

Rapporti tecnici INGV

Il sistema di videoconferenza dell'INGV

118



Istituto Nazionale di
Geofisica e Vulcanologia

Direttore

Enzo Boschi

Editorial Board

Raffaele Azzaro (CT)

Sara Barsotti (PI)

Mario Castellano (NA)

Viviana Castelli (BO)

Anna Grazia Chiodetti (AC)

Rosa Anna Corsaro (CT)

Luigi Cucci (RM1)

Mauro Di Vito (NA)

Marcello Liotta (PA)

Lucia Margheriti (CNT)

Simona Masina (BO)

Nicola Pagliuca (RM1)

Salvatore Stramondo (CNT)

Andrea Tertulliani - coordinatore (RM1)

Aldo Winkler (RM2)

Gaetano Zonno (MI)

Segreteria di Redazione

Francesca Di Stefano - coordinatore

Tel. +39 06 51860068

Fax +39 06 36915617

Rossella Celi

Tel. +39 06 51860055

Fax +39 06 36915617

redazionecen@ingv.it



Rapporti tecnici INGV

IL SISTEMA DI VIDEOCONFERENZA DELL'INGV

Manuela Sbarra, Gianpaolo Sensale, Diego Sorrentino, Francesco Zanolin, Lucio Badiali,
Francesca Caprara, Pietro Ficeli, Melissa Mendicino, Massimiliano Rossi

INGV (Istituto Nazionale di Geofisica e Vulcanologia, Centro Nazionale Terremoti – Servizi Informatici e Reti)

118

Indice

Introduzione	5
1 Lo stato dell'arte	6
1.1 Protocollo H323	6
1.2 Protocollo H320	8
2 Architettura della videoconferenza	9
2.1 I terminali	9
2.2 Gateway	10
2.3 Gatekeeper	10
2.4 Multipoint Control Unit (MCU)	11
3 Integrazione tra la rete INGV, le sedi e la videoconferenza	13
4 Applicazioni	15
4.1 Collegamento con l'Antartide	15
4.2 Incontro con il ministro Gelmini	15
5 Streaming	16
5.1 Architettura del sistema di streaming	16
5.2 Gestione eventi Streaming	17
6 Utilizzo operativo e risparmio di gestione	18
6.1 Effetti della latenza, del jitter e della perdita di pacchetti sulla qualità della videoconferenza	19
6.1.1 Latenza (Ritardo di Trasferimento)	19
6.1.2 Jitter	19
6.1.3 Perdita di pacchetti (Packet loss)	19
7 Appendice - il sistema di prenotazioni integrato	20
Bibliografia	21

Introduzione

Negli ultimi anni la continua globalizzazione e decentralizzazione delle risorse umane delle aziende ha contribuito alla necessità di sviluppare degli strumenti di comunicazione versatili e che facciano risparmiare tempo e denaro.

In questa ottica è stato sviluppato un sistema che potesse soddisfare questi requisiti. La videocomunicazione, grazie anche alla crescente disponibilità di banda, sia su internet che nelle reti LAN private, consente oggi di trasmettere efficacemente audio, video e dati, con un innegabile vantaggio in termini di miglioramento della qualità della comunicazione, della produttività in generale e abbattimento di costi di trasferta del personale. Comunicazioni a distanza con video e audio di alta qualità sono più personali e interattive, creano relazioni di fiducia stabili, consentono presentazioni complesse, spiegazioni dettagliate e coinvolgono anche soggetti geograficamente lontani.

Una struttura di videocomunicazione ben progettata è un investimento in termini di produttività, efficienza e risparmio dei costi.

Il sistema di videoconferenza dell'INGV nasce dall'interesse del TTC Informatico che ha proposto all'Amministrazione i vantaggi funzionali ed economici di questo sistema. Si ringraziano tutti i membri del TTC, cioè tutti gli informatici (*) responsabili nelle varie Sedi dell'INGV che hanno contribuito con il Sir ai vari test perché il sistema andasse in funzione esattamente come progettato.

Valore aggiunto che è stato considerato strategico al CNT (di cui il SIR ha da poco eseguito la ristrutturazione della sala di monitoraggio sismico) sarà la possibilità di usare la videocomunicazione tra le sedi di monitoraggio dell'INGV e con la sala della Protezione Civile in caso di emergenza.

(*) Stefano Cacciaguerra (BO), Mariano La Via (CT), Fabrizio Meroni (MI), Santi Mirena (MI), Luca Nannipieri (PI), Danilo Reitano (CT), Dario Richichi (PA), Gianni Scarpato (NA), Dario Sudati (MI).

1 Lo stato dell'arte

La videoconferenza rappresenta l'interazione sincrona in audio, video e dati fra due o più soggetti. La possibilità di comunicare in videoconferenza dipende dalla disponibilità di apparati che supportino la cattura, codifica, trasmissione e decodifica di audio e video, e dalla capacità degli apparati stessi di colloquiare secondo un protocollo standard comune.

I protocolli maggiormente diffusi sono H.320 e H.323. Vi sono altre suite di protocolli che interessano la videoconferenza ma il livello di sviluppo, consolidamento e diffusione non è ancora capillare. La videoconferenza H.320, nota anche con il nome di videoconferenza su ISDN, definisce le modalità di comunicazione audio, video e dati, sia punto a punto che multipunto, su reti a commutazione di circuito (come ISDN, appunto). La videoconferenza H.323 si applica invece all'applicazione su rete TCP/IP, che definisce le modalità di comunicazione audio, video e dati, sia punto a punto che multipunto, su reti IP.

Un qualunque sistema in grado di convogliare audio, video, dati rispondente allo standard può essere considerato un terminale di videoconferenza. In questa definizione rientrano un'ampia gamma di prodotti con caratteristiche tecniche, funzionali e costi notevolmente diversi. Ognuno di questi prodotti deve essere perciò vagliato in base al contesto di utilizzo. Lo standard indica che la funzionalità minimale da garantire per una videoconferenza è l'audio; l'audio stesso costituisce uno degli elementi che determinano la buona riuscita di una videoconferenza. Se l'audio risulta affetto da rumori, distorsioni oppure eco, si vanifica l'utilità della videoconferenza. Questi problemi sono amplificati nel caso in cui l'incontro non avvenga nella lingua madre. In generale, se ci sono problemi legati alla qualità dell'audio, la videoconferenza risulterà completamente inefficace.

1.1 Protocollo H323

H.323 è uno standard creato nel 1996 dall'ITU Study Group 16 (*International Telecommunication Union*) che stabilisce le specifiche per una serie di protocolli utilizzabili per la trasmissione di dati, audio e video su di una rete a commutazione di pacchetto.

