INDICE

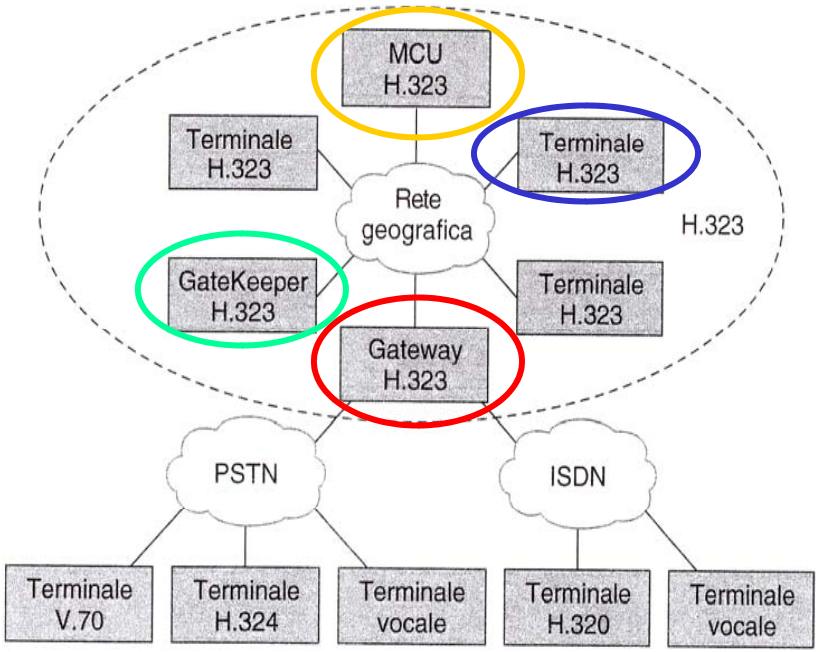
- Motivazioni
  - Integrazione dei servizi
  - Vantaggi e problemi aperti
- Architettura di riferimento
- La codifica vocale
- Il trasporto
  - RTP e RTCP
  - QoS in reti IP e VoIP requirements
- *La segnalazione*
  - *H.323*
  - *SIP*
- *Cenni su VoIP reliability*
- Problemi del VoIP con NAT e firewalls
- Qualità della voce
- Valutazione oggettiva della qualità della voce
  - L'algoritmo PESQ

LA SEGNALAZIONE e CONTROLLO di CHIAMATA

- H.323
  - Raccomandazione ITU-T, sviluppata da uno standard per comunicazioni multimediali (telefonia video) su reti a pacchetto

- SIP
  - Protocollo di segnalazione-controllo simile a http, pensato per reti IP e terminali intelligenti coinvolti in sessioni voce (ed anche in altri tipi di applicazioni)
  - Impiega il paradigma client-server

PRINCIPALI ELEMENTI DI H.323



- Terminali
  - Forniscono le funzionalità di comunicazione, punto-punto e punto-multipunto
- Gateways
  - Connettono alla rete telefonica commutata (PSTN) o alla rete ISDN
- Gatekeepers
  - Garantiscono i servizi di controllo di ammissione ed i servizi degli indirizzi per i terminali o i gateway
- Unità MCU (Multipoint Control Units)
  - Consentono a due o più terminali o gateway di attivare conferenze tramite sessioni audio e/o video

