivata una connessione in fibra ottica sulla rete GARR, che ha sostituito il precedente circuito MPLS Fastweb, ed è stato integrato un collegamento satellitare Starlink come rete di *backup* con possibilità di commutazione su linea satellitare tramite SD-WAN (Software-Defined WAN). L'intervento ha prodotto un significativo miglioramento delle prestazioni di connettività, della sicurezza perimetrale e della resilienza operativa della sede, con benefici diretti per la trasmissione dei dati della stazione sismica della Rete Sismica Nazionale, gestita dall'INGV e installata all'interno del Museo di Geoscienze di Rocca di Papa.

Abstract

In 2025, several technological upgrades were implemented to enhance the resilience of the IT network infrastructure of the INGV Geosciences Museum in Rocca di Papa, operated by the Istituto Nazionale di Geofisica e Vulcanologia (INGV). The interventions included the deployment of two Fortinet FortiGate 101F next-generation firewalls configured in an active-passive High Availability (HA) cluster, an HPE Aruba 2930M Layer 3 switch with network segmentation based on Virtual Local Area Networks (VLANs), and a DNS/DHCP server running Raspberry Pi OS (Raspbian) with BIND9 and ISC DHCP Server on a Raspberry Pi 4 platform.
Additionally, a fiber-optic connection to the GARR research and education network was activated, replacing the previous Fastweb MPLS circuit. A Starlink satellite connection was also integrated as a backup link, enabling automatic failover through a Software-Defined Wide Area Network (SD-WAN) architecture.
These upgrades significantly improved network connectivity, perimeter security, and the operational resilience of the site. They also provided direct benefits for the transmission of seismic data from the National Seismic Network station, operated by INGV and located within the Geosciences Museum in Rocca di Papa.

Keywords Infrastruttura di rete; GARR; Continuità operativa | Network infrastructure; Operational continuity

Introduzione

L'Istituto Nazionale di Geofisica e Vulcanologia (INGV) opera attraverso una rete di sedi distribuite sul territorio nazionale, ciascuna delle quali svolge attività di ricerca e raccolta dati di fondamentale importanza, mentre le attività di monitoraggio sono proprie solo di alcune sedi specializzate per la comprensione dei fenomeni geofisici e vulcanologici che interessano il territorio italiano. Il Museo di Geoscienze di Rocca di Papa, situato nel territorio dei Castelli

Romani in provincia di Roma, costituisce uno dei nodi periferici dell'infrastruttura INGV e ospita, oltre alla struttura museale aperta al pubblico, una stazione sismica della Rete Sismica Nazionale (RSN [INGV, 2005; Michelini et al., 2016]) gestita dall'INGV (sigla della stazione: RDP [1]).
Nel corso degli anni, la connettività del Museo di Geoscienze di Rocca di Papa è stata garantita attraverso soluzioni di tipo commerciale, in particolare tramite un circuito MPLS (*Multiprotocol Label Switching* [Rosen et al., 2001]) fornito dall'operatore Fastweb, che garantisce un collegamento alla rete INGV ma con limitazioni in termini di banda, ridondanza e integrazione con l'infrastruttura centralizzata presso la sede centrale INGV di Roma. La crescente necessità di una rete sicura, efficiente e scalabile, nonché la disponibilità di una connessione alla rete GARR (Gruppo per l'Armonizzazione delle Reti della Ricerca), ha motivato un progetto complessivo di *upgrade* che ha impegnato il personale tecnico specializzato per l'intero anno 2025.
Il presente documento riporta in modo sistematico tutte le fasi del rinnovamento infrastrutturale: dalla progettazione e acquisizione degli apparati, all'attività di posa del cavo in fibra ottica, passando per la configurazione degli apparati di rete e la validazione del sistema. L'obiettivo è fornire una documentazione tecnica di riferimento utile ad altri *team* afferenti all'INGV che si trovino ad affrontare interventi analoghi di modernizzazione infrastrutturale [Zerbinato et al., 2023].

1. Contesto operativo e motivazioni dell'intervento

Il Museo di Geoscienze di Rocca di Papa dell'INGV è ubicato nel territorio dei Castelli Romani, a circa 25 km a sud-est di Roma, a un'altitudine di circa 680 metri sul livello del mare. La posizione geografica, favorevole per l'osservazione geofisica grazie alla relativa distanza dalle sorgenti di rumore antropico della capitale, rende questo sito particolarmente idoneo all'installazione di strumentazione sismica sensibile.
Il Museo ospita due infrastrutture principali: la struttura museale, aperta al pubblico e destinata alla divulgazione scientifica delle attività INGV, e la stazione sismica RDP di Rocca di Papa. La stazione sismica è parte integrante della RSN gestita dall'INGV [2] ed è responsabile dell'acquisizione continua di dati sismici su base 24/7, trasmessi in tempo reale ai centri di elaborazione della sede centrale INGV di Roma. L'infrastruttura informatica e di rete è concentrata in un locale tecnico al piano interrato (livello −1) dell'edificio principale, nel quale sono alloggiati i rack di rete e i sistemi di acquisizione sismica.
Prima dell'intervento oggetto del presente rapporto, la connettività del Museo di Geoscienze di Rocca di Papa era affidata esclusivamente a un circuito MPLS fornito dall'operatore Fastweb, con indirizzamento nella classe 10.230.4.x/24. La tecnologia MPLS presentava limitazioni strutturali significative nel contesto dell'utilizzo scientifico e istituzionale dell'INGV: bassa capacità di banda rispetto alle esigenze crescenti di trasmissione dati sismici in tempo reale, costi di gestione elevati, scarsa flessibilità nella configurazione delle politiche di sicurezza. L'apparato di rete preesistente era non standardizzato rispetto alla sede centrale dell'INGV di Roma, privo di *firewall* dedicato e di segmentazione VLAN, con assenza di servizi di base come DNS/DHCP locale.
Il progetto di *upgrade* dell'infrastruttura del Museo è stato sviluppato con i seguenti obiettivi tecnici principali:

- attivare una connessione in fibra ottica dedicata sulla rete GARR, con banda nominale pari a 1 Gbit/s e collegamento diretto con la sede centrale dell'INGV di Roma;
- implementare un sistema di *firewall* ad alta disponibilità con funzionalità avanzate di sicurezza;
- modernizzare l'infrastruttura switching con segmentazione VLAN allineata agli standard della sede principale;
- dotare la sede di servizi DNS/DHCP locali indipendenti dalla WAN;

- integrare una connessione satellitare Starlink come *backup* ad alta resilienza;
- migliorare la connettività della stazione sismica RDP.

