INTRODUZIONE

Il fenomeno della telefonia sulla rete Internet, comunemente detto VoIP (Voice Over IP), sta svolgendo un ruolo di primaria importanza nello sviluppo delle telecomunicazioni, e non solo per la potenziale riduzione in termini significativi del costo delle comunicazioni vocali a lunga distanza, ma soprattutto nei vantaggi operativi e di semplificazione delle infrastrutture.

In più, la telefonia su IP apre la strada a nuovi e avanzati sistemi in aggiunta alla comunicazione verbale, quali il video conferencing, l'application sharing e il white-boarding, capaci di rivoluzionare l'interazione e l'operatività a tutti i livelli.

Per poter realizzare appieno gli obiettivi del VoIP occorre, tra l'altro, far convergere le reti di telecomunicazioni in modo tale da poter integrare fra loro i dati, la voce ed il video, offrendo così un servizio multimediale e real-time.

A fronte di tutto ciò si è resa necessaria la creazione di centralini telefonici che svolgessero le analoghe funzioni delle centrali telefoniche tradizionali, ma nel nuovo contesto della rete IP.

Questi centralini sulla rete IP vengono definiti IP-PBX (acronimo di Private Branch eXchange). L'IP-PBX è un software che viene installato su di un server di rete ed ha la capacità di gestire contemporaneamente e quindi integrare fra loro ogni tipo di comunicazione, sia questa video, audio o dati, visto che tutto viaggerà sempre sotto forma di pacchetti sulla rete IP.

Tra le funzioni tipiche dei centralini IP-PBX ricordiamo l'hold, cioè la messa in attesa di una chiamata, la deviazione di chiamata, l'utilizzo di IVR (risponditori automatici), la gestione delle code e la possibilità di registrare le chiamate e di associare ad ogni utente una segreteria telefonica, ma anche funzionalità non previste nei tradizionali

centralini PBX, come poter rinviare una chiamata verso un certo utente piuttosto che un altro in base all'orario, oppure il poter scegliere quale compagnia telefonica utilizzare durante una certa fascia oraria a seconda delle tariffe più convenienti.

Un IP - PBX che ha una vastissima diffusione e che è alla base di molti dei centralini IP che vengono commercializzati è Asterisk, utilizzato in questa tesi.

Nel primo capitolo di questo lavoro di tesi, dopo un'introduzione alle caratteristiche del VoIP, si è analizzata la raccomandazione H.323 e i protocolli su cui fa affidamento, nonché tutte le entità funzionali di una tipica architettura di rete basata su tale standard.

Analogamente, si sono analizzati i protocolli SIP e IAX ed i tipici componenti di una rete che sfruttano questi protocolli per trasmettere la voce a pacchetti, per poi concludere con una visione del sistema 3G – 324M.

Il secondo capitolo è dedicato per intero alle caratteristiche e i vantaggi nell'uso del VoIP PBX Asterisk, alle sue funzionalità, la descrizione e la configurazione base del suo dialplan, l'uso di contesti, estensioni, applicazioni, per concludere con una visione d'insieme circa le schede hardware e tipi di telefoni supportati, e qualche esempio di reti realizzabili sfruttando appunto Asterisk.

Il terzo e ultimo capitolo illustra, attraverso le fasi di installazione, compilazione e configurazione, il semplice test di telefonia e videotelefonia via softphone e telefoni IP realizzato utilizzando Asterisk come centralino, primo e basilare step verso una più accurata e complessa configurazione di un sistema telefonico interno ad una struttura come un ateneo, per facilitare, ad esempio, le comunicazioni tra studenti ed insegnanti.

SUMMARY

Internet Telephony, commonly called VoIP (Voice Over IP), is carrying out a role of primary importance in the development of the telecommunications, and the reason isn't only for progressive cost reduction of the long distance vocal communications, but mostly in the operative advantages and of infrastructures' semplification.

Moreover, the telephony over IP provide video conferencing, application sharing and the white-boarding, able to revolution interaction and the operability to all the levels.

For achieve this purpose of the VoIP is also necessary to converge telecommunications' net in such way from being able to integrate data, voice and video, and therefore to offer a multimedia and real-time service.

Therefore it has been made a new kind of PBX able to provide analogous functions of traditional pbx, but in the new context of IP, called IP-PBX (acronym of Private Branch eXchange). The IP-PBX is a software that comes installed on a net server and has the ability at the same time to manage and therefore to integrate betweene each other every type of communication, as video, audio or data, since everything will always move as packages over IP.

Between the typical functions of IP-PBX we remember on - hold, that is the call waiting, the call shunting line, use of IVR, queue management, and calls record and to associate a voicemail to every customer, but also functionalities not provided by traditional PBX, as to send back one call towards a customer rather than an other based on the timetable, or can choose own telephone provider to use according to time and so to choose convenient rates.

A very large diffusion IP - PBX and that is to the base of many commercial telephones exchange is Asterisk, used in this thesis.

In the first chapter of thesis, after an introduction to the VoIP characteristics, there is an analysis of the H.323 recommendation and its protocols, and its entities of the architecture based on such standard.

Analogous, there is a look on SIP and IAX protocols and the typical members of a net who use these protocols in order to transmit packets voice, in order then to end with a discussion about system 3G - 324M.

The second chapter is full dedicated to VoIP PBX Asterisk, to its functionalities, the description and the configuration base of its dialplan, the use of contexts, extensions, applications, in order to conclude with a discussion about supported hardware and telephones and some example of internet which use just Asterisk.

The third and last chapter illustrates, through installation, compilation and configuration, an easy test of telephony and video call via softphone and IP telephone realized using Asterisk as telephone exchange: it's a first and basic step towards one more accurate and complex configuration of internal telephone system to one structure like an athenaeum, with a main goal to make more easy, for example, the communications between students and teachers.