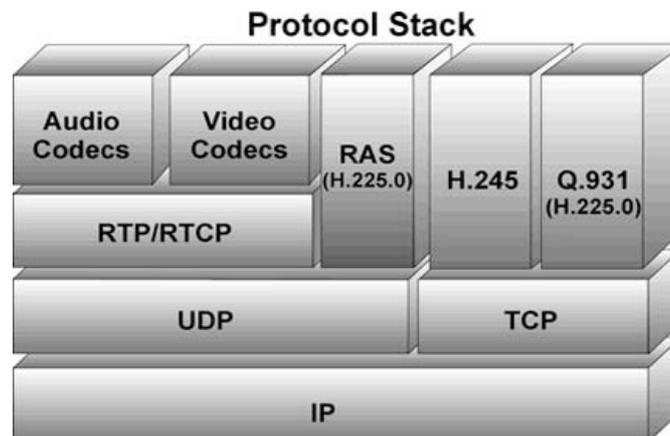


Figura 1. Stack Protocol H323.

L'architettura di un sistema basato su tali protocolli si compone di quattro entità:

1. **Terminale:** è un dispositivo di rete utilizzato dall'utente per ricevere ed effettuare chiamate in grado di codificare e decodificare le varie tipologie di dati secondo gli standard ITU; può essere un PC sul quale è in esecuzione un *software* conforme allo standard H.323, oppure un dispositivo dedicato (*IP Phone*). H.323 permette agli utenti di individuare i Terminali mediante un *Alias Address*, un indirizzo simbolico di tipo stringa di caratteri, che il chiamante compone per selezionare il destinatario della chiamata.

2. **Gateway**: definito anche come *media gateway*, è un apparato che permette la comunicazione *real-time* tra i vari terminali instaurando comunicazioni multimediali tra reti a commutazione di pacchetto senza QoS e reti a commutazione di circuito che realizzano la QoS.
3. **MCU**: l'entità *Multipoint Control Unit* permette le comunicazioni multipunto, coordinando la segnalazione di controllo e manipolando i flussi multimediali prodotti dai Terminali.
4. **Gatekeeper**: effettua il controllo dello stato delle comunicazioni in H.323 monitorando le risorse di banda.
Ad ogni gatekeeper viene assegnata una porzione della rete H.323.

Tutti i terminali contattano il proprio *gatekeeper*, al momento in cui effettuano una chiamata, utilizzando pacchetti UDP in broadcast. Il *gatekeeper* risponde a questo pacchetto comunicando al terminale il proprio indirizzo IP. Il terminale invia una richiesta di registrazione ed una volta ricevuta la risposta richiede al *gatekeeper* le risorse di banda necessarie ad effettuare una chiamata. Se la banda è sufficiente il *gatekeeper* accetta la richiesta ed il terminale invia il numero da contattare, attraverso il canale di segnalazione. Dopo che la chiamata è stata accettata dal terminale remoto il *gatekeeper* si svincola dai due terminali che negoziano il *codec* da utilizzare ed i vari parametri necessari della comunicazione.

H.323 racchiude e collega insieme una serie di protocolli applicativi. Il suo funzionamento è indipendente dal protocollo di livello trasporto e dalla rete a pacchetti sottostanti, anche se lo standard specifica il tipo di servizi che devono necessariamente essere forniti dal livello inferiore e che sono un servizio affidabile *end to end* di trasporto dei datagrammi, ad esempio TCP per quanto concerne le reti IP o un servizio inaffidabile *end to end* di trasporto dei datagrammi, quale UDP.

H.323 fa riferimento al protocollo H.225 per due funzionalità fondamentali: il protocollo *Registration, Admission, Status* (RAS) e il protocollo *Call Signaling*.

Il protocollo H.225 RAS (*Registration, Admission, Status*) definisce i messaggi per lo scambio di segnalazione di controllo tra gli *endpoints* ed il *gatekeeper*. I messaggi RAS sono scambiati su un canale inaffidabile utilizzando il protocollo UDP. Tale canale è aperto indipendentemente da una chiamata e quindi prima dell'instaurazione di qualunque altro canale. Mediante il protocollo RAS si realizzano le procedure di *discovery* del *gatekeeper*, registrazione, controllo di ammissione, modifica della banda assegnata ad una comunicazione, scambio di informazioni di stato, cancellazione di registrazioni.

Il protocollo H.225.0 *Call Signaling* definisce i messaggi scambiati al fine di stabilire l'instaurazione e l'abbattimento di una connessione tra *endpoints*, sulla quale avverrà lo scambio di dati *real-time*.

Lo scambio dei messaggi avviene su un canale affidabile, quindi TCP per le reti basate su IP. Questo protocollo si rifà, sostanzialmente, al protocollo Q.931, definito per il controllo di chiamata in reti ISDN. Infatti, i messaggi H.225.0 utilizzati nell'instaurazione e nell'abbattimento di una chiamata, sono identici a quelli usati per una chiamata ISDN. Tipici messaggi di *Call Signaling* sono: *Setup, CallProceeding, Alerting, Connect, ReleaseComplete*.

Il protocollo H.245 viene utilizzato per il controllo delle comunicazioni; con H.245 si realizzano le procedure per attivare e gestire una comunicazione multimediale tra due o più entità H.323. Ogni entità deve instaurare un canale dedicato di tipo affidabile (TCP), detto H.245 *Control Channel*, per ogni comunicazione alla quale partecipa; tale canale sarà permanentemente aperto durante tutta la connessione. L'instaurazione degli H.245 *Control Channel* avviene dopo il dialogo H.225 (RAS e *Call Signaling*). Nel caso una delle entità sia un MCU, che può supportare più chiamate contemporaneamente, è necessaria l'apertura di più canali H.245 di controllo.

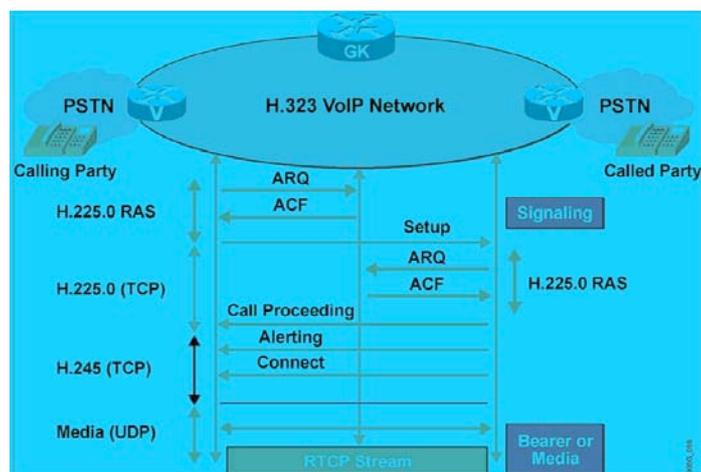


Figura 2. H.323 Protocol.

1.2 Protocollo H320

L'H320 è un protocollo ITU (*International Telecommunication Union*) che fissa le specifiche per definire un'infrastruttura di trasmissione di dati multimediali, quali audio e video, su linee analogiche ISDN utilizzando la compressione H.261/H.263.

Le specifiche per la compressione H.261 prevedono l'uso di uno o più canali a 64kbits al secondo. L'H263 è stato sviluppato come un miglioramento del *codec* H.261.

La Sede Centrale dell'Istituto Nazionale di Geofisica e Vulcanologia in alcuni casi ha necessità di usare tale protocollo quando la controparte della telecomunicazione è vincolata a questo, come nel caso presentato nel paragrafo 4.1 con la Base Antartica Italiana.