2. Architettura hardware dell'infrastruttura di rete rinnovata

2.1 Dispositivi di interconnessione di rete

Il componente centrale della nuova infrastruttura di sicurezza è costituito da una coppia di dispositivi Fortinet FortiGate 101F, configurati in modalità di Alta Disponibilità (*High Availability*, HA) attivo-passivo. Il FortiGate 101F è un dispositivo di nuova generazione (*Next-Generation FireWall*, NGFW) della serie FortiGate 100F di Fortinet, progettato per ambienti distribuiti che richiedono prestazioni elevate, sicurezza avanzata e affidabilità operativa. L'*appliance* è dotata di un processore dedicato alla sicurezza (*Security Processing Unit*, SPU) che accelera le operazioni di ispezione del traffico, permettendo velocità di *throughput* in regime di protezione attiva superiori a 2 Gbps [3].
Nella configurazione HA adottata, un'unità opera come dispositivo primario, gestendo attivamente tutto il traffico di rete, mentre la seconda rimane in stato di *standby* sincronizzato. La sincronizzazione avviene tramite un collegamento *heartbeat* dedicato (canale di comunicazione riservato tra i due dispositivi, utilizzato per verificarne reciprocamente la disponibilità e sincronizzarne lo stato), che consente il trasferimento continuo dello stato delle sessioni attive, delle configurazioni e delle politiche di sicurezza. Il *failover* automatico avviene in pochi secondi, garantendo la continuità operativa anche in caso di guasto *hardware* o aggiornamento *firmware*. Le funzionalità di sicurezza implementate includono: ispezione *stateful* del traffico TCP/UDP/ICMP, Application Control *Layer* 7, IPS con aggiornamento automatico delle firme, *Web Filtering*, ispezione SSL/TLS, *antivirus gateway* e supporto *Virtual Private Network* (VPN) IPsec/SSL. Lo schema della configurazione HA è illustrato in Figura 1.

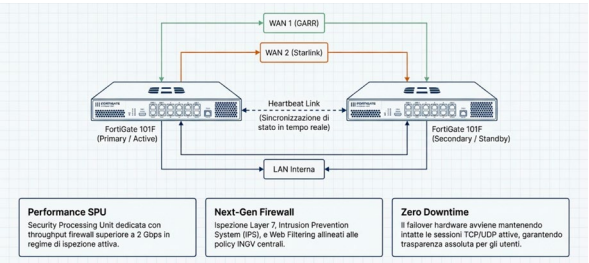


Figura 1 Schema della configurazione HA attivo-passivo dei *firewall* Fortinet FortiGate 101F presso il Museo di Geoscienze di Rocca di Papa.
Figure 1 *Active-passive HA configuration diagram of the Fortinet FortiGate 101F firewalls at the Rocca di Papa Geosciences Museum.*

Gli apparati di sicurezza perimetrale sono stati configurati seguendo le *best practice* Fortinet e allineati alle politiche di sicurezza in uso nella sede centrale di Roma, gestita tramite la piattaforma FortiManager [3]. Il *tunnel* VPN Ipsec con la sede centrale è configurato con algoritmi AES-256 per la cifratura del *payload* e SHA-256 per l'integrità, con autenticazione reciproca tramite certificati X.509 gestiti dall'infrastruttura di Public Key Infrastructure (PKI) dell'INGV.

Lo *switch* installato presso il Museo di Geoscienze di Rocca di Papa è un HPE Aruba 2930M, dispositivo di classe *enterprise* appartenente alla famiglia Aruba 2930 Series di Hewlett Packard Enterprise. Si tratta di uno *switch Layer* 3 gestito (*managed*), con supporto nativo per la segmentazione del traffico tramite VLAN IEEE 802.1Q [4], il che lo rende particolarmente adatto alla realizzazione di architetture di rete segmentate e sicure. Il modello qui adottato dispone di 24 porte PoE+ (*Power over Ethernet Plus*) da 1 Gbps e di porte *uplink* in fibra SFP+ da 10 Gbps. La gestione avviene tramite interfaccia grafica *web* (*Graphical User Interface*, GUI), CLI via SSH e piattaforma Aruba Central [5].
La configurazione dello *switch* è stata allineata agli standard adottati nella sede centrale INGV di Roma. Sono state implementate funzionalità di sicurezza *Layer* 2: *port security*, DHCP *snooping* per prevenire attacchi di tipo DHCP spoofing, *Dynamic ARP Inspection* (DAI) e *Rapid Spanning Tree Protocol* (RSTP) IEEE 802.1w per prevenire *loop* di rete. L'architettura complessiva dell'infrastruttura locale è illustrata in Figura 2.

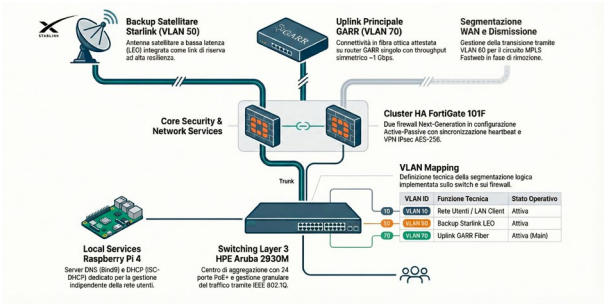


Figura 2 Schema architetturale dell'infrastruttura di rete locale del Museo di Geoscienze di Rocca di Papa: livelli WAN/Edge, Security (cluster HA FortiGate 101F), Switching (HPE Aruba 2930M), Services (VLAN 10/50/60/70) e Access. Immagine prodotta con il supporto di strumenti di intelligenza artificiale.
***Figure 2** Architectural diagram of the local network infrastructure of the Rocca di Papa Geosciences Museum: WAN/Edge, Security (FortiGate 101F HA cluster), Switching (HPE Aruba 2930M), Services (VLAN 10/50/60/70) and Access layers. Image produced with the support of artificial intelligence tools.*

Si segnala che l'attuale infrastruttura prevede un unico *switch* per la segmentazione VLAN e l'instradamento interno, scelta dettata anche da limiti di *budget* nella presente fase, che rappresenta un possibile punto singolo di guasto (*Single Point of Failure*). L'introduzione di un secondo apparato in configurazione ridondata rappresenta un possibile sviluppo futuro dell'infrastruttura.