1. VOICE OVER IP E PROTOCOLLI DI COMUNICAZIONE

In questo capitolo, dopo un'introduzione al VoIP e alla differenza tra rete tradizionale a commutazione di circuito e rete a commutazione di pacchetto, si analizzano le caratteristiche generali degli standard di videocomunicazione H.323, SIP, IAX e del sistema 3G-324M.

» 1.1 Introduzione al VoIP: caratteristiche, vantaggi e svantaggi

Voice over IP (Voce tramite protocollo Internet), acronimo VoIP, è la tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione ad Internet o un'altra rete che utilizza il protocollo IP (Internet Protocol), anziché utilizzare esclusivamente la normale linea di trasmissione telefonica, permettendo di eliminare le centrali di commutazione ed economizzare sulla larghezza di banda occupata. Vengono instradati sulla rete pacchetti di dati contenenti le informazioni vocali, codificati in forma digitale, e ciò solo nel momento in cui è necessario, cioè quando uno degli utenti collegati sta parlando. Le conversazioni VoIP possono usare come mezzo trasmissivo una qualsiasi rete basata sul protocollo IP come una rete privata locale (LAN) all'interno di un edificio o di un gruppo di edifici o una rete più ampia (WAN), fino alla grande rete pubblica, Internet.

La telefonia via Internet permette una maggiore efficienza nell'uso della rete, grazie all'utilizzo della commutazione di pacchetto che, a differenza della commutazione di circuito, non assegna staticamente le risorse disponibili durante l'intera durata di una comunicazione ma

ne consente la condivisione con altri sistemi di comunicazione dati, quali testo e video.

I sistemi IP offrono, inoltre, mezzi più economici per la fornitura di connessioni telefoniche, permettendo innanzitutto di aggirare il sistema delle tariffe d'accesso internazionali.

Lo standard IP non è proprietario ed è frutto degli accordi tra sviluppatori hardware e software che ne hanno sancito la libertà di utilizzo da parte di chiunque. Questa architettura aperta permette ad imprese innovative di sviluppare nuovo hardware e software in grado di integrarsi perfettamente con la rete. Al contrario, il network a commutazione di circuito funziona come un sistema chiuso e di conseguenza rende più difficile implementare nuove applicazioni e servizi da parte di imprese innovative.

La tecnologia VoIP permette applicazioni impossibili ai tradizionali network telefonici: ad esempio si può portare il proprio telefono VoIP ovunque sia disponibile una connessione Internet e ricevere ed effettuare chiamate come se si fosse a casa propria, rimanendo raggiungibili allo stesso numero. In parallelo con la conversazione telefonica si possono scambiare flussi video in tempo reale (videoconferenza), possono essere inviati e ricevuti messaggi o files e si può partecipare a conferenze audio tra più persone in modo intuitivo ed a costi molto bassi.

Tra i vantaggi del VoIP rispetto alla telefonia tradizionale va poi senz'altro annoverato la diffusione a larga scala di applicazioni come la videoconferenza e la videotelefonia, supportata non solo dalla significativa riduzione del costo delle comunicazioni a lunga distanza, ma soprattutto nei vantaggi operativi e di semplificazione delle infrastrutture.
La tecnologia VoIP ha comunque diversi punti deboli che possono rallentare una sua larga diffusione.

Il problema di fondo della tecnologia VoIP è che la rete Internet è una rete Best Effort e non dà quindi nessun tipo di garanzia né in termini di ritardo, di perdita e di ordine sulla ricezione e la ricostruzione dei pacchetti di dati ricevuti. Risulta quindi necessario assicurare che il

"flusso audio" mantenga la corretta coerenza temporale. Questi problemi saranno però sempre meno rilevanti, grazie a tecnologie che permettono di assegnare una priorità diversa a certi pacchetti dati, garantendo la qualità del servizio (QoS).

Altre problematiche sono quelle relative all'affidabilità: i telefoni tradizionali senza cavo di alimentazione (la quasi totalità dei telefoni fissi) sono alimentati dalla linea telefonica, e in caso di black-out continuano a funzionare grazie a batterie e generatori all'interno delle centrali telefoniche. I telefoni VoIP (apparecchi, simili ad un tradizionale telefono, che si collegano direttamente ad un modem-router connesso ad Internet) hanno bisogno della corrente elettrica per funzionare e non sarebbero quindi disponibili durante un black-out rendendo impossibile qualsiasi telefonata. Inoltre le connessioni Internet a "banda larga" possono essere meno affidabili di una linea telefonica, e se si presentano dei ritardi nell'invio o nella ricezione dei pacchetti o una perdita degli stessi la comunicazione vocale viene momentaneamente interrotta. Questi fenomeni si presentano in modo più evidente quando applicazioni VoIP utilizzano reti altamente congestionate o le distanze tra i punti finali sono molto lunghe.

Forse uno dei problemi più rilevanti di questa tecnologia è che al momento risulta ancora difficile fornire un rintracciamento geografico veloce di una chiamata tramite VoIP, questo a causa della particolare natura delle reti IP che difficilmente permettono di individuare la posizione geografica degli utenti (si pensi ad esempio all'uso del proprio telefono VoIP da un HotSpot Wireless). Le chiamate di emergenza quindi non possono essere facilmente indirizzate verso le centrali più vicine e con alcuni sistemi VoIP sono tuttora impossibili. Inoltre nel caso in cui chi chiama non sia in grado di fornire un indirizzo preciso i servizi di emergenza non possono rintracciare il chiamante in alcun altro modo. Sono però in fase di studio e sperimentazione alcune soluzioni per aggirare il problema simili a quelle già applicate nella telefonia mobile.