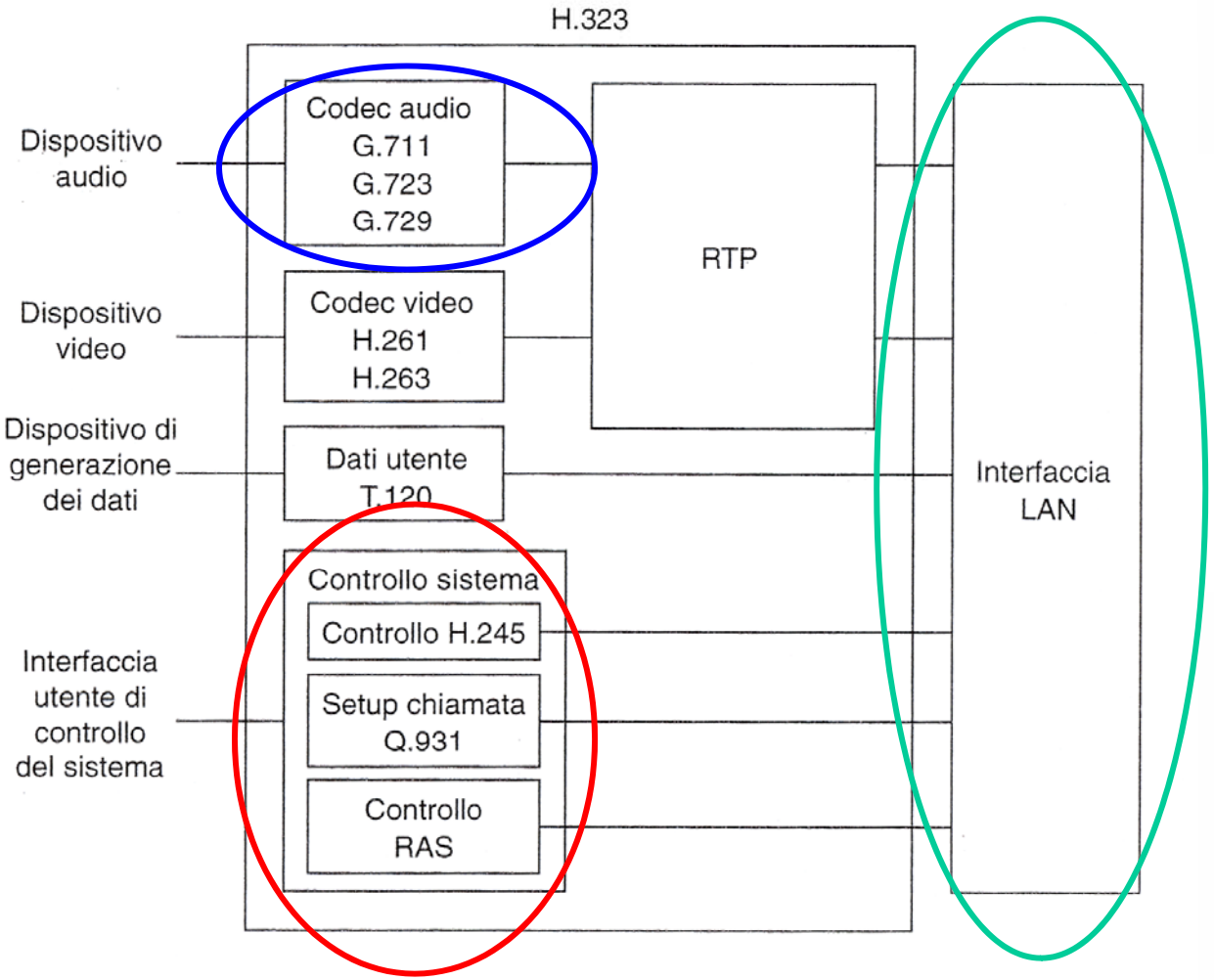
IL TERMINALE

Include i seguenti elementi funzionali:

- Codec audio
- Unità di controllo di sistema: gestisce
  - il setup della chiamata
    - ✓ Via protocollo Q.931
  - il controllo della chiamata
    - ✓ via protocollo H.245

    Tale protocollo negozia vari aspetti della connessione
    - Quale algoritmo di compressione
    - Quale bit-rate
- Unità per la formattazione di tutti i flussi trasmessi all'interfaccia di rete (audio, video, controllo, eventualmente dati) e per la ricezione dei flussi dall'interfaccia di rete
  - Flussi audio: formato dettato dal protocollo H.225.0
  - Sequence numbering, error detection e error correction
- Interfaccia di rete, che consente servizi TCP e UDP