2.2 Server DNS/DHCP su Raspberry Pi 4

Per la gestione dei servizi di rete locale è stato configurato un *server* DNS/DHCP su piattaforma Raspberry Pi 4 con sistema operativo Raspberry Pi OS (precedentemente noto come Raspbian, distribuzione GNU/Linux basata su Debian) [6]. I *software* utilizzati sono Bind9, per il servizio DNS, e ISC-DHCP-Server, per il servizio DHCP. Il Raspberry Pi 4 è dotato di processore Broadcom BCM2711 quad-core ARM Cortex-A72 a 1.8 GHz, 8 GB di RAM LPDDR4 e connettività Gigabit *Ethernet*. Il consumo energetico ridotto (< 10W) e le dimensioni compatte lo rendono adatto all'installazione in *rack* Figura 3.
Bind9 [7] è configurato come *server* DNS locale con risoluzione ricorsiva verso i *resolver upstream* della rete GARR, e ISC-DHCP-Server [8] come *server* DHCP per la rete utenti (VLAN 10).

La configurazione prevede *lease* statici per gli apparati principali e per i dispositivi del personale interno. In caso di interruzione della connessione verso la sede centrale, il *server* continua a erogare i servizi DNS/DHCP localmente in modalità *standalone*.
La configurazione iniziale del sistema avviene tramite ricette Puppet [9], mediante autenticazione del nodo locale verso il *server* Puppet master attivo nella sede centrale di Roma.
L'aggiornamento dei dati avviene, su richiesta, tramite la *web application* ManageNet, strumento interno INGV per la gestione centralizzata dei dispositivi di rete.

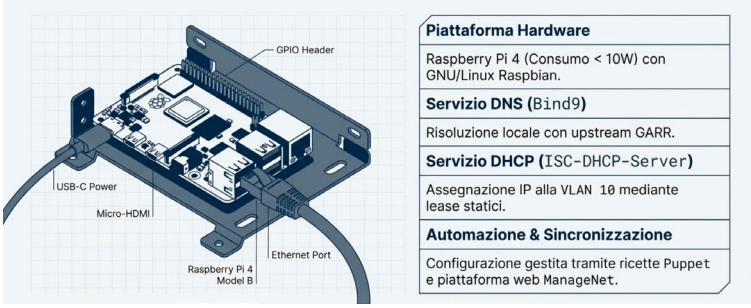


Figura 3 Schema del *server* DNS/DHCP su piattaforma Raspberry Pi 4 installato presso il Museo di Geoscienze di Rocca di Papa: architettura *hardware*, servizi *software* (Bind9 e ISC-DHCP-Server) e modalità di automazione tramite Puppet e ManageNet.
Figure 3 *Diagram of the DNS/DHCP server on Raspberry Pi 4 platform installed at the Rocca di Papa Geosciences Museum: hardware architecture, software services (Bind9 and ISC-DHCP-Server), and automation via Puppet and ManageNet.*

Rispetto alla ridondanza adottata per *firewall* e *switch*, il servizio DNS/DHCP su singolo Raspberry Pi 4 riflette una criticità operativa minore: un suo guasto non impatta il traffico già instradato né la trasmissione dei dati sismici, basata su indirizzamento statico.
Si segnala che ISC-DHCP-Server risulta in stato di *End-of-Life* dal 2022, sebbene continui a ricevere aggiornamenti di sicurezza tramite la distribuzione Raspberry Pi OS; la migrazione al successore Kea DHCP resta un possibile sviluppo futuro.

3. Connettività GARR in fibra ottica

Il GARR è il gestore della rete informatica italiana per la ricerca e l'istruzione [10], che interconnette università, enti di ricerca e istituzioni culturali con la rete europea GÉANT (*Gigabit European Academic Network* [11]). L'INGV, in qualità di ente di ricerca, è membro della rete GARR e usufruisce dei servizi di connettività offerti per le proprie sedi.
L'estensione della connettività GARR al Museo di Geoscienze di Rocca di Papa ha richiesto un iter negoziale e autorizzativo di notevole complessità. Il principale ostacolo tecnico era la necessità di posare un cavo in fibra ottica lungo le strade adiacenti al museo per raggiungere il punto di distribuzione GARR più vicino. Tale posa richiedeva l'autorizzazione dell'Ufficio Tecnico competente per il territorio del comune di Rocca di Papa, nonché il coordinamento con gli operatori GARR. La trattativa è durata diversi mesi e ha richiesto l'intervento dell'Ufficio Tecnico dell'INGV per ottenere le autorizzazioni necessarie e coordinare le varie operazioni necessarie per finalizzare l'attività di posa.
Una volta ottenute le autorizzazioni, gli operatori GARR hanno provveduto alla posa del cavo. Il *router* è stato installato congiuntamente dal personale tecnico INGV e dagli operatori GARR,

che si sono occupati della configurazione del lato WAN, mentre i tecnici dell'INGV hanno provveduto all'integrazione con l'infrastruttura romana. Al termine dell'intervento (novembre 2025), il collegamento è risultato pienamente operativo.
La connessione GARR è attestata sul *firewall* FortiGate 101F tramite la VLAN 70, dedicata al traffico GARR Internet. I *test* di velocità condotti al termine dell'installazione hanno evidenziato le seguenti prestazioni: velocità di *download* pari a 935,43 Mbps e velocità di *upload* pari a 864,91 Mbps, con *round-trip time* (RTT) verso Roma nell'ordine di pochi millisecondi, *packet loss* 0% e *jitter* trascurabile in condizioni operative normali. Tali valori, prossimi alla capacità nominale massima di un collegamento Gigabit *Ethernet*, confermano la qualità del collegamento in fibra ottica e l'efficienza della configurazione implementata.