A questo va aggiunto che i canali di telecomunicazione hanno un'intrinseca limitatezza in termini di capacità nel trasportare dati, per

cui è necessario adottare delle strategie di codifica. In quest'ottica gli organismi internazionali preposti alla standardizzazione hanno sviluppato e approvato protocolli sempre più leggeri ed efficaci, emanando opportune raccomandazioni e definendo i terminali e le componenti tecniche necessarie per la comunicazione multimediale su diversi tipi di sottoreti.

In particolare i protocolli al momento più utilizzati sono:

H.324, H.320, H.323 e dell'ITU – T, SIP dell'IETF e 3G-324-M del 3GPP.

Molto spesso queste raccomandazioni sono implementate su sistemi non sempre compatibili e connessi a reti di diverse tipologie come LAN (Local Area Network), xDSL (Digital Subscriber Line), ISDN (Integrated Services Digital Network), linee telefoniche analogiche e linee wireless.

Nel trasmettere audio e video su reti eterogenee, ad esempio, la connessione tra sorgente e destinatario può essere stabilita su link con diverse caratteristiche e capacità. In questi casi il bit rate del segnale trasmesso deve essere adattato alla banda del canale, a cui è collegato l'utente finale.

Se poi la comunicazione avviene tra sistemi che usano protocolli di segnalazione e codec diversi, c'è anche la necessità di convertire il flusso di bit originario, codificato secondo le regole sintattiche di uno standard, in un nuovo bit stream che sia interpretabile dal ricevitore.

Per fare ciò occorre utilizzare, oltre ai gateway tradizionali, anche da nuove apparecchiature, in grado di collegare la rete dati Internet e la rete telefonica tradizionale. Queste apparecchiature sono note come Internet Telephony Gateway (o Voice Gateway) e sono solitamente installate presso gli operatori di telefonia via Internet.

I gateway manipolano le trasmissioni vocali convertendole, dalla rete tradizionale, in forme idonee alla trasmissione su reti a commutazione di pacchetto. Permettono quindi di terminare sulla rete tradizionale PSTN telefonate che hanno avuto origine sulla rete IP di un operatore di telefonia via Internet o viceversa di rendere

accessibile un utente di telefonia VoIP dalla rete telefonica tradizionale.
In questo ambito si colloca il gateway VoIP PBX Open Source Asterisk utilizzato in questo lavoro di tesi.

Di seguito saranno messe a confronto le due tipologie di rete che permettono di fornire servizi di telefonia: la tradizionale rete a commutazione di circuito e le reti dati, a commutazioni di pacchetto.

» 1.2 Rete telefonica e la commutazione di circuito

La rete PSTN (Public Switched Telephony Network) è stata pensata e progettata per il trasporto della voce ed adotta la tecnologia a commutazione di circuito, vale a dire ogni volta che una comunicazione è iniziata, gli switch interni della rete commutano per creare un circuito "fisico" diretto fra la parte chiamante e quella chiamata.

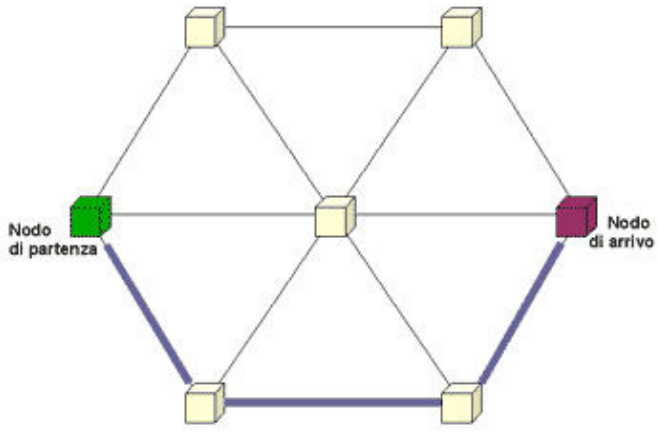

Fig. 1 – schema esemplificativo di rete a commutazione di circuito

Quindi per tutta la durata della comunicazione, gli interlocutori dispongono di un canale dedicato non accessibile agli altri utenti,

indipendentemente dal fatto che le parti siano in conversazione attiva o in silenzio. Si ha, così, un'allocazione statica delle risorse ed ogni circuito garantisce una banda di 64 kbps bidirezionale (full duplex).

La banda costante e il collegamento diretto tra le due parti permettono, al segnale vocale, di avere qualità garantita per tutta la durata della comunicazione, ma al tempo stesso si ha una bassa percentuale di utilizzazione della rete; in altre parole non si trae vantaggio dal fenomeno del multiplexing statistico.

Infatti, durante una comunicazione vocale, un interlocutore passa più della metà del tempo in silenzio, in quanto i due interlocutori non parlano contemporaneamente, ed inoltre anche tra una parola e l'altra ci sono degli istanti di silenzio.

I 64 kbps allocati sono, perciò, usati per meno della metà del periodo della conversazione e la banda libera rimane inutilizzata. Il costo di una chiamata tramite PSTN è basato sulle risorse riservate, non in base alle risorse effettivamente impiegate.

Un altro limite della rete telefonica è l'utilizzo di un codec standard e predeterminato a priori, il PCM (Pulse Code Modulation), descritto nella Raccomandazione ITU-T G.711, a 64 kbps. Questo fattore è limitante sia nel momento in cui si volesse utilizzare la rete telefonica per il trasporto di audio compresso con una maggiore efficienza, sia nel momento in cui si volesse trasportare audio ad alta qualità (ad esempio aumentando il bitrate oppure utilizzando un codec con caratteristiche migliori). Per realizzare il circuito virtuale tra le parti è necessaria inoltre una fase di segnalazione e di set-up che possono richiedere un tempo anche dell'ordine del secondo, con un considerevole lavoro di gestione della chiamata da parte della rete.