2 Architettura della videoconferenza

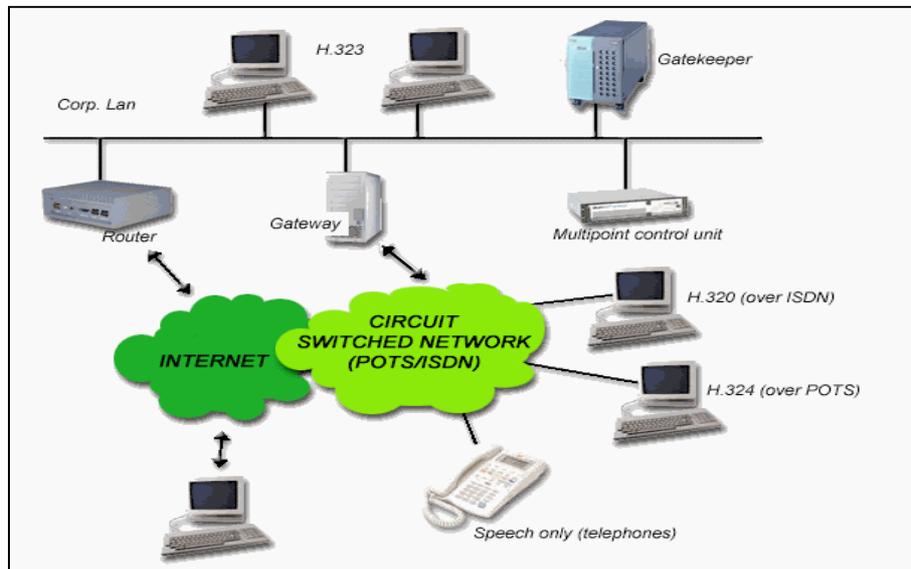


Figura 3. Architettura H.323.

2.1 I terminali

I terminali sono *endpoints* che originano e terminano i flussi di dati e la segnalazione H.323, e sono in grado di instaurare una comunicazione bidirezionale *real-time* con un altro terminale, un *Gateway* o un MCU. Un Terminale H.323 deve supportare obbligatoriamente comunicazioni audio e, facoltativamente, video e dati. Per fare ciò tutti devono supportare i protocolli di controllo per negoziare l'uso del canale (H.245), per l'instaurazione della chiamata (RAS - *Call Signalling*) e per la trasmissione stessa dei pacchetti (RTP), oltre ovviamente ai codificatori/decodificatori per i flussi audio e video (dove possibili) e i protocolli relativi allo scambio di dati.

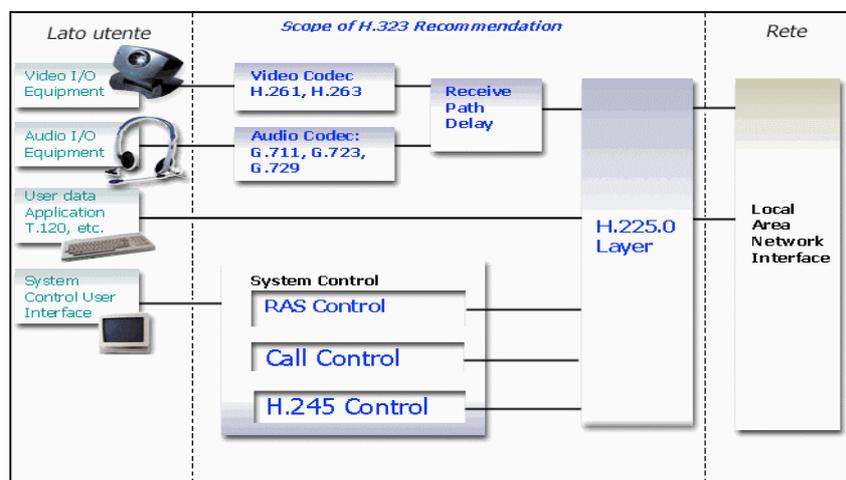


Figura 4. Terminale H.323.

2.2 Gateway

Il *gateway* è un elemento non obbligatorio in una conferenza H.323, ma necessario ogni volta che occorre mettere in comunicazione reti eterogenee tra loro. La connessione avviene tramite traduzione dei protocolli applicativi relativi alle due reti e talvolta anche attraverso la traduzione dei protocolli di trasferimento e la conversione di codifica dei flussi audio/video. Il *gateway* si incarica dell'attivazione e dell'abbattimento della chiamata su entrambe le reti che mette in contatto. Un esempio è quello di un *gateway* che "vede" sia la rete IP che la PSTN (*Public Switched Telephone Network*).

L'aggiunta del *gateway* all'architettura ha dato ad H.323 la possibilità di interfacciarsi con tutte le altre realtà esistenti, e di conseguenza ha permesso allo standard di diffondersi in maniera capillare.

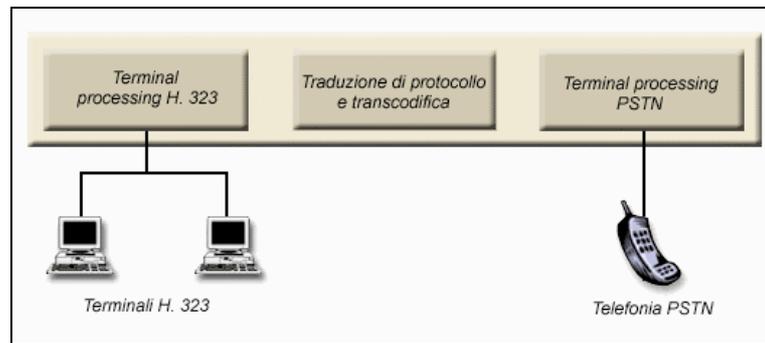


Figura 5. Gateway verso la rete PSTN.

2.3 Gatekeeper

Il *gatekeeper* è il componente centrale dell'architettura: agisce come punto di riferimento per tutte le chiamate all'interno della sua zona e fornisce servizi di controllo di chiamata agli *endpoint* registrati. In particolare, esso può limitare l'accesso al servizio secondo le disposizioni dell'amministratore dello stesso, e la quantità di capacità trasmissiva allocata per le applicazioni multimediali ad un livello tale da non degradare troppo la qualità offerta agli altri servizi (email, trasferimento dati ecc.).

Lo standard definisce in maniera precisa le funzionalità offerte dal *gatekeeper*, alcune obbligatorie e altre opzionali. Tra quelle obbligatorie bisogna citare:

- *Address Translation*: trasformazione di un numero telefonico (E.164) o di un indirizzo alias in un indirizzo IP e viceversa. Esiste, internamente al *gatekeeper*, una tabella delle registrazioni, continuamente aggiornata attraverso i messaggi del protocollo RAS.
- *Admission Control*: controllo di ammissione di un *endpoint* in una Zona H.323. Attraverso i messaggi ARQ (*Admission ReQuest*), ACF (*Admission ConFirm*) e ARJ (*Admission ReJect*), ad un *endpoint* viene permesso o meno l'accesso alla LAN. L'accesso può essere basato su autorizzazioni alla chiamata, banda richiesta o altri criteri.
- *Bandwidth Control*: controllo di banda. Il *gatekeeper* usa i messaggi BRQ (*Bandwidth ReQuest*), BCF (*Bandwidth ConFirm*) e BRJ (*Bandwidth ReJect*) per la gestione della banda disponibile.
- *Zone Management*: controllo dei componenti H.323 appartenenti alla Zona H.323; il *gatekeeper* offre i propri servizi solo a Terminali, Gateway e MCU ad esso registrati.