4. Configurazione delle VLAN e segmentazione della rete informatica

La segmentazione della rete del Museo di Geoscienze di Rocca di Papa tramite VLAN è stata realizzata in conformità agli standard di configurazione adottati dalla sede centrale di Roma. La gestione delle VLAN è affidata al sistema di interconnessione di rete (paragrafo 2.1), che opera come dispositivo di aggregazione *Layer* 2/3 per tutta l'infrastruttura locale. Le VLAN implementate sono riportate in Tabella 1.

VLAN ID	Denominazione / Funzione	Stato
VLAN 10	Rete utenti – traffico LAN dei dispositivi utente e delle postazioni di lavoro	Attiva
VLAN 50	Rete Starlink – connessione satellitare di *backup*	Attiva (*backup*)
VLAN 60	Rete MPLS Fastweb – circuito WAN in dismissione	In dismissione
VLAN 70	Rete GARR – connessione in fibra ottica, *uplink* principale	Attiva (principale)

Tabella 1 Schema delle VLAN configurate sull'infrastruttura di rete del Museo di Geoscienze di Rocca di Papa.
Table 1 *VLAN scheme configured on the Rocca di Papa Geosciences Museum network infrastructure*

La segmentazione in VLAN consente l'isolamento del traffico tra i diversi segmenti di rete, con benefici in termini di sicurezza, QoS e semplificazione del *troubleshooting*. Sul sistema di sicurezza perimetrale sono configurate politiche di routing e sicurezza distinte per ciascuna VLAN.

La rete locale del Museo utilizza il piano di indirizzamento IPv4 della classe 10.236.1.0/24, coerente con il piano generale dell'INGV che riserva blocchi della classe 10.0.0.0/8 alle sedi periferiche [12][13], come definito nel documento interno di riferimento per i referenti informatici di rete a livello nazionale «Referenti IT e connettività». Il vecchio *router* Fastweb MPLS (in dismissione) utilizzava la classe 10.230.4.0/24, garantendo assenza di conflitti di routing durante la transizione. Gli indirizzi IP pubblici GARR (192.206.x.x) sono utilizzati per:

- Terminazione WAN della connessione GARR sul *firewall* primario.
- Gestione remota degli apparati.
- Terminazione del *tunnel* VPN IPsec con Roma.

5. Connessione satellitare Starlink come rete di backup

Starlink è il servizio di accesso a Internet tramite costellazione di satelliti in orbita bassa terrestre (*Low Earth Orbit*, LEO) sviluppato e gestito da SpaceX [14]. La costellazione è composta da

migliaia di satelliti a quote comprese tra 340 km e 570 km. La minore distanza rispetto ai sistemi geostazionari (GEO, ~36.000 km) si traduce in latenze tipiche di 20-60 ms, contro i 600-800 ms dei sistemi GEO. Il servizio Starlink Business offre velocità di *download* tipicamente comprese tra 100 e 500 Mbps e di *upload* tra 20 e 100 Mbps.
I principali vantaggi dell'integrazione di Starlink come rete di *backup* nell'infrastruttura di Rocca di Papa sono:

- Resilienza geografica: il collegamento satellitare non è soggetto a interruzioni causate da guasti fisici all'infrastruttura terrestre, inclusi quelli innescati da eventi sismici.
- Indipendenza dagli operatori terrestri: elimina la dipendenza da un singolo operatore, aumentando la resilienza complessiva della connettività.
- Rapidità di ripristino: la commutazione sulla connettività satellitare è possibile tramite SD-WAN in pochi secondi.
- Supporto alla trasmissione dati sismici: la bassa latenza della connettività satellitare garantisce la continuità della trasmissione dei dati sismici anche in modalità *backup*.

L'*antenna* Starlink è collegata al sistema di interconnessione di rete tramite la VLAN 50 dedicata. Sul *firewall* FortiGate è configurata una *policy* di routing basata su Software-Defined WAN (SD-WAN), che consente la gestione intelligente del traffico sui diversi *uplink* (GARR e Starlink) in base alla disponibilità del *link*, latenza, perdita di pacchetti e banda disponibile. In condizioni operative normali, tutto il traffico è instradato sull'*uplink* GARR (VLAN 70). La connessione Starlink (VLAN 50) rimane attiva in background con monitoraggio continuo; in caso di degradazione o interruzione del collegamento GARR, la commutazione su linea satellitare avviene in maniera trasparente per gli utenti, con un tempo di convergenza nell'ordine di decine di secondi. L'architettura end-to-end del sistema Starlink è illustrata in Figura 4.

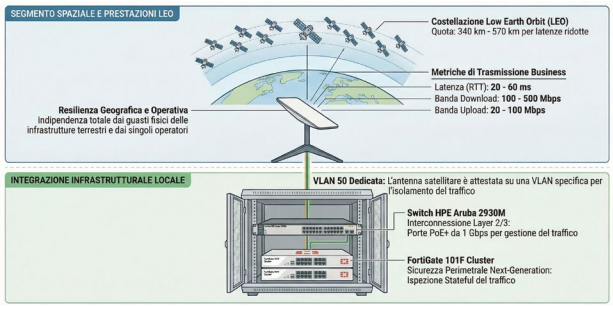


Figura 4 Schema tecnico del sistema Starlink: architettura end-to-end dalla costellazione LEO all'*antenna* utente installata presso il Museo di Geoscienze di Rocca di Papa.
***Figure 4** Technical diagram of the Starlink system: end-to-end architecture from the LEO constellation to the user antenna installed at the Rocca di Papa Geosciences Museum.*

5.1 Dismissione della rete MPLS Fastweb

Con l'attivazione della connessione GARR in fibra ottica, il precedente circuito MPLS fornito dall'operatore Fastweb (*subnet* 10.230.4.0/24) è entrato in una fase di dismissione programmata. La tecnologia MPLS si basa sulla commutazione di pacchetti tramite etichette apposte ai pacchetti IP, consentendo un instradamento rapido attraverso i nodi della rete dell'operatore [Rosen et al., 2001]. Sebbene offra garanzie di QoS adatte ad applicazioni *enterprise*, il suo modello di costo e la rigidità delle configurazioni la rendono meno competitiva per applicazioni ad alta banda.