Questi motivi portano a concludere che, tecnicamente, la tecnologia su cui si basa la telefonica classica può essere migliorata, ed è proprio su questi punto che andrà a puntare la tecnologia VoIP.

» 1.3 La rete dati e la commutazione di pacchetto

La totalità delle reti dati oggi esistenti si basa sul concetto di commutazione di pacchetto: ossia la creazione di un'unità elementare di trasporto che sia in grado di viaggiare in maniera più o meno autonoma sulla rete, recapitando a destinazione il suo contenuto informativo.

In tale caso non si stabilisce nessun percorso fisico in anticipo tra chiamante e ricevente; con la commutazione di circuito, qualsiasi larghezza di banda non usata su un circuito allocata è persa, invece con la commutazione di pacchetto essa può essere utilizzata da altri pacchetti provenienti da altre sorgenti e diretti verso altre destinazioni, poiché i circuiti non sono dedicati.

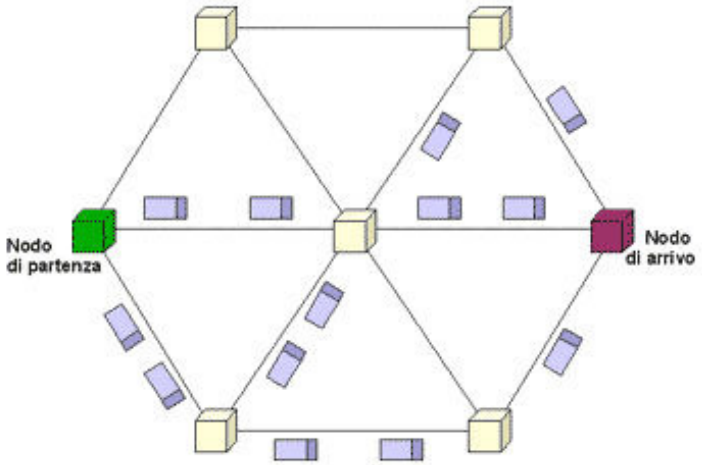

Fig. 2 – schema esemplificativo di rete a commutazione di pacchetto

L'architettura di rete dati allo stato attuale è la rete IP, caratterizzata da un servizio di tipo best effort, senza meccanismi di prenotazione di risorse. Gli apparati intermedi (nodi) instradano il pacchetto nella giusta direzione in base all'informazione contenuta nell'intestazione dello stesso. In questo modo non si ha allocazione di risorse riservate, perciò su una linea di collegamento (link) possono transitare contemporaneamente anche pacchetti appartenenti a flussi diversi, aumentando notevolmente la percentuale d'utilizzazione della rete rispetto a quella telefonica.

» 1.4 Protocolli VoIP

La tecnologia VoIP richiede due tipologie di protocolli di comunicazione in parallelo, uno è per il trasporto dei dati (pacchetti voce su IP), in tal caso, nella grande maggioranza delle implementazioni di VoIP viene adottato il protocollo RTP (Real-time Transport Protocol).

Esistono poi altri protocolli per la codifica della segnalazione della conversazione (ricostruzione del frame audio, sincronizzazione, identificazione del chiamante, ecc.) ma in questo contesto il processo di standardizzazione non si è ancora concluso.
Al momento, sono coinvolti tre enti internazionali di standardizzazione: l'ITU (International Telecommunications Union), l'IETF9 (Internet Engineering Task Force) e l'ETSI10 (European Telecommunication Standard Institute) con alcuni consorzi (per esempio, Softswitch, H.323ORG, Vivida ecc.).
I principali protocolli utilizzati sono:

• SIP (Session Initiation Protocol) della IETF

• H.323 della ITU

• Skinny Client Control Protocol, protocollo proprietario della Cisco

• Megaco (conosciuto anche come H.248) e MGCP

• MiNET, protocollo proprietario della Mitel

• IAX, usato dai server Asterisk open source PBX e dai relativi software client

• XMPP, usato da Google Talk. Inizialmente pensato per l'IM ora esteso a funzioni Voip grazie al modulo Jingle.

In particolare in questo capitolo, da qui in poi si analizzeranno più da vicino le caratteristiche salienti del protocollo H.323, SIP, IAX, per poi concludere con la specifica 3G-324M.

» 1.5 Lo standard H.323

Il protocollo H.323 è una raccomandazione ITU – T (International Telecommunications Union – Telecommunication Standardization Sector) che specifica il modo in cui il traffico multimediale deve essere trasmesso in reti a commutazione di pacchetto che non prevedono qualità del servizio (in particolare la rete IP). Questo standard si occupa delle segnalazioni e del controllo delle chiamate, la trasmissione e il controllo di informazioni multimediali e il controllo di ampiezza di banda nelle conferenze in tempo reale punto – punto e multipunto.