Tra le funzionalità opzionali del *gatekeeper* possiamo elencare:

- *Call Control Signalling*: in una conferenza punto - punto il *gatekeeper* può processare i segnali di controllo H.225.0 oppure farli scambiare direttamente tra gli *endpoints*.
- *Call Authorization*: il *gatekeeper* può rifiutare una chiamata per motivi ad esempio di mancata autorizzazione. I criteri per determinare queste autorizzazioni sono al di fuori della raccomandazione.
- *Bandwidth Management*: il *gatekeeper* può rifiutare una chiamata se non c'è abbastanza banda disponibile, ma i criteri per definire la banda disponibile vanno al di fuori della raccomandazione. Tale funzione può operare anche dopo la fase di inizializzazione della chiamata, qualora gli utenti decidessero di cambiare il tipo di media che si stanno scambiando nella chiamata in atto.

- *Call Management*: il *gatekeeper* può tenere, ad esempio, una lista degli utenti occupati in comunicazioni.
- *Routing* della segnalazione di chiamata: il *gatekeeper* si fa carico dell'inoltro agli *endpoint* della segnalazione di chiamata. Questo permette, ad esempio, a un *service provider* di monitorare le chiamate sulla rete a scopi di *billing*, oppure di inoltrare chiamate ad altri *endpoint* ove quelli chiamati non siano disponibili, ecc.
- *Routing* del controllo di chiamata: il canale di controllo H.245, invece di essere stabilito tra i due *endpoint*, passa attraverso il *gatekeeper* (H.245 Routed Mode).

2.4 Multipoint Control Unit (MCU)

L'MCU è l'entità che permette a tre o più terminali di partecipare a una conferenza. Se da una parte può essere considerato un Terminale, in quanto può generare e terminare flussi audio e video, dall'altra la differenza è come agisce su questi. Infatti, l'MCU riceve tutti i flussi audio e video dai partecipanti alla conferenza e restituisce a tutti un unico flusso contenente i contributi di ognuno. Per quanto riguarda l'audio, le varie comunicazioni vengono sovrapposte come nella realtà, mentre, per quel che riguarda il video, viene spedita un'immagine di formato standard, ma comprendente al suo interno riquadri più piccoli con i partecipanti alla videoconferenza. Al suo interno sono comprese due parti:

- *Multipoint Controller* (MCU), che gestisce i segnali di controllo (H.245) e stabilisce dei *codec* audio e video comuni a tutti gli *endpoints*, come pure una larghezza di banda sostenibile da tutti i partecipanti alla conferenza. Esso non ha a che fare direttamente con i flussi voce/video.
- *Multipoint Processor* (MVP), che si occupa di processare e mescolare i flussi audio/video.

Esistono vari tipi di conferenza multipunto, e per ognuno di questi l'MCU funziona in maniera differente.

- **Conferenza di tipo centralizzato**: tutti i terminali mandano audio, video e dati all'MCU in modalità punto - punto. Il *Media Controller* gestisce la conferenza usando le funzioni del protocollo H.245, nei messaggi del quale si trovano anche le *capability* dei singoli terminali. Il *Media Processor* effettua l'unione dell'audio e del video dei flussi, e spedisce il flusso risultante a ognuno dei terminali, sempre in modalità punto - punto.
- **Conferenza di tipo decentralizzato**: fa uso del *multicast*. I terminali H.323 che partecipano alla conferenza mandano i flussi audio e video a un indirizzo *multicast*, senza spedirli a un MCU. Quest'ultimo continua a gestire la conferenza usando il controllo H.245: infatti, anche in questo secondo caso, i terminali mandano all'MCU i messaggi H.245 in modalità punto - punto. In questo tipo di conferenza sono i terminali che devono farsi carico del processamento dei segnali audio e video; essi usano i canali di controllo H.245 per indicare all'MCU quanti flussi audio e video sono in grado di decodificare.

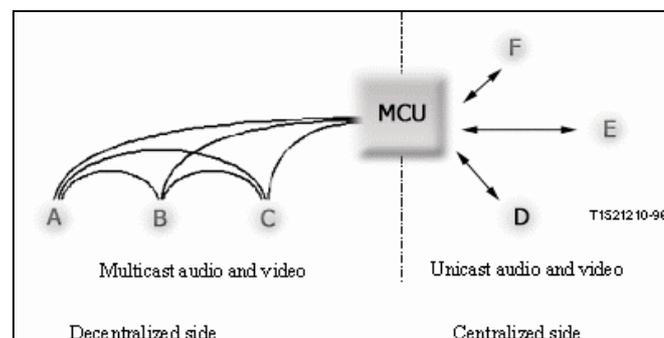


Figura 6. Conferenze multipunto Decentralizzata e Centralizzata.

- **Conferenza di tipo ibrido**: è una combinazione delle due precedenti. La segnalazione H.245 e alcuni dei flussi audio e video vengono mandati all'MCU in modalità punto - punto, mentre i rimanenti flussi audio/video vengono trasmessi in modalità *multicast*.

Il sistema presente in INGV è altamente compatibile e interoperabile con terminali di comunicazione audio e video, MCU e *gatekeeper standard*. Permette di connettere in un'unica rete di videocomunicazione tutti i sistemi di videoconferenza di un ufficio, indipendentemente dal protocollo e dal tipo di rete utilizzata. La famiglia dei *gateway* AETHRA include soluzioni flessibili e scalabili per installazioni centralizzate o distribuite nella propria rete di comunicazione. Il nostro sistema può essere abbinato con l'unità di conferenza multi - punto, applicativi di collaborazione via web, sistemi di prenotazione, moduli di sicurezza e strumenti di *network management*, per realizzare una comunicazione veramente multimediale. Come si può notare nelle figg. 7 e 8 la nostra architettura è di tipo centralizzato. Disponiamo di una unità centrale di controllo (MCU) che fa da *convergence layer* per più tipi di applicazioni e protocolli, quali IP, ISDN , SIP , H324.

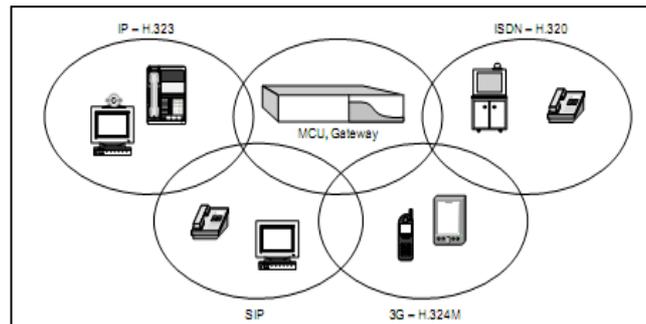


Figura 7. Componenti del Sistema.