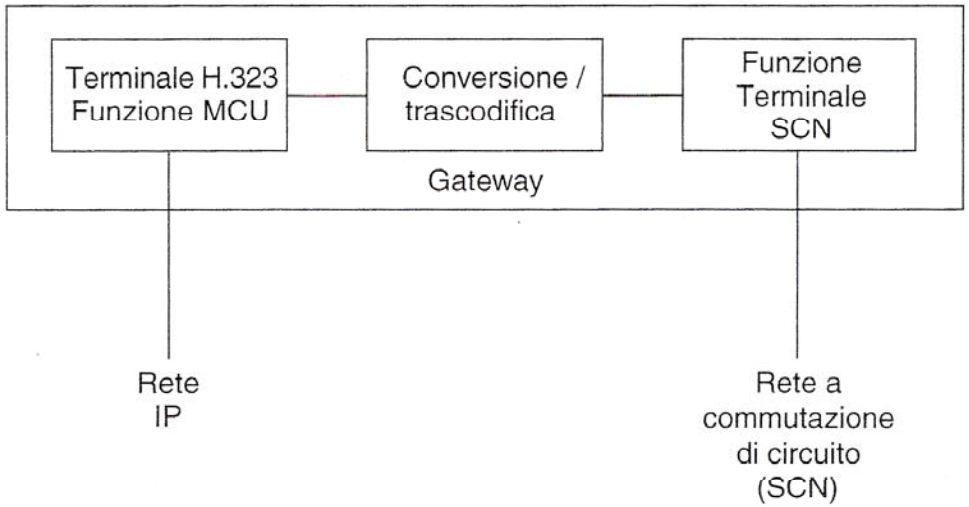
SCHEMA FUNZIONALE



IL GATEWAY

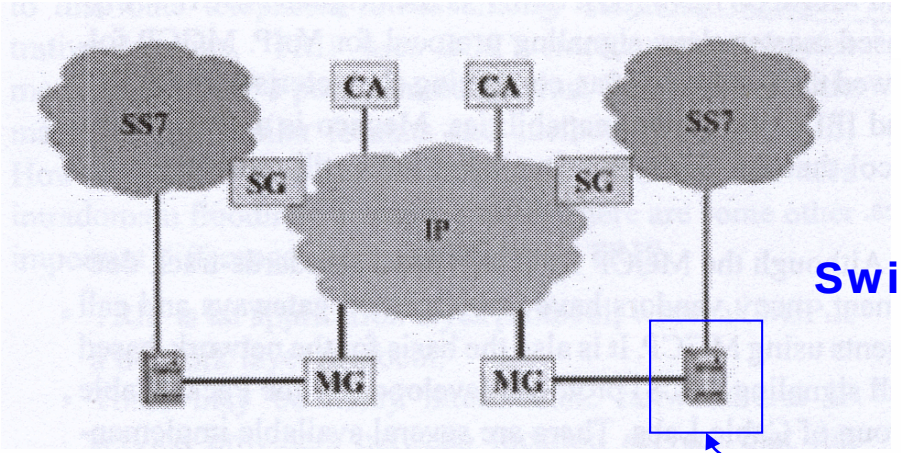
- Un gateway fornisce
  - Traslazione di protocollo (formati e segnalazione diversi) tra un endpoint H.323 e un endpoint che tale non è
  - Può inoltre contemplare operazioni di transcoding e di compressione

ESEMPIO:



GATEWAY VoIP

- I gateway impiegati dal VoIP sono in realtà di due tipi
  - MEDIA gateway MG
    - ✓ Accetta voce o altro tipo di traffico multimediale dagli switch a commutazione di circuito e pacchetizza la voce per trasmetterla sulla rete IP
    - ✓ CONSENTE CONNESSIONI tra RETI DISSIMILI fornendo MEDIA CONVERSION e/o FUNZIONALITÀ di TRANSCODING
  - SIGNALING gateway SG
    - ✓ Esegue operazioni di relay, traslazione e terminazione dei segnali di controllo tra la rete a pacchetto e quella a commutazione di circuito



NOMENCLATURA ...

- Il Call Agent è l'applicazione che controlla i gateway ed esegue il call processing
  - Spesso referenziato come media gateway controller
  - Può controllare più di un gateway
  - Non necessariamente è co-locato vicino ad un gateway
  - Deve tuttavia comunicare con questo per controllarne le funzioni
- SGCP (Simple Gateway Control Protocol)
  - ✓ originario
- MGCP (Media Gateway Control Protocol)
- e Megaco/H.248
  - ✓ IETF, più recente

  sono i protocolli sviluppati per questo tipo di comunicazioni

IL GATEKEEPER

Presenta le seguenti funzionalità fondamentali:

- Gestione di zona (Zone management)
  - Un terminale si può registrare presso un solo gatekeeper
  - Tale gatekeeper fornisce le funzioni esposte nel seguito ai terminali e ai gateway registrati presso di lui
- Traduzione di indirizzi
  - da indirizzi E.164 a indirizzi di trasporto
- Controllo di ammissione
  - Il gatekeeper autorizza l'accesso alla rete (con messaggi H.225)
- Controllo di banda
  - Controlla quanta banda un terminale può impiegare