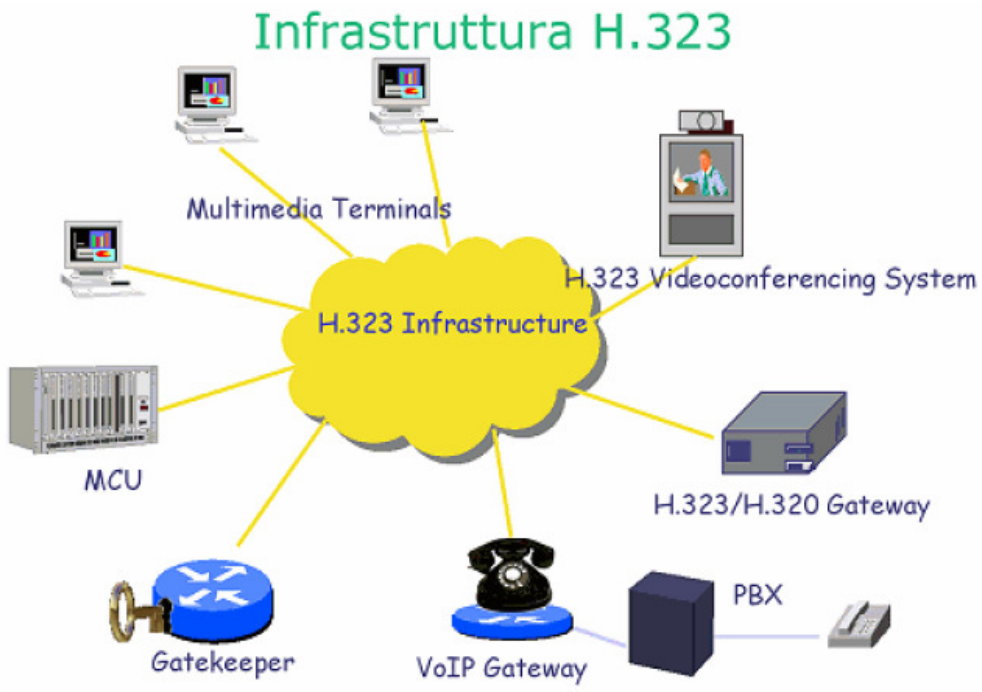

Fig. 3 – infrastruttura H.323

Gli elementi fondamentali di un sistema H.323 (vedi fig. 3) sono:

- **I terminali,** ovvero dispositivi che si interfacciano con gli utenti (es. un PC o un telefono), o con apparecchi telefonici analogici tradizionali. Offrono funzionalità di controllo del sistema, formattazione di flussi audio/video che devono essere trasmessi, codifica audio e video (quest'ultima opzionale),

supporto di applicazioni (come ad es. conferenze audiografiche);

- **I gateway,** che traducono i vari formati di trasmissione audio, video e dati connettendo, di fatto, reti di tipo diverso (come la rete IP, la rete telefonica tradizionale, la rete ISDN, ecc.);
- **Il gatekeeper,** è il componente centrale dell'infrastruttura H.323, nonostante sia considerato un elemento opzionale. Tra le funzioni svolte da un gatekeeper troviamo: fornire un metodo di autenticazione di terminali e gateway, gestire la banda e l'accounting (ovvero raccogliere gli elementi per fatturare i servizi erogati);
- **MCU (Multipoint Control Unit)**, si tratta del sistema che permette di estendere la comunicazione da punto a punto a punto multi-punto. Gestisce conferenze multipoint tra tre o più terminali. E' costituito da un *MC (Multipoint Controller)*, che assicura un livello minimo di comunicazione e da uno o più *processori MP (Multipoint Processor)*, per l'audio, il video o i dati.

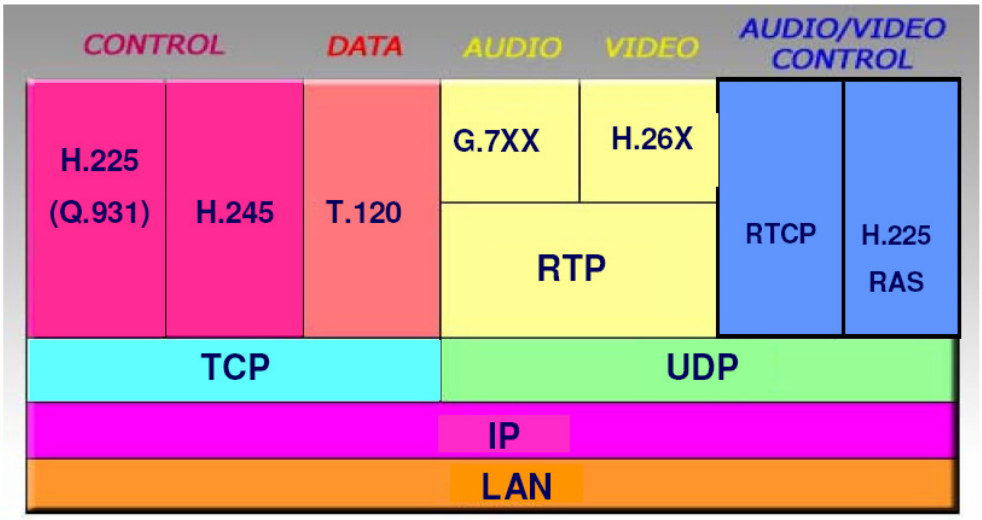

Fig. 4 – pila protocollare nel sistema H.323

I protocolli che fanno parte dello standard H.323 si occupano del supporto dell'ammissione, l'instaurazione, lo stato, il rilascio, la gestione dei mezzi trasmessivi e i messaggi di gestione della chiamata.

Essi si dividono in due categorie secondo il protocollo di trasporto sul quale si appoggiano:

- Protocolli che si appoggiano su un canale connesso e quindi sicuro quale TCP (H.225, Q.931, H.245);
- Protocolli che si appoggiano su un canale non connesso e quindi inaffidabile quale UDP (RTP, RTCP, RAS).

Un ulteriore classificazione è basata sull'area di controllo:

- Segnali di registrazione, ammissione e stato (RAS): forniscono il controllo pre – chiamata nelle reti basate su gatekeeper H.323;
- Segnali di controllo della chiamata: usati per connettere, mantenere e disconnettere le chiamate fra i terminali.
- Controllo e trasmissione sul mezzo trasmissivo: fornisce il canale affidabile H.245 che trasmette i messaggi di controllo del mezzo trasmissivo. Il trasporto utilizza un flusso UDP inaffidabile.