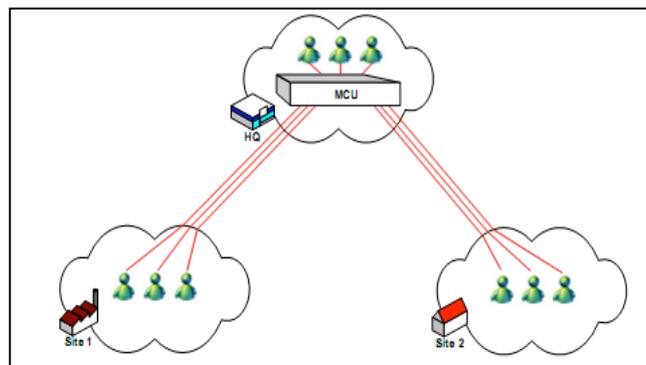


Figura 8. Architettura Centralizzata.

3 Integrazione tra la rete INGV, le sedi e la videoconferenza

Le sedi INGV quali Milano, Bologna, Pisa, Roma, Napoli, Palermo, Catania, hanno a disposizione i *client hardware* del sistema composti da videocamera e televisore, mentre per le altre sedi come ad es. Grottaminarda è possibile utilizzare un *client software*. Tutti i *client* sono collegati verso l'MCU (fig.9), ed è possibile gestire da remoto ed in automatico gli interventi delle varie sedi. Nel caso in cui una sede non disponga dell'*hardware*, si può procedere all'installazione sia di *software* proprietario che utilizzare *software open source* che sfrutti il protocollo standard H323.

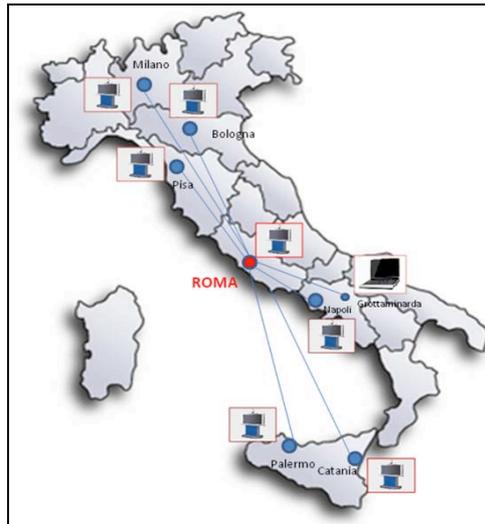


Figura 9. Rete della Videoconferenza Sedi INGV.

L'INGV sede di Roma è il nodo centrale del sistema di videoconferenza a cui afferiscono le altre sedi. Qui sono stati installati il *gatekeeper*, l'MCU e l'MVP che costituiscono il *core* della comunicazione. Gli apparati si trovano su di una rete pubblica a 60 Mb/s, non mascherati dal *firewall* e per garantire la sicurezza, le reti delle altre sedi sono in *trust* solo sulle porte strettamente necessarie al corretto funzionamento. Le sale di interesse della sede romana sono state dotate di opportune porte ethernet che in *Virtual LAN* sono esposte in rete pubblica.

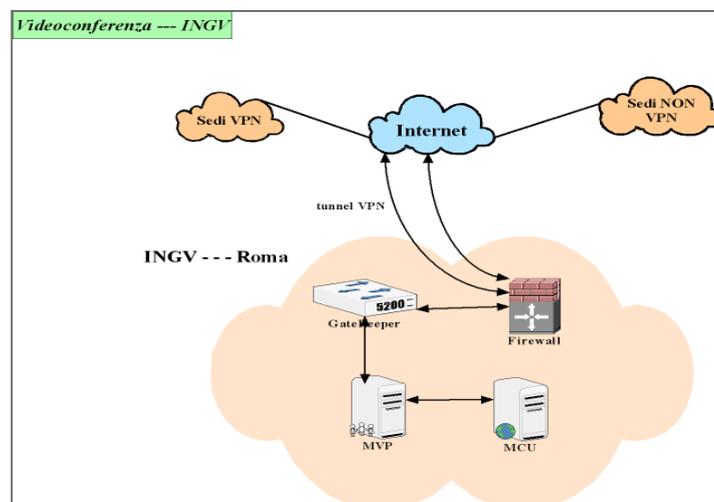


Figura 10. Rete della Videoconferenza Sede di Roma.

Uno dei ruoli fondamentali dell'INGV è quello di programmare e gestire le varie attività di videoconferenza, con la possibilità di estendere questo servizio anche ad altri enti sia nazionali che internazionali, mantenendo gli *standard* di sicurezza adeguati. La programmazione comprende anche l'invio, sfruttando il servizio di posta elettronica istituzionale, di inviti ai partecipanti di una determinata videoconferenza.

La gestione avviene via web ed è visibile all'indirizzo <http://teleconferenza.rm.ingv.it:8080>.

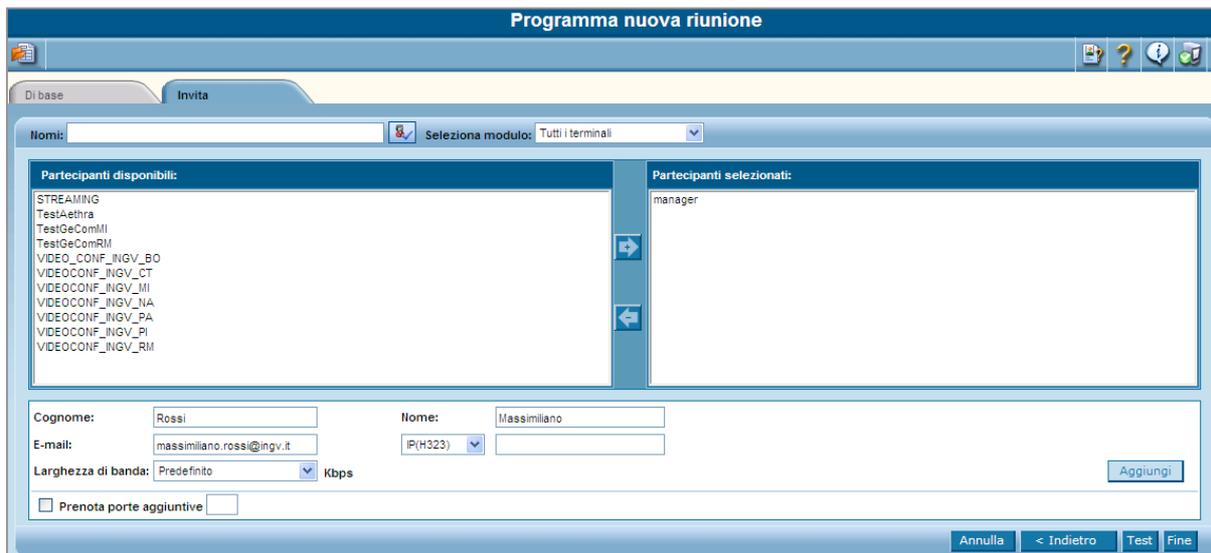


Figura 11. Programmazione Videoconferenza.