I terminali comunicano con il gatekeeper attraverso il protocollo H.225

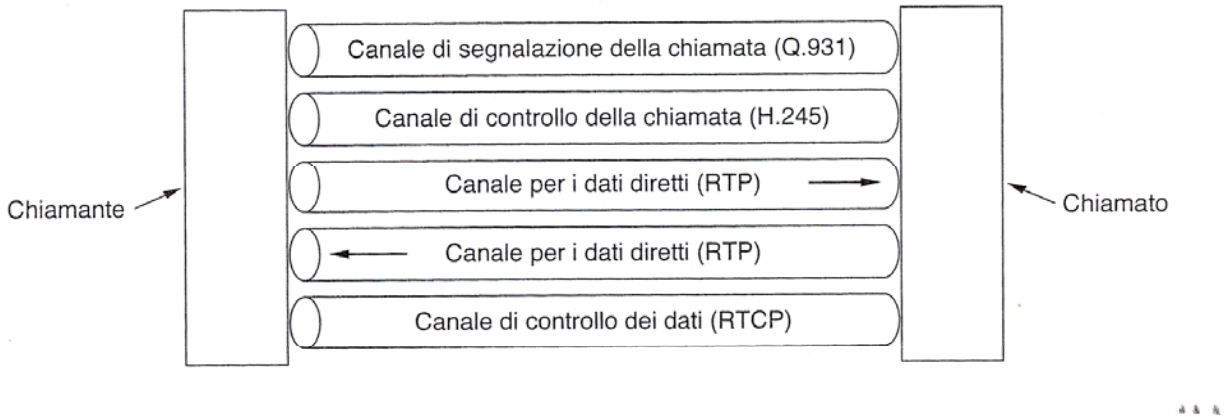
Gatekeeper e Canale RAS

- Il RAS Channel (Registration, Admissions and Status Channel)
  - È il canale logico che trasporta i messaggi impiegati
    - ✓ Nel processo di registrazione di un endpoint con il gatekeeper di zona
      - – associa l'alias di endpoint (tipicamente l'indirizzo E.164) con il suo indirizzo e porta TCP
  - È inoltre impiegato per la trasmissione dei messaggi di
    - ✓ ammissione
    - ✓ modifica di banda
    - ✓ status
    - ✓ disconnessione dell'endpoint dal suo gatekeeper

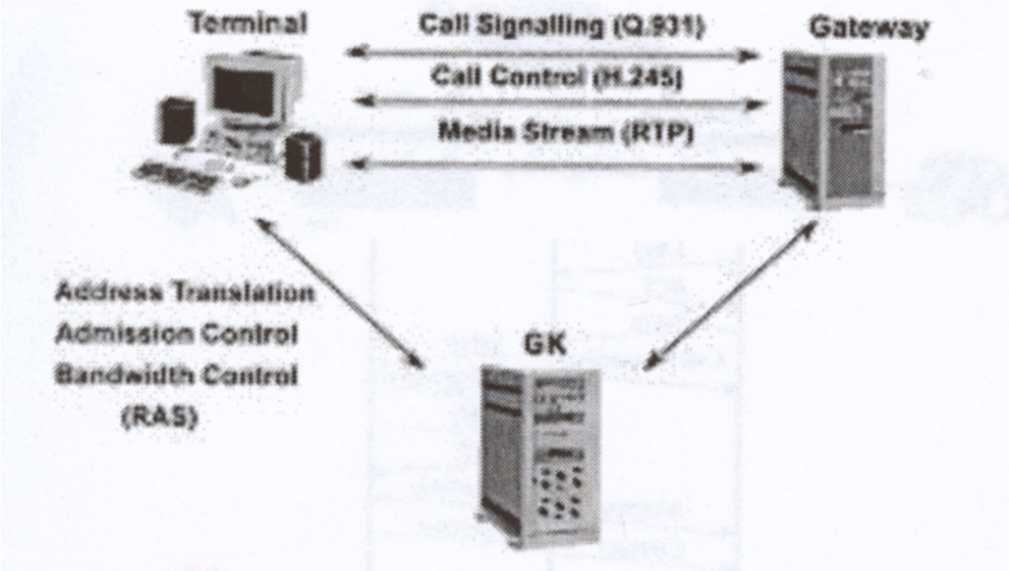
STACK PROTOCOLLARE H.323

<table>
<tr><td>Parlato</td><td colspan="4">Controllo</td></tr>
<tr><td>G.7xx</td><td rowspan="2">R TCP</td><td rowspan="2">H.225
(RAS)</td><td rowspan="2">Q.931
(segnalazione
chiamata)</td><td rowspan="2">H.245
(controllo
chiamata)</td></tr>
<tr><td>RT P</td></tr>
<tr><td colspan="3">UDP</td><td colspan="2">TCP</td></tr>
<tr><td colspan="5">IP</td></tr>
<tr><td colspan="5">Protocollo dello strato data link</td></tr>
<tr><td colspan="5">Protocollo dello strato fisico</td></tr>
</table>