Le operazioni più importanti nello standard H.323 sono:

l'attivazione del canale RAS con la conseguente registrazione presso il Gatekeeper e l'instaurazione di una chiamata.

Il canale RAS è un canale di comunicazione inaffidabile tra i terminali e il gatekeeper. Viene aperto prima che venga attivato qualsiasi altro canale, e trasporta i messaggi RAS che svolgono le procedure di registrazione, ammissione, variazione dell'ampiezza di banda, stato e disconnessione.

La ricerca del gatekeeper è un processo manuale o automatico utilizzato dai terminali per identificare il gatekeeper sul quale si devono registrare.

Con il metodo manuale, i terminali vengono configurati con l'indirizzo IP del gatekeeper, mentre il metodo automatico richiede un meccanismo di ricerca automatica, che consente ad un terminale, che non conosce il proprio gatekeeper, di trovarlo tramite l'invio di un messaggio multicast.

La registrazione è il processo che consente ai gateway, ai terminali e alle unità MCU di collegarsi ad una zona e fornire al gatekeeper i propri indirizzi IP e alias.

Da sottolineare che su una rete H.323 è previsto l'impiego di due tipi diversi di indirizzo: la coppia indirizzo di rete/identificatore TSAP e gli indirizzi alias.

Ogni entità H.323 deve possedere almeno un indirizzo di livello rete per poterla identificare univocamente all'interno della rete stessa. Comunque, tale indirizzo non è sufficiente per portare a termine la comunicazione: infatti sarà necessario attivare, sulla stessa macchina, delle connessioni di controllo e delle connessioni dati.

L'identificazione di tali connessioni viene fatto con gli identificatori TSAP (Transport layer Service Access Point). Gli identificatori TSAP possono essere ben definiti, o negoziati a run- time. Della prima categoria fanno parte gli identificatori per l'instaurazione delle chiamate (devono essere well known, altrimenti il chiamante non può effettuare la chiamata).

Invece appartengono alla seconda categoria gli identificatori TSAP per i canali di controllo H.245, audio, video e dati.

Vediamo ora gli indirizzi alias: un alias può essere un indirizzo E.164 (numero di telefono), un identificatore H.323 (es. un indirizzo di e-mail), ecc.

Questi indirizzi hanno il compito di rendere più semplice l'identificazione del terminale utente mediante l'impiego di un nome più conosciuto rispetto all'indirizzo IP.

Gli indirizzi alias sono disponibili solamente nel caso in cui la rete preveda un Gatekeeper, il quale, a fronte di una chiamata, si occupa della loro traduzione in indirizzi IP.

Una volta ultimata la fase di registrazione, e prima che venga instaurata la chiamata vera e propria, i terminali e gatekeeper possono scambiarsi tra loro messaggi per il controllo delle ammissioni e dell'ampiezza di banda, e messaggi di stato con cui il gatekeeper si rende conto se il terminale è in linea o no.

La raccomandazione H.225 ITU si occupa delle procedure di controllo della chiamata che specificano l'uso e il supporto dei messaggi di segnalazione Q.931. Attraverso la porta 1720, i terminali si scambiano messaggi con lo scopo di connettere, gestire e disconnettere le chiamate. I messaggi più utilizzati sono:

- Setup: l'entità chiamante avverte l'entità chiamata che vuole stabilire una connessione;
- Call Proceeding: l'entità chiamata informa la chiamante dell'inizio delle procedure di instaurazione della chiamata;
- Alerting: risposta dell'entità chiamata che avvisa il chiamante che sta squillando il telefono;
- Connect: indica all'entità chiamante che il chiamato ha risposto alla sua telefonata;
- Release Complete: il terminale che inizia la disconnessione avverte l'altro terminale che la chiamata è stata rilasciata (sempre che il canale sia ancora aperto e attivo);
- Facility: un messaggio Q.932 che serve per richiedere l'acknoledgement (cioè il messaggio di verifica e conferma) di servizi supplementari.

La raccomandazione H.245 gestisce tutti i messaggi punto-a-punto fra le entità H.323, definendo delle procedure per il controllo e la trasmissione di informazioni audio, video, dati. Viene stabilito un canale di controllo affidabile sulla rete IP, che consente anche lo scambio di funzionalità di trasmissione e ricezione e la negoziazione delle funzioni come ad esempio la scelta del codec da usare.

Il protocollo **RTP** (Real-Time Protocol) fornisce le funzionalità di trasporto delle informazioni in H.323.

In particolare, RTP consente il trasferimento in tempo reale punto-a-punto di informazioni interattive audio, video e dati su reti unicast o multicast: un tipico scenario di utilizzo è la videoconferenza. Le funzioni svolte da questo protocollo comprendono la ricostruzione al ricevitore della corretta sequenza dei pacchetti e della loro posizione nella scala dei tempi, consentendo quindi la ricostruzione dei sincronismi. Questo protocollo non permette, nativamente, di sincronizzare più sessioni multimediali tra di loro in quanto ogni sessione RTP è in grado di trasportare un solo flusso. Questo non impedisce, tuttavia, il dialogo tra N soggetti, che è anzi supportato nativamente attraverso lo sfruttamento di un'eventuale tecnologia multicast sulla rete sottostante. Tuttavia in presenza di più sessioni distinte (ad esempio audio e video) è necessario attivare più sessioni RTP, ognuna delle quali è identificata da una coppia di indirizzi di livello trasporto (indirizzo IP + numero di porto), e nel caso di multicast l'indirizzo di destinazione è comune a tutti i partecipanti.