4 Applicazioni

Il sistema di videoconferenza ha trovato un ampio utilizzo presso l'INGV, in particolar modo in convegni, riunioni di Unità di Progetto e dei TTC (Temi Trasversali Coordinati) dell'INGV, riunioni del personale tra le varie sedi, etc. ed è uno strumento in continua crescita per nuove iniziative che possano mettere in evidenza le attività svolte dall'Ente. Inoltre, in caso di evento sismico o vulcanico significativo di rilevanza nazionale, le tre sedi di monitoraggio sono ora in grado di utilizzare il servizio per collegare le varie unità di crisi come pure attivare dei punti di emergenza in loco così da raggiungere le zone interessate (*crisis management* di moderna concezione). Seguono alcuni casi significativi che abbiamo sperimentato sino ad oggi.

4.1 Collegamento con l'Antartide

Evento importante è stato un video collegamento con le nostre basi al polo sud in occasione del convegno su "osservatori geofisici in Antartide e tecniche di radiocomunicazione digitale", tenuto in Roma il 25 novembre 2008 (fig. 12). Questo collegamento è stato stabilito tramite il protocollo H320 (ISDN come in paragrafo 1.2). A tale evento ha partecipato anche il Presidente Emerito Francesco Cossiga da casa tramite applicativo *software* con supporto del SIR.



Figura 12. Collegamento ISDN con Antartide.

4.2 Incontro con il ministro Gelmini

Una videoconferenza di rilievo si è tenuta in occasione della visita del ministro M. Gelmini, incontro molto sentito per la questione del precariato all'INGV (fig. 13).



Figura 13. Incontro con il ministro Gelmini.

5 Streaming

Nella gestione della videoconferenza abbiamo sviluppato un sistema per la trasmissione via *streaming* degli eventi, per dare la possibilità di assistere anche solo in maniera passiva a convegni e conferenze in cui non è necessaria una interazione paritetica. Il vantaggio di tale sistema risiede sempre nell'azzeramento dei costi di viaggio, pernottamento e dei vari spostamenti del personale.

5.1 Architettura del sistema di streaming

Lo "*streaming*" identifica un flusso audio/video trasmesso da una sorgente a una o più destinazioni utilizzando la rete telematica.

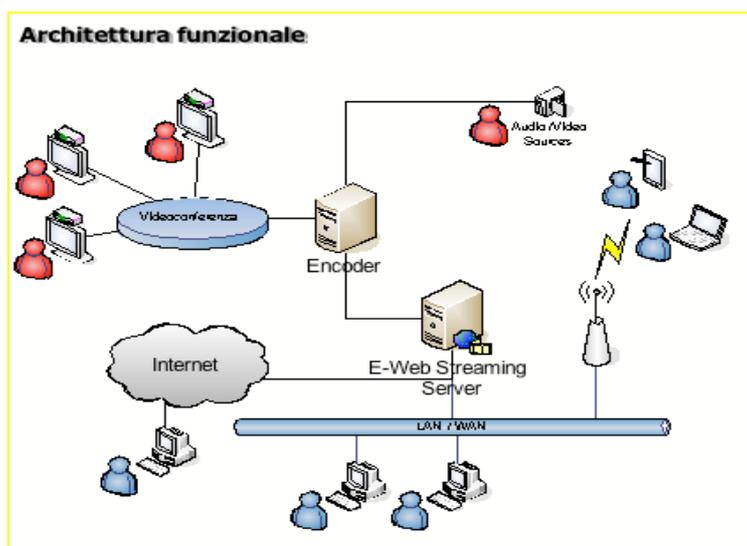


Figura 14. Architettura Streaming.

I contenuti audio/video sono compressi e memorizzati su un *server* come *file*. La richiesta di questi contenuti viene effettuata dall'utente che non deve scaricarli per intero sul PC per poterli riprodurre: i dati ricevuti vengono decompressi e riprodotti pochi secondi dopo l'inizio della ricezione. Questo ritardo iniziale ha lo scopo di rimediare ai ritardi o microinterruzioni della rete.

L'utilizzo dello *streaming* sfrutta una piattaforma con un'interfaccia utente *web-based* per la gestione completa di eventi *Live* (in diretta) e *On-Demand* (in differita).

La piattaforma è in grado di trasmettere sia eventi di videoconferenza, sia eventi direttamente ripresi da sorgenti Audio/Video, siano esse analogiche o digitali (Telecamere, DVD, etc.).

L'architettura scalare di *E-WebStreaming/TC* la rende estremamente flessibile; in particolare, con specifico riferimento a quanto richiesto nel Capitolato Tecnico, lo *streaming server hardware* è proposto in 2 configurazioni per supportare le seguenti capacità:

- 25 flussi contemporanei con il massimo *bitrate*
- 100 flussi contemporanei a 512 Kbps

Tramite la piattaforma offerta è possibile gestire una agenda di eventi, prenotare risorse dedicate agli eventi, amministrare gruppi di partecipanti e notificare automaticamente la richiesta di partecipazione all'evento.

La piattaforma include inoltre un sistema di autenticazione e permette la creazione del profilo degli utenti, per garantire la più completa sicurezza e riservatezza, che è basato su tre livelli:

1. Autenticazione utenti (*login* di sistema)
2. Controllo fisico su IP
3. Controllo di sessione.

Inoltre il sistema si integra in un'eventuale architettura *Active Directory* già esistente.

Sono definiti tre profili di accesso al sistema:

1. *Administrator*: è un utente amministrativo che gestisce la piattaforma.
2. *Scheduler*: è un utente abilitato alla creazione, configurazione e modifica di eventi *live* e *on-demand*. *E-WebStreaming T/C* consente infatti agli utenti autorizzati di inoltrare direttamente richieste di prenotazione eventi.
3. *User*: è l'utente generico abilitato alla visione della propria agenda di eventi ed alla fruizione degli stessi.

E-WebStreaming/TC integra inoltre un modulo di amministrazione semplice ed intuitivo, completamente *web-based*. L'interfaccia grafica di *E-WebStreaming/TC* è personalizzabile e personalizzabile da parte degli amministratori di sistema al fine di integrarla all'interno di portali esistenti.

Il sistema è inoltre multilingua (Italiano ed Inglese) configurabile a livello utente.

5.2 Gestione eventi Streaming

Dopo aver effettuato l'accesso alla piattaforma *E-WebStreaming* la prima *form* è per la gestione degli eventi, suddivisa in quattro sotto cartelle.