Durante la fase transitoria, il circuito MPLS Fastweb è stato mantenuto attivo in parallelo alla connessione GARR come *uplink* secondario nella configurazione SD-WAN del *firewall*. Questo ha consentito di: (i) effettuare *test* comparativi tra le due connessioni; (ii) garantire la continuità operativa durante la stabilizzazione del nuovo collegamento; (iii) assicurare un *fallback* di sicurezza in caso di criticità. La dismissione definitiva comporterà la disattivazione della VLAN 60 sul sistema di interconnessione di rete e la rimozione delle politiche di routing corrispondenti sul sistema di sicurezza perimetrale. A regime, la rete informatica di Rocca di Papa sarà dotata di due soli *uplink* attivi: GARR (principale, VLAN 70) e Starlink (*backup*, VLAN 50).

6. Cable management e riorganizzazione del rack di rete

Contestualmente agli interventi di *upgrade*, è stata effettuata un'attività di riorganizzazione fisica del *rack* di rete posizionato nel locale tecnico al piano interrato dell'edificio principale. Il locale ospita sia gli apparati di rete sia la strumentazione della stazione sismica, rendendo particolarmente importante una corretta organizzazione fisica per garantire manutenibilità e riduzione delle interferenze elettromagnetiche.
Le operazioni di *cable management* hanno incluso:

1. rimozione dei cavi obsoleti relativi al vecchio circuito MPLS e all'infrastruttura preesistente;
2. etichettatura sistematica di tutti i cavi attivi con indicazione degli apparati di origine e destinazione, delle VLAN di appartenenza e della funzione del collegamento;
3. organizzazione dei percorsi tramite passacavi e fascette, separando cavi di alimentazione e cavi di segnale;
4. riposizionamento degli apparati nel *rack* secondo un ordine logico e funzionale. Al termine, tutta la documentazione relativa al cablaggio è stata aggiornata e resa disponibile al personale tecnico INGV interno responsabile della manutenzione.

7. Test di funzionamento e validazione del sistema

Al termine di ciascuna fase dell'intervento e al completamento del progetto, sono stati eseguiti *test* sistematici di funzionamento e validazione di tutti i componenti dell'infrastruttura rinnovata. I *test* hanno incluso verifiche a livello di singolo apparato (*unit testing*), verifiche dell'integrazione tra i componenti (integration *testing*) e verifiche del funzionamento complessivo del sistema (system *testing*). I principali *test* eseguiti e i relativi risultati sono i seguenti:

- *Test* di velocità della connessione GARR — Risultati: 935,43 Mbps in *download*, 864,91 Mbps in *upload*. Latenza verso Roma: < 5 ms. *Packet loss*: 0%.
- *Test* del collegamento punto-a-punto firewall-to-firewall (FW/FW) con Roma - Risultato: connettività confermata tramite *ping*, *traceroute* e trasferimento dati verso i sistemi INGV. Latenza nella norma, nessuna perdita di pacchetti.
- *Test* di commutazione Starlink — Risultato: commutazione su linea satellitare completata in < 30 secondi, connettività ripristinata su Starlink, ripristino su GARR al ripristino del collegamento principale.
- *Test* del *server* DNS/DHCP — Risultato: funzionamento corretto in tutte le condizioni testate, inclusa la modalità standalone (disconnessione dalla sede di Roma).
- *Test* di *failover* HA dei *firewall* — Risultato: *failover* completato senza interruzione del traffico di rete, sessioni attive mantenute.
- Verifica segmentazione VLAN — Risultato: isolamento del traffico tra le diverse VLAN confermato, politiche di sicurezza verificate.

7.1 Stazione sismica di Rocca di Papa

La stazione sismica installata all'interno del Museo è uno dei nodi periferici della rete di monitoraggio sismico dell'INGV. Le stazioni della RSN svolgono un ruolo fondamentale nella rilevazione e localizzazione degli eventi sismici, contribuendo ai sistemi di allerta precoce. Dal punto di vista tecnico, la stazione è composta da sismometri broadband e/o corto periodo, da un datalogger e da un sistema di comunicazione per la trasmissione in tempo reale dei dati verso il centro di acquisizione di Roma tramite protocollo SeedLink (protocollo di *streaming* dati sismici in tempo reale) in formato MiniSEED (Standard for the Exchange of Earthquake Data, formato compresso per dati sismici).
Il miglioramento della connettività conseguito con l'attivazione della fibra GARR e del collegamento FW/FW con Roma ha prodotto i seguenti benefici diretti:

- Riduzione della latenza di trasmissione, con impatto positivo sull'efficacia dei sistemi di *early warning*.
- Aumento della banda disponibile (> 900 Mbps nominali), sufficiente anche in caso di espansione futura della strumentazione.
- Maggiore resilienza grazie alla disponibilità di due *uplink* (GARR + Starlink) con possibilità di commutazione su linea satellitare.
- Collegamento diretto e sicuro alla rete INGV tramite *tunnel* VPN IPsec, con QoS configurabile e protezione da accessi non autorizzati.

8. Conclusioni

Il progetto di *upgrade* dell'infrastruttura della rete informatica della sede museale di Rocca di Papa rappresenta un significativo miglioramento delle capacità operative e della sicurezza informatica di uno dei nodi periferici della rete informatica istituzionale. I principali risultati conseguiti possono essere sintetizzati in tre ambiti: connettività, sicurezza e resilienza. Dal punto di vista della connettività, l'attivazione del collegamento in fibra ottica GARR ha portato la banda disponibile da meno di 10 Mbps (circuito MPLS Fastweb) a oltre 900 Mbps, determinando un significativo miglioramento delle prestazioni di rete. Il collegamento FW/FW con la sede centrale INGV di Roma ha creato un percorso diretto e sicuro per il traffico istituzionale e per la trasmissione dei dati sismici, eliminando la dipendenza da infrastrutture di terze parti.
Dal punto di vista della sicurezza, l'implementazione dei *firewall* Fortinet FortiGate 101F in configurazione HA ha dotato la sede di un sistema di sicurezza perimetrale di livello *enterprise*, allineando la sede museale agli standard della sede principale. La segmentazione della rete in VLAN dedicate ha migliorato l'isolamento tra i diversi segmenti e ridotto la superficie di attacco complessiva.
Dal punto di vista della resilienza, la disponibilità di due *uplink* WAN (GARR e Starlink) con possibilità di commutazione su linea satellitare garantisce una continuità operativa significativamente superiore rispetto alla situazione precedente. La stazione sismica di Rocca di Papa beneficia direttamente di questi miglioramenti, con ricadute positive sulle attività di monitoraggio sismico della RSN.