Utilizzando due sessioni RTP è possibile fare in modo ad esempio che alcuni partecipanti ricevano sia l'audio che il video, mentre altri ricevano solo uno dei due.

L'header di un pacchetto RTP è composto da una parte fissa e un'estensione utilizzata per scopi sperimentali.

La parte fissa dell'header si articola su 12 byte e contiene i seguenti campi:

- V (Version): indica la versione di RTP utilizzata
- P (Padding): se il bit vale uno, il pacchetto contiene almeno un byte addizionale di riempimento non facenti parte del payload, l'ultimo byte di padding contiene il valore di quanti byte padding sono presenti.
- X (extension): se impostato ad uno, indica la presenza di un'estensione dell'header.
- CC (CSRC Count): è il numero di CSRC presenti dopo la parte fissa dell'header.
- M (Marker): l'interpretazione di questo bit è legata al profilo.
- PT (Payload Type): identifica il contenuto del pacchetto, nel profilo è fissata staticamente la corrispondenza tra il codice e il formato del payload.
- Numero di sequenza: è incrementato di uno per ogni pacchetto inviato; può essere utilizzato dal destinatario per accorgersi della perdita di pacchetti e per ricostruire l'ordine corretto della sequenza.
- Timestamp: riflette l'istante di campionamento del primo ottetto dei dati. L'istante di campionamento deve essere derivato da un clock che si incrementa monotonamente e linearmente nel tempo per permettere i controlli di sincronizzazione e le misure dell'incertezza sugli arrivi dei pacchetti (arrival jitter).
- SSRC: identifica la stazione trasmittente.
- CSRC: questo campo è opzionale ed è presente solo se un elemento della rete ha unito in un unico flusso contributi provenienti da diverse sorgenti; al suo interno sono elencati gli SSRC delle singole stazioni.

In ogni sessione la stazione che genera/riceve traffico RTP acquisisce un codice univoco, il SSRC, che permette alla stazione stessa di essere univocamente identificata all'interno della sessione real-time in esame.

RTCP (Real-Time Control Protocol) monitorizza l'invio dei dati e controlla e identifica i servizi. Dunque riconosce automaticamente il tipo di compressione utilizzato sulla linea e segnala al mittente e al destinatario eventuali problemi riscontrati sulla rete o sulla stazione di lavoro (identificandone la fonte), tenendo sotto controllo e fornendo feedback circa la qualità di ricezione e distribuzione dei dati (n° dei pacchetti ricevuti o persi sul jitter, ecc.) .

» 1.6 SIP

Il SIP (Session Initiation Protocol) è un protocollo del livello applicazione che nasce in ambito IETF come alternativa più semplice al sistema H.323, ed è utilizzato per attivare, gestire e chiudere le sessioni multimediali.

Esso trova applicazione non solo nella telefonia su IP e nei servizi telefonici supplementari, ma anche nella video-comunicazione, nei giochi interattivi, nella messaggistica istantanea.

Il protocollo SIP ha fondamentalmente le seguenti funzioni:

- Invitare gli utenti a partecipare ad una sessione;
- Localizzare gli utenti: determina le caratteristiche dell'utente in termini di risorse audio/video e i parametri da usare;

- Acquisire le preferenze degli utenti;
- Determinare la capacità degli utenti, cioè le caratteristiche dell'utente in termini di risorse audio/video e i parametri da usare;
- Trasportare una descrizione della sessione;
- Instaurare le connessioni di sessione;
- Setup della chiamata, cioè la gestione di eventuali modifiche dei parametri di sessione;
- Rilasciare le parti;
- Cancellare la sessione in qualunque momento si desideri;

SIP è un protocollo text-based, orientato al Web, simile ad HTTP, con una struttura client-server. Questa scelta porta anche ad una facilità di integrazione con Internet: poiché, come vedremo, gli indirizzi utilizzati da SIP sono strutturati in maniera identica a quelli di posta elettronica, l'integrazione nelle pagine Web è intuitivamente identica.

Per instaurare una sessione, avviene un three-way handshaking (Request, Response, Ack - concettualmente simile a quello che avviene con il protocollo TCP).

Tra le sue caratteristiche peculiari vi è l'idea di inserire l'intelligenza, ove possibile, ai bordi della rete, lasciando alla rete il suo compito peculiare di smistamento dei messaggi, ottenendo qui eccellenti caratteristiche di scalabilità.

La suite SIP definisce componenti piccoli e mono-funzionali, in modo da evitare la duplicazione di funzioni e fare sì che siano modulari, a differenza di quello che succede in H.323 dove per una funzione elementare sono necessarie iterazioni di più protocolli.

Il protocollo SIP, per questioni di semplicità, non specifica la trasmissione dei dati audio/video (e dati), demandando questo compito al già collaudato protocollo RTP/RTCP.

Per lo stesso motivo non si preoccupa di riservare la banda per una chiamata.

In particolare, SIP può inviare al terminale chiamato invitato le informazioni necessarie per l'allocazione di risorse sulla rete: è fortemente integrato, infatti, con il protocollo SDP (Session Description Protocol), e con RSVP, Resource reSerVation Protocol, che hanno il compito di dare una descrizione dettagliata delle risorse necessarie all'instaurazione della chiamata e di riservarle.

Il protocollo SIP supporta la mobilità ed è dialog-oriented: un dialogo è una relazione persistente tra entità paritetiche che si scambiano richieste e risposte in un contesto comune.

Per quanto riguarda l'indirizzamento, lo standard prevede che ogni utente abbia un indirizzo SIP: dunque l'indirizzo è proprio dell'utente, non del terminale.

Gli indirizzi (le cosiddette SIP URL) hanno la forma del tipo *nomeutente@dominio.com*, quindi sono simili a indirizzi e-mail.