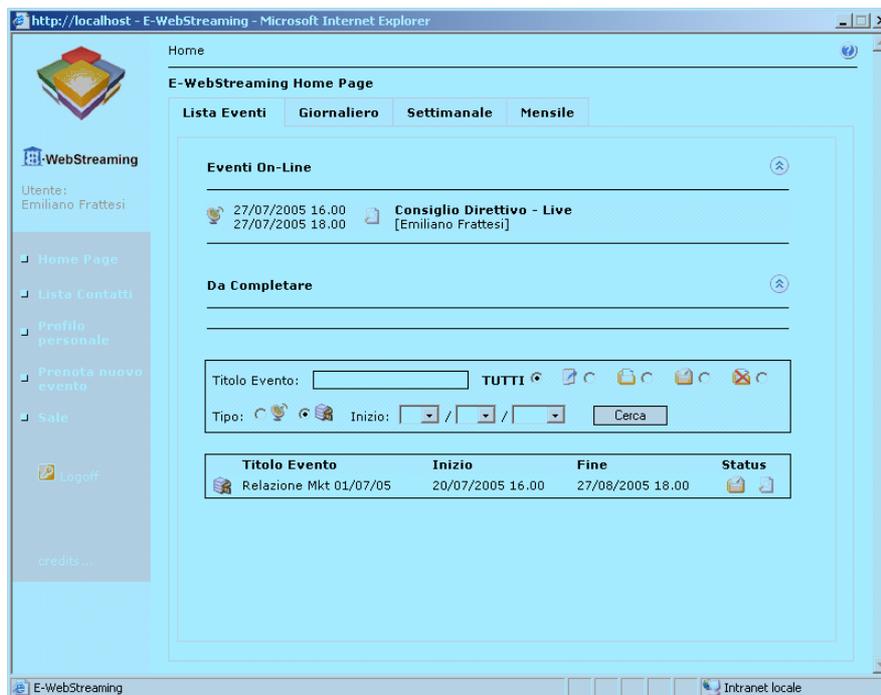


Figura 15. E-WebStreaming.

La cartella "Lista Eventi" è suddivisa in tre sotto sezioni principali:

- Lista di eventi in corso
- Lista eventi da completare
- Motore di ricerca eventi

Lista di eventi *Live* e *On-Demand* in corso: è la lista degli eventi che sono in corso e a quali si è stati invitati. In particolare per ogni evento viene indicato:

-  Simbolo per gli eventi di tipo *Live*
-  Simbolo per gli eventi di tipo *On-demand*
-  Simbolo per visualizzare i dettagli dell'evento

Per ogni evento viene inoltre indicata la data e ora di inizio e di fine, il titolo dell'evento e chi ha prenotato l'evento. Selezionando il titolo dell'evento, l'utente verrà collegato direttamente alla pagina di visione dell'evento. Selezionando "Dettagli dell'evento" viene aperta una pagina riassuntiva dei dettagli dell'evento e in particolare viene indicato:

- Titolo della conferenza - nome assegnato all'evento;
- Creatore - persona che ha prenotato l'evento;
- Inizio - data e ora di inizio dell'evento;
- Fine - data e ora di fine dell'evento;
- Descrizione - breve commento all'evento;
- Opzioni - vengono descritte le opzioni disponibili durante l'evento e in particolare:
 - 🌐 audioconferenza: durante l'evento è possibile collegarsi ad una *conference call* tramite normale apparecchio telefonico per poter interagire con i presentatori;
 - 💬 *chat room*: durante l'evento è possibile utilizzare una chat integrata per poter interagire con i partecipanti;
- Allegati: è possibile scaricare e/o visualizzare i documenti che il promotore del servizio ha allegato alla presentazione;
- Relatori: lista delle persone che condurranno l'evento;
- Partecipanti: Lista Utenti che sono stati invitati a partecipare all'evento;
- Partecipanti: Lista Gruppi che sono stati invitati a partecipare all'evento.

6 Utilizzo operativo e risparmio di gestione

Come si può notare dalle figure 16 e 17, abbiamo utilizzato, alla data di compilazione della presente, il sistema per una durata complessiva di 144 ore e con una media di cinque sedi partecipanti, con un picco di due videoconferenze contemporanee. Considerando che gli spostamenti di personale tra le varie sedi implicano una spesa media, tra pernottamento e trasferimento di circa 800 euro, facendo un calcolo approssimativo possiamo affermare di aver risparmiato fino a luglio 2009 intorno ai 25000 euro. Questa operazione si è resa possibile sfruttando la sola infrastruttura di rete esistente.

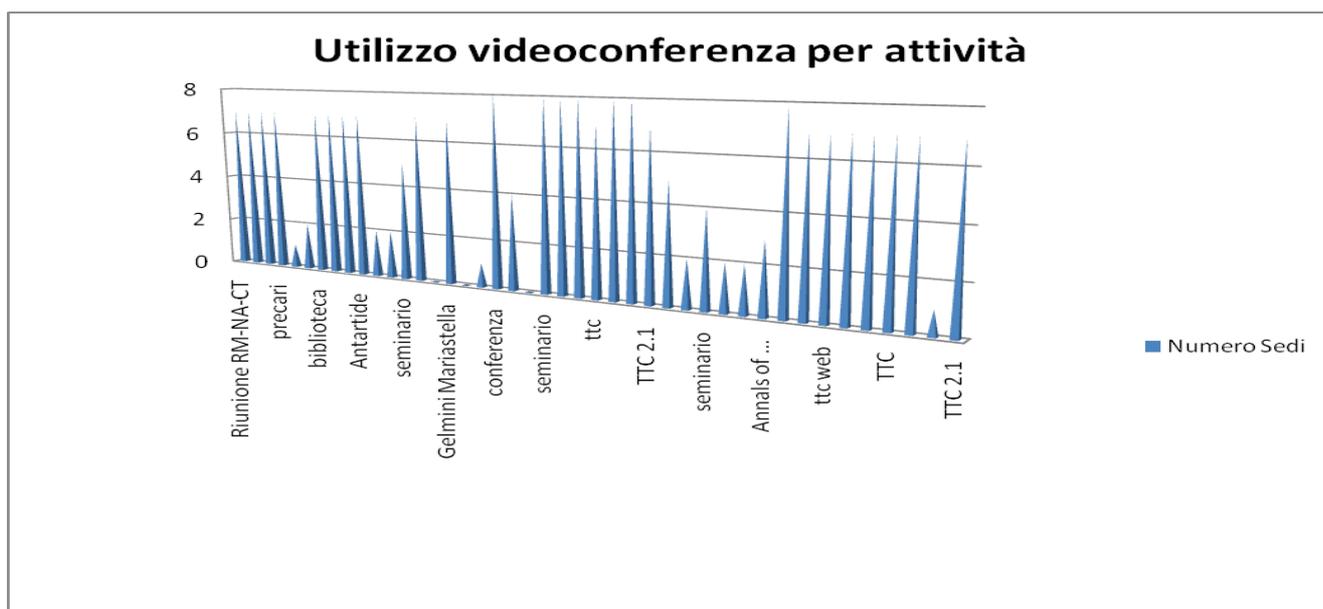


Figura 16. Utilizzo per attività.