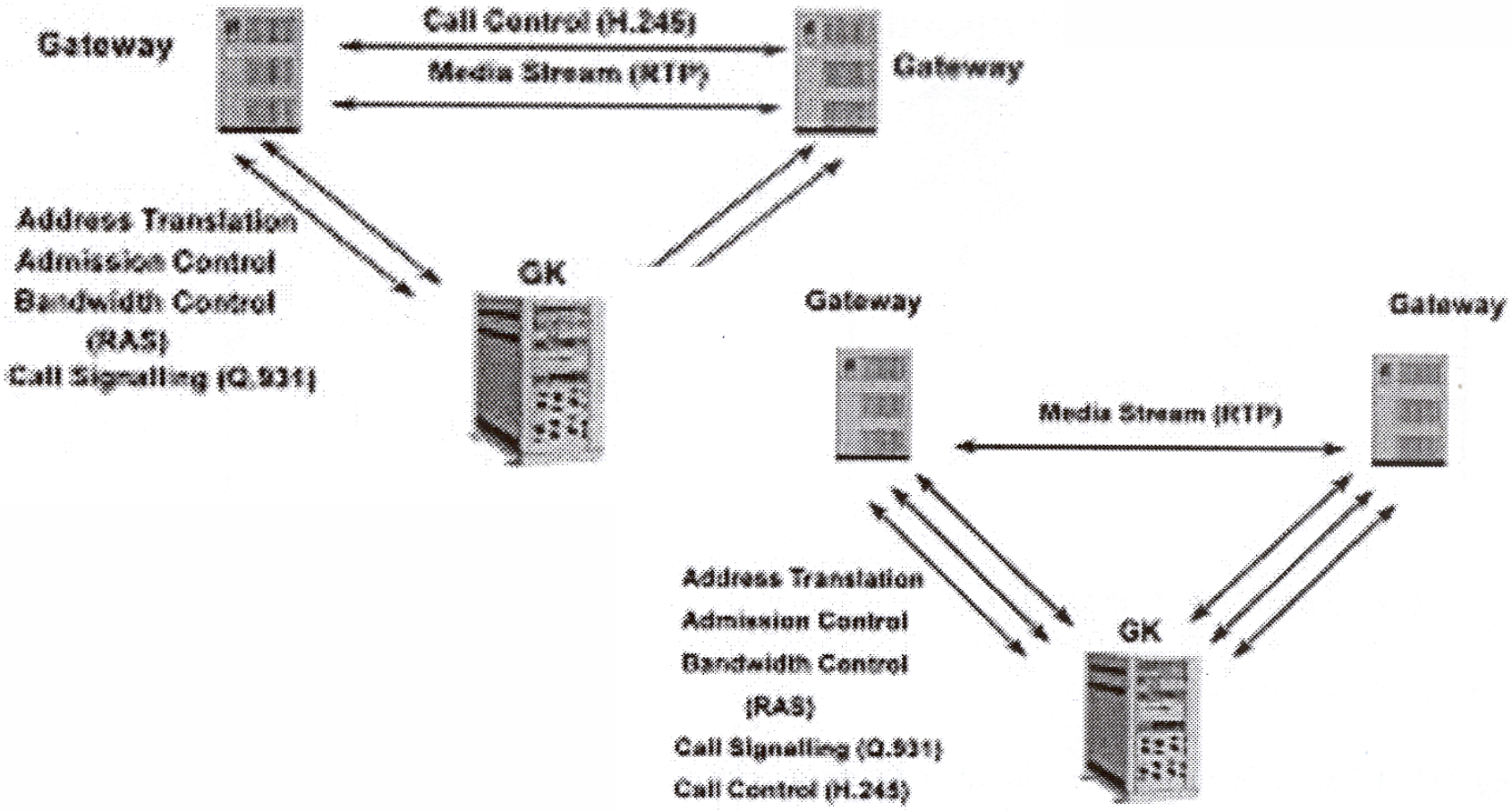
- Endpoint H.323 e gatekeepers impiegano messaggi Q.931 per la segnalazione di chiamata (call signaling)
  - Stabilire e rilasciare la connessione
  - Fornire i toni di composizione
  - Produrre gli squilli
- Il controllo di chiamata (call control) viene invece attuato attraverso il canale logico di controllo H.245
  - Funzione chiave: capabilities exhange
  - Apertura e chiusura di canali logici, controllo di flusso, …
- Viene aperto un canale H.245 per ogni chiamata cui l'endpoint partecipa, e rimane aperto per l'intera durata della chiamata



- Nelle reti senza gatekeepers gli endpoint inviano i messaggi di call signaling direttamente all'altro endpoint
- Se la rete ha un gatekeeper, l'endpoint chiamante invia il messaggio di ammissione iniziale al gatekeeper
  - Il gatekeeper comunica all'endpoint se inviare i messaggi di call signaling direttamente all'altro end-point
    - In tal caso il gatekeeper può processare un numero elevato di chiamate, ma
    - presenterà una capacità limitata di eseguire funzioni di management (call completion rates, call detail recording, …)