Ringraziamenti

Gli autori ringraziano l'Ufficio Tecnico competente per il territorio di Rocca di Papa per le autorizzazioni concesse e per il supporto fornito durante le operazioni di posa del cavo in fibra

ottica. Un ringraziamento è rivolto inoltre a tutti i colleghi dell'INGV che hanno contribuito, a vario titolo, alla realizzazione del progetto.

Bibliografia

Istituto Nazionale di Geofisica e Vulcanologia (INGV) (2005). Rete Sismica Nazionale (RSN) [Data set]. Istituto Nazionale di Geofisica e Vulcanologia (INGV). https://doi.org/10.13127/SD/X0FXNH7QFY

Michelini, A., Margheriti, L., Cattaneo, M., Cecere, G., D'Anna, G., Delladio, A., Moretti, M., Pintore, S., Amato, A., Basili, A., Bono, A., Casale, P., Danecek, P., Demartin, M., Faenza, L., Lauciani, V., Mandiello, A. G., Marchetti, A., Marcocci, C., Mazza, S., Mele, F. M., Nardi, A., Nostro, C., Pignone, M., Quintiliani, M., Rao, S., Scognamiglio, L., and Selvaggi, G. (2016). The Italian National Seismic Network and the earthquake and tsunami monitoring and surveillance systems, *Adv. Geosci.*, 43, 31–38. https://doi.org/10.5194/adgeo-43-31-2016

Rosen, E., Viswanathan, A., & Callon, R. (2001). Multiprotocol label switching architecture. RFC 3031. *Internet Engineering Task Force*. https://doi.org/10.17487/RFC3031

Zerbinato, G., Perfetti, P., Marino, S., Scarpato, G., & Cacciaguerra, S. (2023). Trasloco dell'infrastruttura ICT del Centro di Monitoraggio delle attività del Sottosuolo. *Rapporti Tecnici INGV*, 467, 24 pp. https://doi.org/10.13127/rpt/467

Sitografia

[1] INGV – Monitoraggio sismico: https://terremoti.ingv.it/instruments/station/RDP (ultima consultazione: 15.01.2026)

[2] Sito web istituzionale INGV: https://www.ingv.it/ (ultima consultazione: 03.07.2026)

[3] Fortinet Inc. (2023). FortiGate 100F/101F Data Sheet. https://www.fortinet.com/it/resources/data-sheets/fortigate-100f-series (ultima consultazione: 15.01.2026)

[4] IEEE 802.1Q – IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks: https://standards.ieee.org/ieee/802.1Q (ultima consultazione: 30.06.2026)

[5] HPE. (2023). HPE Aruba Networking 2930M Switch Series Data Sheet. Hewlett Packard Enterprise. – https://www.hpe.com/psnow/doc/PSN1009875107ITIT (ultima consultazione: 15.01.2026)

[6] Raspberry Pi OS (GNU/Linux Raspbian): https://www.raspberrypi.com/software/operating-systems/ (ultima consultazione: 15.01.2026)

[7] Internet Systems Consortium (ISC). Bind9 – The most widely used DNS software. https://www.isc.org/bind/ (ultima consultazione: 30.06.2026)

[8] Internet Systems Consortium (ISC). ISC DHCP. https://www.isc.org/dhcp/ (ultima consultazione: 30.06.2026)

[9] Puppet by Perforce – Infrastructure automation software. https://www.puppet.com (ultima consultazione: 30.06.2026)

[10] GARR – Rete italiana dell'università e della ricerca: https://www.garr.it (ultima consultazione: 15.01.2026)

[11] GÉANT – Rete europea per la ricerca: https://geant.org (ultima consultazione: 15.01.2026)

[12] Internet Assigned Numbers Authority (IANA). (2002). Special-Use IPv4 Addresses. RFC 3330. https://datatracker.ietf.org/doc/html/rfc3330 (ultima consultazione: 30.06.2026)

[13] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). Address Allocation for Private Internets. RFC 1918. https://datatracker.ietf.org/doc/html/rfc1918

(ultima consultazione: 30.06.2026)
[14] SpaceX Starlink – https://www.starlink.com (ultima consultazione: 15.01.2026)