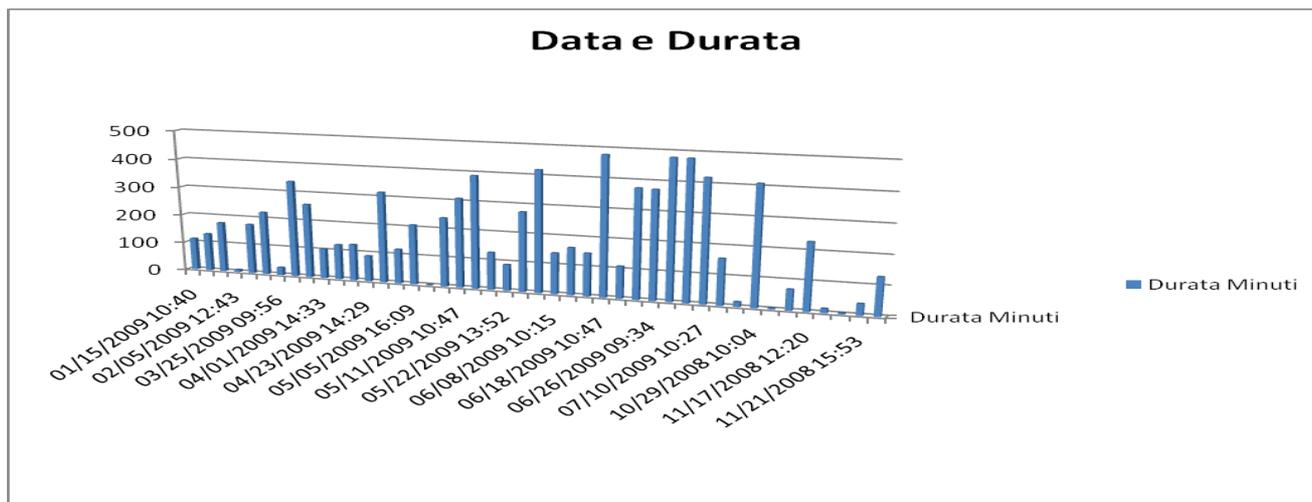


Figura 17. Data e Durata VideoConferenze.

6.1 Effetti della latenza, del jitter e della perdita di pacchetti sulla qualità della videoconferenza

6.1.1 Latenza (Ritardo di Trasferimento)

La latenza di rete è definita come il tempo impiegato da un determinato flusso di dati ad andare dall'interfaccia di rete di un terminale all'altro. La latenza è data dalla somma di diversi addendi: ritardo di propagazione, ritardo di elaborazione, ritardo di trasmissione, ritardo di permanenza in coda, ecc. per ciascun nodo attraversato. In una WAN il ritardo di permanenza in coda è in genere il fattore più critico, dovuto alla congestione sui *router*; politiche di controllo della priorità, della lunghezza dei pacchetti e delle congestioni influenzano il tempo di latenza effettivo. La latenza non influenza la qualità del particolare flusso audio o video, bensì la dinamica della conversazione, rendendo molto difficoltosa l'interattività. Inoltre quando il tempo di latenza è elevato l'eco può risultare particolarmente elevato e difficile da cancellare. La codifica del video, in videoconferenze altamente interattive, è responsabile della maggior parte del tempo di ritardo totale; il ritardo di codifica è più fastidioso a bassi *bit rate* e in presenza di transcodifica. In tali casi è richiesto che la latenza della rete sia particolarmente bassa. Reti IP di elevata qualità sono in grado di contenere il ritardo di permanenza in coda entro i 10 ms; come regola generale, la latenza di rete non dovrebbe mai superare i 100 ms.

6.1.2 Jitter

Quando un flusso di pacchetti attraversa una rete IP, i ritardi non sono costanti bensì variabili per ciascun pacchetto. Il terminale ricevente deve ricostruire un flusso di pacchetti costante per poter decodificare l'audio e il video. Ciò si ottiene attraverso un *buffer* di *dejittering*, la cui lunghezza è stabilita in base a una stima del *jitter* di picco rilevato nella rete. Ogni pacchetto RTP è contrassegnato con *time-stamp* che consentono la risincronizzazione del flusso e il riordinamento dei pacchetti. Sfortunatamente il *buffer* di *dejittering* ha come effetto collaterale l'aumento del tempo di ritardo totale, per cui è bene che sia il più corto possibile. Nelle sessioni di videoconferenza il *jitter* non costituisce un problema per l'audio, in quanto questo viene già ritardato per sincronizzarlo con il video (*lip sync*), mentre può portare a perdite di trame video se il *jitter* effettivo è superiore a quello stimato.

6.1.3 Perdita di pacchetti (*Packet loss*)

La perdita di pacchetti può avvenire a causa della congestione nei *router*, a causa della presenza di errori di trasmissione o perché i pacchetti arrivano oltre un certo *time-out*. La videoconferenza H.323 usa un trasporto "inaffidabile" (*stack* RTP/UDP/IP), in quanto lo schema *acknowledge*/ritrasmissione di un trasporto affidabile (TCP/IP) comporterebbe un tempo di ritardo intollerabile per applicazioni interattive. La perdita di pacchetti ha un impatto diretto sulla qualità della videocomunicazione, provocando fenomeni quali: immagini con scacchi, video a scatti o bloccato, audio rumoroso o a scatti. I terminali di videoconferenza si scambiano informazioni

sulla perdita dei pacchetti e cercano di contrastarla abbassando il *bit rate*, cosa che in ogni caso si ripercuote sulla qualità. Nei casi in cui sia probabile la perdita di pacchetti, è preferibile per la codifica audio scegliere in primis G.711, poi G.722 e infine G.728. Con la codifica G.711 la qualità dell'audio è accettabile in presenza di perdita di pacchetti bassa o moderata. Per il video, la perdita dei pacchetti dovrebbe restare al di sotto dell'1% per una buona qualità e non superare mai il 3% per avere una qualità accettabile. L'elevata perdita di pacchetti può rendere molto lento anche il *set-up* della comunicazione.

7 Appendice - il sistema di prenotazioni integrato

Per rendere fruibile e ben organizzate le sessioni di videoconferenza con le varie sale dell'INGV, il SIR, su richiesta del TTC 2.1, ha sviluppato un sistema per la gestione e prenotazione delle sale adibite a video conferenza, all'indirizzo web <http://prenotazioni.rm.ingv.it>, il cui Rapporto Tecnico è in corso di sottomissione, figg. 18 e 19. Questo sistema è comunque quello ufficiale per la prenotazione delle sale riunioni della sede di Roma dell'INGV e delle sue collegiate.

Figura 18. Sistema di prenotazioni.

Figura 19. Servizio aggiuntivo videoconferenza.

Bibliografia

[SIR, 2009]: Massimiliano Rossi, Emanuele Sammali, Manuela Sbarra, Gianpaolo Sensale, Diego Sorrentino, Francesco Zanolin, Lucio Badiali, Francesca Caprara, Pierluigi Cau, Pietro Ficeli, Melissa Mendicino (2009). *Rete Informatica INGV Roma*, Rapporti Tecnici INGV n. 107.

[Kurose-Ross, 2003]: Internet e reti

Coordinamento editoriale e impaginazione

Centro Editoriale Nazionale | INGV

Progetto grafico e redazionale

Laboratorio Grafica e Immagini | INGV Roma

© 2009 INGV Istituto Nazionale di Geofisica e Vulcanologia

Via di Vigna Murata, 605

00143 Roma

Tel. +39 06518601 Fax +39 065041181

<http://www.ingv.it>



Istituto Nazionale di Geofisica e Vulcanologia