- Oppure se eseguirne il routing attraverso il gatekeeper

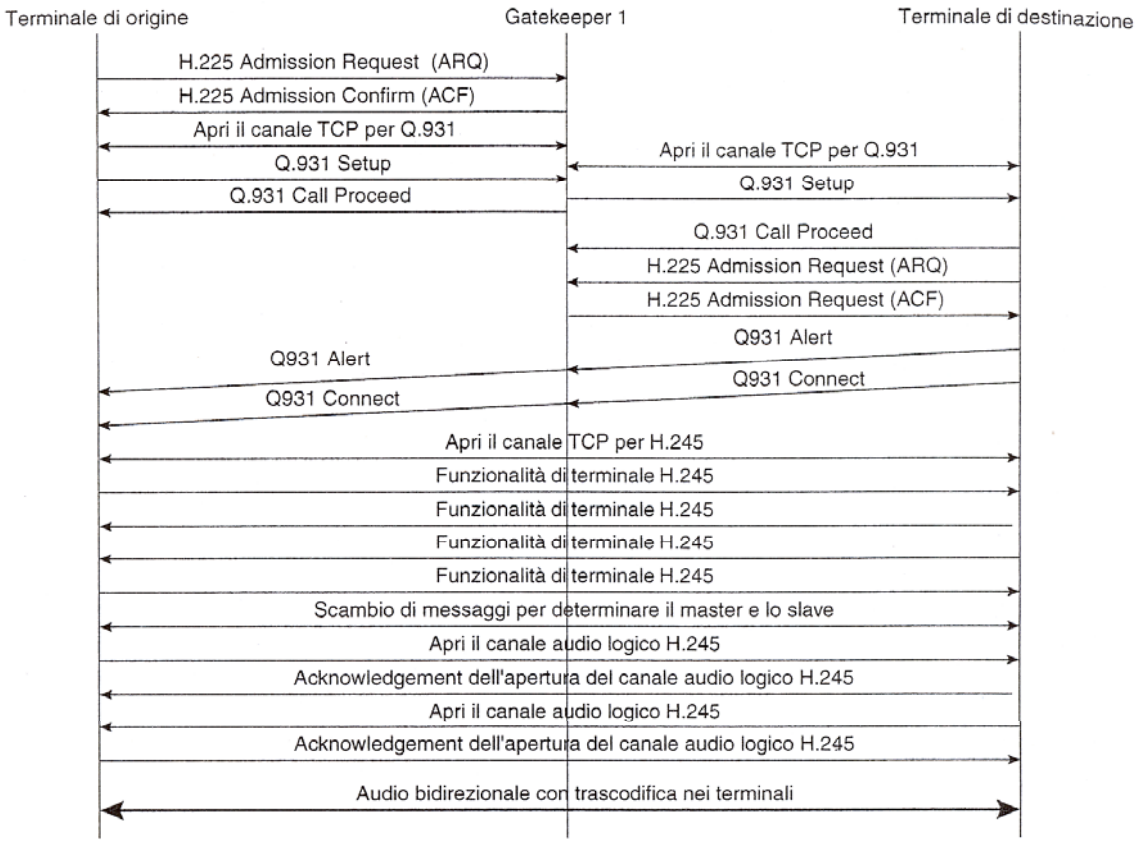


Esempio di segnalazione via unico gatekeeper

Ipotesi:

✓chiamate vocali

✓Gli endpoint hanno già completato la fase di registrazione con il gatekeeper appropriato



SIP RFC 2543

- Il Session Initiation Protocol è un protocollo simile a http
  - Si tratta di un protocollo di segnalazione e controllo che opera a livello applicazione
  - Impiegato per aprire, gestire e chiudere *sessioni multimediali*

- Modello client-server
  - Il client invia una SIP request, che dà inizio ad una transazione
  - La richiesta invoca una funzione del server (metodo)
  - Il server
    - ✓ accetta la SIP request
    - ✓ Esegue il requested method (REGISTER, INVITE, ACK, CANCEL, BYE, OPTIONS)
    - ✓ Risponde