Glossario

AES - Advanced Encryption Standard. Algoritmo di cifratura simmetrica utilizzato per proteggere i dati.
ARP - Address Resolution Protocol. Protocollo che associa un indirizzo IP a un indirizzo MAC all'interno di una rete locale.
ARM - Advanced RISC Machine. Architettura di processori a basso consumo energetico ampiamente utilizzata nei sistemi embedded.
BCM2711 - Broadcom BCM2711. System-on-Chip (SoC) sviluppato da Broadcom e utilizzato nel Raspberry Pi 4.
BIND 9 - Berkeley Internet Name Domain versione 9. Software open source utilizzato per implementare il servizio DNS.
Bind9 - Software open source che implementa il servizio DNS.
Broadband - Sensore sismico a larga banda utilizzato per il monitoraggio sismico.
CLI - Command Line Interface. Interfaccia testuale per la gestione e configurazione dei sistemi.
DAI - Dynamic ARP Inspection. Funzione di sicurezza che previene attacchi ARP spoofing.
Datalogger - Dispositivo per l'acquisizione, la registrazione e la trasmissione dei dati provenienti dalla strumentazione.
DHCP - Dynamic Host Configuration Protocol. Protocollo che assegna automaticamente indirizzi IP e parametri di rete ai dispositivi.
DNS - Domain Name System. Sistema che traduce i nomi di dominio in indirizzi IP.
Failover - Commutazione automatica su un sistema o collegamento ridondante in caso di guasto.
Fastweb - Operatore di telecomunicazioni che forniva il precedente collegamento MPLS del Museo di Geoscienze.
FortiGate - Firewall di nuova generazione sviluppato da Fortinet per la protezione delle reti informatiche.
FortiManager - Piattaforma Fortinet per la gestione centralizzata dei firewall e delle relative configurazioni.
FW - Firewall. Sistema hardware o software che controlla e filtra il traffico di rete.
GARR - Gruppo per l'Armonizzazione delle Reti della Ricerca. Rete nazionale italiana dedicata alla ricerca e all'istruzione.
Gbps - Gigabit per secondo. Unità di misura della velocità di trasmissione dati pari a un miliardo di bit al secondo.
GEO - Geostationary Earth Orbit. Orbita geostazionaria a circa 36.000 km dalla superficie terrestre.
GNU - GNU's Not Unix. Progetto per lo sviluppo di un sistema operativo libero e open source.
GUI - Graphical User Interface. Interfaccia grafica che consente l'interazione con un sistema tramite elementi visuali.
HA - High Availability. Configurazione che garantisce continuità operativa in caso di guasto.
Heartbeat - Collegamento dedicato tra dispositivi HA utilizzato per monitorarne lo stato e sincronizzarne le configurazioni.
HPE - Hewlett Packard Enterprise. Azienda produttrice di soluzioni hardware e software per infrastrutture IT.
IANA - Internet Assigned Numbers Authority. Organizzazione che gestisce l'assegnazione di indirizzi IP e altri identificatori Internet.
ICMP - Internet Control Message Protocol. Protocollo utilizzato per diagnostica e gestione della rete.

ICT - Information and Communication Technology. Insieme delle tecnologie dell'informazione e della comunicazione.
IEEE - Institute of Electrical and Electronics Engineers. Organizzazione che sviluppa standard internazionali per reti e telecomunicazioni.
INGV - Istituto Nazionale di Geofisica e Vulcanologia. Ente pubblico italiano di ricerca nei settori della geofisica e della vulcanologia.
IP - Internet Protocol. Protocollo fondamentale per l'instradamento dei pacchetti nelle reti IP.
IPsec - Internet Protocol Security. Insieme di protocolli per proteggere le comunicazioni IP tramite cifratura e autenticazione.
IPS - Intrusion Prevention System. Sistema che rileva e blocca automaticamente tentativi di attacco informatico.
ISC - Internet Systems Consortium. Organizzazione che sviluppa software open source per servizi di rete.
LAN - Local Area Network. Rete informatica locale che collega dispositivi all'interno di un'area limitata.
Layer 2 - Livello 2 del modello OSI (Data Link Layer). Livello responsabile della commutazione dei frame e della comunicazione nella rete locale.
Layer 3 - Livello 3 del modello OSI (Network Layer). Livello responsabile dell'instradamento dei pacchetti IP tra reti differenti.
Lease (DHCP lease) - Periodo di validità dell'assegnazione di un indirizzo IP da parte del server DHCP.
LEO - Low Earth Orbit. Orbita terrestre bassa utilizzata da costellazioni satellitari come Starlink.
LPDDR4 - Low Power Double Data Rate 4. Memoria RAM a basso consumo energetico utilizzata nei dispositivi embedded.
MAC - Media Access Control. Indirizzo fisico univoco assegnato a un'interfaccia di rete.
ManageNet - Applicazione interna INGV per la gestione centralizzata degli apparati di rete.
MiniSEED - Mini Standard for the Exchange of Earthquake Data. Formato standard compatto per l'archiviazione e lo scambio di dati sismici.
MPLS - Multiprotocol Label Switching. Tecnologia di instradamento che utilizza etichette per ottimizzare il traffico di rete.
NGFW - Next-Generation Firewall. Firewall di nuova generazione con funzionalità avanzate di sicurezza e ispezione del traffico.
ORCID - Open Researcher and Contributor ID. Identificativo univoco internazionale per ricercatori e autori scientifici.
OS - Operating System. Sistema operativo che gestisce le risorse hardware e software di un computer.
Payload - Parte utile di un pacchetto di rete contenente i dati trasmessi.
PKI - Public Key Infrastructure. Infrastruttura che gestisce certificati digitali e crittografia a chiave pubblica.
PoE - Power over Ethernet. Tecnologia che consente di alimentare un dispositivo tramite il cavo Ethernet.
PoE+ - Power over Ethernet Plus. Tecnologia che fornisce alimentazione elettrica e dati tramite un unico cavo Ethernet con maggiore potenza rispetto al PoE standard.
Puppet - Software di automazione per la configurazione e gestione centralizzata dei sistemi informatici.
QoS - Quality of Service. Tecniche che garantiscono priorità e qualità del traffico di rete.
RAM - Random Access Memory. Memoria volatile utilizzata dal sistema per l'esecuzione dei programmi.
Raspberry Pi - Single-board computer utilizzato come server DNS/DHCP e per applicazioni embedded.