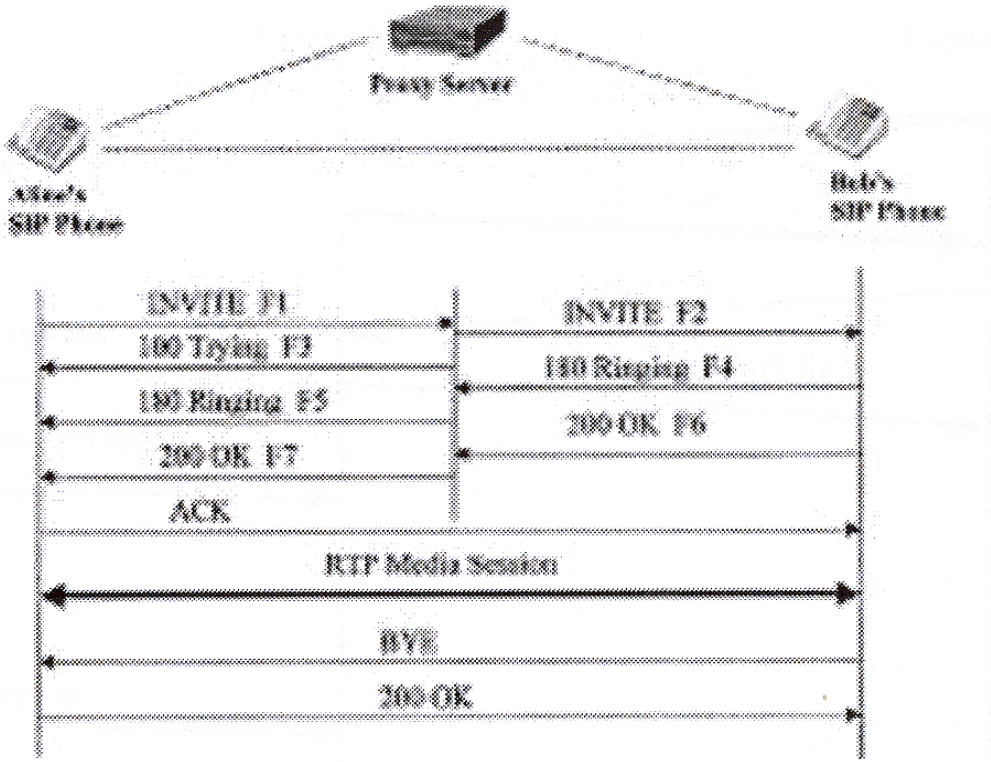
Entità funzionali

- **User agent**
  - sono applicazioni operanti nel sistema terminale
    - ✓ Possono richiedere l'inizio di una sessione (operano come client)
    - ✓ Oppure rispondere ad una richiesta (operano come server)
- **SIP proxy**
  - Instradano i messaggi di segnalazione tra il terminale chiamante ed il terminale chiamato
- **Registrar**
  - È un server SIP che riceve, autentica e accetta REGISTER requests dai SIP clients
  - Tiene traccia degli utenti all'interno del proprio dominio
  - Può essere co-locato con un SIP-proxy server
  - Analogia con GK H.323 !

- **Location server**
  - Memorizza informazioni di utente in un database e consente di determinare a quale indirizzo IP inviare una richiesta
  - Può essere co-locato con un SIP proxy server
- **Redirect server**
  - Risponde ad una richiesta SIP fornendo al client l'indirizzo di un altro server da contattare

Esempio con un solo proxy server

- Ipotesi: telefonia IP, SIP based, entro una singola azienda o campus, con telefoni VoIP (evidentemente SIP)



- Aline e Bob lavorano nella medesima azienda
- Aline chiama Bob
  - Il suo telefono SIP non è a conoscenza dell'indirizzo IP del telefono SIP di Bob, in quanto non lo contatta frequentemente
  - L'interno di Aline è 555-1234
- Aline compone il numero interno di Bob, 555-6666
- Il suo telefono SIP
  1. lo converte nel corrispondente **SIP URI**,

     sip:555-6666@nice.com
  2. Invia un **INVITE** al SIP proxy server

Messaggio INVITE

INVITE sip:bob@nice.com SIP/3.0
Via: SIP/3.0/UDP 192.2.4.4:5060
To: Bob < sip:555-6666@nice.com >
From: Aline < sip:555-1234@nice.com >
Tag=203 941 885
Call-ID: b95c5d87f7721@192.2.4.4
Cseq: 26 563 897 INVITE
Contact: < sip:555-1234@192.2.4.4 >
Content-Type: application/SDP
Contact-Length: 142
Segue SDP

- La prima riga precisa il nome del METODO. Si tratta di un INVITE
- *Via*: contiene l'indirizzo IP, il numero di porta e il protocollo di livello trasporto che Aline vuole che si impieghi nella risposta
- *To*: contiene un nome di display e la SIP URI a cui tale richiesta viene inviata
- *From*: contiene un nome di display e una SIP URI che identificano la sorgente del messaggio
- *Call-ID* contiene un globally unique identifier per questa chiamata
- *To, From e Call-ID* identificano un "dialogo"
- *Cseq*: tale command sequence contiene un intero ed il nome di un metodo
  - Il telefono SIP di Aline incrementa tale valore per ogni nuova richiesta
- *Contact*: contiene lo username di Aline ed il suo IP address nella forma di un URI. Serve per comunicare al proxy server e al telefono SIP di Bob dove inviare richieste future per questo specifico dialogo
- *Content-type*: descrive il corpo del messaggio
- *Contact-Length*: fornisce la lunghezza in byte del corpo messaggio
- Tale corpo, non mostrato in figura, contiene una descrizione della sessione
  - Tipo di codec, dimensione dei pacchetti, … in un formato che è quello prescritto da SDP (Session Description Protocol)
  - Il modo in cui il messaggio SIP trasporta un messaggio SDP è analogo a quello in cui http trasporta una pagina web

- Poichè il telefono SIP di Aline non conosce l'indirizzo IP di Bob, il messaggio di INVITE giunge prima al proxy server
- Il proxy risponde con un 100 Trying, che indica che il proxy sta tentando di indirizzare l'INVITE al telefono di Bob
  - In generale, le risposte SIP sono identificate da un codice a tre cifre seguito da una frase descrittiva
- La risposta 100 trying contiene i medesimi valori dei campi to, from, call-ID e C-seq del messaggio INVITE, così che il telefono SIP di Aline può correlare tale risposta alla richiesta che aveva in precedenza inviato
- Il proxy server aggiunge un ulteriore header Via, con il suo indirizzo IP, all'INVITE che ha ricevuto, e lo forwarda al telefono SIP di Bob
- Quando tale telefono lo riceve, squilla. Poiché il nome di Aline è nell'header from, il telefono SIP può eseguirne il display
- Il telefono SIP di Bob invia un 180 Ringing Response (altro tipo di risposta SIP) al telefono di Aline, via proxy server
- Il proxy impiega l'header Via per determinare dove inviare tale risposta, e rimuove il proprio indirizzo dal top del messaggio
- Quando il telefono di Aline riceve il 180 ringing response, da il tono di ringback
- Quando Bob spinge il bottone per parlare, il suo telefono SIP invia un messaggio di risposta 200 OK per indicare che ha accettato la chiamata
  - Il corpo del messaggio 200 OK contiene la descrizione del media così come dettata da SDP per caratterizzare il tipo di sessione che il telefono di Bob può stabilire per la chiamata

- C`è dunque uno scambio nei due versi di messaggi SDP, allo scopo di negoziare le “capabilities” da impiegare durante la chiamata
- A questo punto il telefono SIP di Aline manda un ACK direttamente al telefono SIP di BOB (non passa attraverso il proxy server) e
- La sessione RTP può avere inizio
- ***I pacchetti vocali vengono inoltrati direttamente da un telefono SIP all’altro, ed i loro header non hanno nozione dei messaggi SIP o del/dei proxy server coinvolti durante il setup***

VANTAGGI del SIP

- Il SIP consente ai proxy server di prendere decisioni anche complesse sul routing della chiamata
  - Un proxy può inviare un INVITE a più destinazioni simultaneamente
    - ✓ Chiamata instradata contemporaneamente ad un voicemail e ad un ufficio periferico
  - Oppure attuare un instradamento selettivo, decidendo la destinazione sulla base
    - ✓ Dell'ora di arrivo
    - ✓ Dell'interfaccia da cui la chiamata arriva
    - ✓ Dell'attuale livello di utilizzo di un distributore di chiamate
- Il SIP facilita
  - la mobilità
  - lo sviluppo/creazione di nuovi servizi

Problemi di security del SIP

- Le soluzioni SIP incontrano problemi nel garantire la confidenzialità e l'integrità delle SIP requests
  - Obiettivo: prevenire denial of service attacks (DOS), message spoofing, …
- I messaggi SIP possono contenere informazioni sensibili
  - Chi comunica, quando e per quanto tempo, da quali indirizzi IP
  - Tale informazione deve rimanere privata!

- SOLUZIONE: Encryption ??
  - Non è possibile impiegarla sui campi *Request-URI, Route, Via*
  - Se include il SDP payload, le entità di rete non sono in grado di determinare il tipo di codec impiegato, la dimensione dei pacchetti, …
- ALLORA: IPSec
  - Protocollo di security a livello rete, adatto per le VPN

VoIP reliability

- L'affidabilità del servizio che il VoIP garantisce non può essere sottovalutata
  - La PSTN opera con una availability al 99.999 % (cinque nove)
  - Disponibile anche durante blackout di energia elettrica

- Attualmente non si può dire lo stesso per tutte le applicazioni VoIP
  - L'availability dei router attuali si attesta tra i tre e quattro nove
  - È ancora necessario migliorare
    - ✓ Il progetto dei router VoIP
    - ✓ La qualità dell'HW e del SW
    - ✓ Procedure migliori per prevenire e rilevare DDOS (Distributed …) che possono causare dei fuori servizio prolungati