Raspberry Pi OS - Sistema operativo ufficiale del Raspberry Pi, basato su Debian.
Raspbian - Nome storico della distribuzione oggi denominata Raspberry Pi OS.
RDP - Rocca di Papa. Codice identificativo della stazione sismica INGV installata presso il Museo di Geoscienze.
Resolver - Server DNS che effettua la risoluzione delle richieste verso altri server DNS.
RFC - Request for Comments. Documenti tecnici che definiscono standard e protocolli Internet.
RSN - Rete Sismica Nazionale. Infrastruttura dell'INGV dedicata al monitoraggio sismico del territorio italiano.
RSTP - Rapid Spanning Tree Protocol. Protocollo che previene i loop di rete e accelera la convergenza della topologia Ethernet.
RTT - Round-Trip Time. Tempo impiegato da un pacchetto per raggiungere la destinazione e tornare al mittente.
SD-WAN - Software-Defined Wide Area Network. Tecnologia che gestisce dinamicamente il traffico su più collegamenti WAN.
SeedLink - Protocollo per lo streaming in tempo reale dei dati sismici tra stazioni e centri di acquisizione.
SFP+ - Small Form-factor Pluggable Plus. Modulo ricetrasmettitore utilizzato per collegamenti in fibra ottica fino a 10 Gbit/s.
SHA-256 - Secure Hash Algorithm a 256 bit. Algoritmo crittografico utilizzato per garantire l'integrità dei dati.
SoC - System-on-Chip. Circuito integrato che incorpora CPU, memoria e altre componenti in un unico chip.
SPU - Security Processing Unit. Processore dedicato all'accelerazione delle funzioni di sicurezza nei firewall Fortinet.
SSH - Secure Shell. Protocollo sicuro per l'accesso remoto e l'amministrazione di sistemi informatici.
SSL - Secure Sockets Layer. Protocollo di sicurezza per la cifratura delle comunicazioni, oggi sostituito da TLS.
Stateful Inspection - Tecnica di ispezione del traffico che tiene traccia dello stato delle connessioni per migliorarne la sicurezza.
TCP - Transmission Control Protocol. Protocollo di trasporto orientato alla connessione che garantisce affidabilità nella trasmissione dei dati.
Throughput - Quantità di dati trasferibili in un determinato intervallo di tempo attraverso una rete o un dispositivo.
TLS - Transport Layer Security. Protocollo crittografico che protegge le comunicazioni sulle reti informatiche.
Traceroute - Strumento di diagnostica che mostra il percorso seguito dai pacchetti in rete fino alla destinazione.
UDP - User Datagram Protocol. Protocollo di trasporto senza connessione, utilizzato per applicazioni che richiedono bassa latenza.
Uplink - Collegamento verso un livello superiore della rete o verso la rete WAN.
VLAN - Virtual Local Area Network. Tecnologia che consente di suddividere logicamente una rete fisica in reti indipendenti.
VPN - Virtual Private Network. Connessione cifrata che consente di collegare in modo sicuro reti o dispositivi remoti.
WAN - Wide Area Network. Rete geografica che collega sedi e reti distribuite su vaste aree.
WAN/Edge - Wide Area Network / Edge. Livello periferico della rete in cui avviene la connessione verso reti esterne o Internet.
X.509 - Standard per certificati digitali a chiave pubblica. Definisce il formato dei certificati utilizzati nelle infrastrutture PKI.

QUADERNI di GEOFISICA

ISSN 1590-2595 https://collane-editoriali.ingv.it/index.php/qdg/it/index/

QUADERNI di GEOFISICA è una rivista scientifica che pubblica dati, misurazioni e osservazioni geofisiche (anche preliminari) in italiano e inglese. L'obiettivo è una diffusione rapida e gratuita per la comunità scientifica, garantita da un processo di peer-review e da un Editorial Board multidisciplinare. La rivista è inclusa in "Emerging Sources Citation Index" di Clarivate Analytics e "Open Access Journals" di Scopus, e adotta il modello Diamond Open Access, che non prevede costi né per gli autori né per i lettori.

QUADERNI di GEOFISICA is a scientific journal that publishes geophysical data, measurements and observations, including preliminary results, in Italian and English. Its aim is to ensure rapid and free dissemination to the research community, supported by a peer-review process and by a multidisciplinary Editorial Board. The journal is included in the Emerging Sources Citation Index of Clarivate Analytics and it's included in the Open Access journals of Scopus. It follows the Diamond Open Access model, with no charges for either authors or readers.

RAPPORTI TECNICI INGV

ISSN 2039-7941 https://collane-editoriali.ingv.it/index.php/rt/it/index

RAPPORTI TECNICI INGV è una rivista tecnico-scientifica che mette in mostra le numerose attività tecnologiche e di ricerca condotte dai ricercatori e tecnici INGV, e non solo. Pubblicata in italiano e inglese, RAPPORTI TECNICI INGV è ideata per valorizzare anche quei lavori che offrono un contributo significativo dal punto di vista tecnico, operativo o documentale fondamentale per lo sviluppo dell'Ente. La rivista adotta il modello Diamond Open Access, che non prevede costi né per gli autori né per i lettori.

RAPPORTI TECNICI INGV is a technical–scientific journal that showcases the wide range of technological and research activities carried out by INGV researchers and technical staff, as well as by external contributors. Published in Italian and English, RAPPORTI TECNICI INGV is designed to highlight works that provide a significant contribution from a technical, operational, or documentary perspective, and that are essential to INGV development. The journal follows the Diamond Open Access model, with no charges for either authors or readers.

MISCELLANEA INGV

ISSN 2039-6651 https://collane-editoriali.ingv.it/index.php/mi/it/index

MISCELLANEA INGV rappresenta una tipologia di editoria non tradizionalmente catalogabile nelle ordinarie riviste scientifiche di settore. Pubblicata in lingua italiana e inglese, MISCELLANEA INGV offre uno spazio per la pubblicazione di materiali eterogenei che, pur non rientrando nei formati più strutturati delle altre Collane editoriali INGV, rivestono un interesse scientifico, tecnico o divulgativo. La rivista adotta il modello Diamond Open Access, che non prevede costi né per gli autori né per i lettori.

MISCELLANEA INGV represents a form of publishing that cannot be classified within the standard scientific journals. Published in Italian and English, MISCELLANEA INGV provides a venue for the publication of heterogeneous materials that are of scientific, technical or outreach interest, even though they do not fall within the more structured formats of the other INGV editorial series. The journal follows the Diamond Open Access model, with no charges for either authors or readers.

Progetto grafico
Barbara ANGIONI
Istituto Nazionale di Geofisica e Vulcanologia

Ufficio Editoriale
Francesca DI STEFANO | Coordinatore

Segreteria di redazione
segreteria.collane-editoriali@ingv.it

Editing | Produzione | Grafica redazionale
Barbara ANGIONI
Massimiliano CASCONE
Francesca DI STEFANO
Patrizia PANTANI

© 2026 the Author(s). Open Access.
This article is licensed under a Creative Commons Attribution 4.0 International License.



Creative Commons Attribution 4.0 International



ISTITUTO NAZIONALE **DI GEOFISICA E VULCANOLOGIA**