La parte iniziale dell'indirizzo (*nomeutente*) è il nome dell'utente o un numero telefonico, la parte finale (*dominio.com*), può essere il nome di dominio oppure un indirizzo di rete.

Grazie a questo meccanismo, SIP supporta anche l'interlavoro con la rete telefonica classica: un indirizzo nella forma *07762993748@unicas.it* può indicare la volontà di raggiungere l'utente telefonico indicato attraverso un gateway tra mondo IP e mondo telefonico presso l'università di Cassino (in questo caso si deve indicare, attraverso il parametro *user=phone,* che l'identificativo è un numero telefonico).

Passiamo ad analizzare l'architettura SIP: i componenti fondamentali sono gli user agent e i server di rete.

Gli **User Agent** sono applicazioni operanti sul sistema terminale che includono due componenti:

- User Agent Client: si occupa delle procedure necessarie a far partire una chiamata;
- User Agent Server: riceve le richieste di chiamate in arrivo e restituisce le risposte dell'utente chiamato.

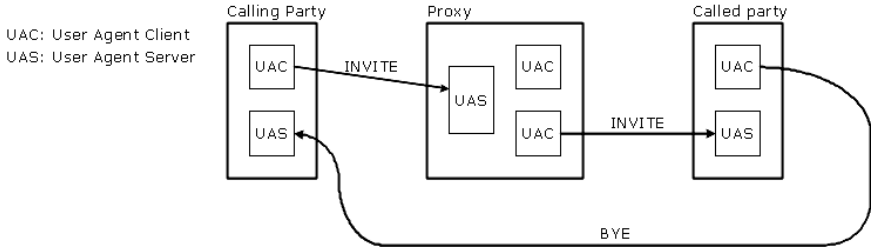

Fig.5 – User Agent Client e User Agent Server

Il **Proxy Server** è un server intermedio; può rispondere direttamente alle richieste oppure "ruotarle" ad un client, ad un server o ad un ulteriore proxy. Un proxy server analizza i parametri di instradamento dei messaggi e "nasconde" la reale posizione del destinatario del messaggio - essendo quest'ultimo indirizzabile con un nome convenzionale del dominio di appartenenza. Il vantaggio nel suo utilizzo sta nel fatto che al proxy server può essere delegata in toto la gestione della chiamata, ragion per cui i terminali utente non devono preoccuparsi di tutte le procedure di segnalazione nella loro interezza.

Il **Redirect Server** accetta le richieste SIP e invia al client una risposta di redirezione contenente l'indirizzo del server successivo. Questo tipo di server non accetta chiamate e non elabora o inoltra le richieste SIP.

Il **Location Server** implementa un servizio di risoluzione degli indirizzi: è dunque un database contenente informazioni sull'utente, come il profilo, l'indirizzo IP, l'URL.

Il **Registrar Server** è un server dedicato o collocato in un proxy. Quando un utente è iscritto ad un dominio, invia un messaggio di registrazione del suo attuale punto di ancoraggio alla rete ad un Registrar Server.

Il **Multi Conference Unit** è un oggetto in grado di realizzare chiamate tra 3 o più persone, con le stesse caratteristiche dell'analogo componente presente in H.323.

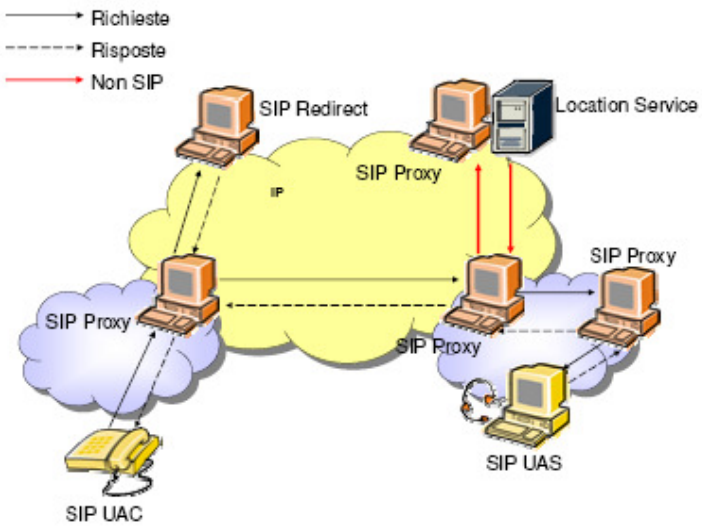

Fig. 6 - Architettura SIP

Un messaggio SIP è una richiesta (attivata dai client) o una risposta (restituita dai server); una sequenza di una richiesta e una o più risposte è detta transazione: una transazione è identificabile da un transaction-ID, un identificativo che ne specifica la sorgente, la destinazione e il numero di sequenza. E' possibile trasmettere le transazioni SIP sia in UDP che in TCP.

Ogni messaggio contiene un'intestazione che descrive i dettagli della comunicazione, specificando il chiamante, il chiamato, il percorso e il tipo di messaggio contenuto in una chiamata.

I messaggi SIP più frequenti sono:

- Register: messaggi inviato da uno User Agent quando vuole registrare presso un Registrar Server il proprio punto di ancoraggio alla rete;
- Bye: utilizzato per porre fine ad un dialogo SIP;
- Cancel: per terminare un dialogo se la sessione non ha ancora avuto inizio;
- Invite: serve ad invitare un utente a partecipare ad una sessione;
- Ack: è un messaggio di riscontro;
- Trying e Ringing: messaggi provvisori, mantengono i parametri della richiesta a cui rispondono;
- Subscribe e Notify: utilizzati per E-Presence.

Ecco un esempio di messaggio Invite:

```
INVITE sip:utente@domain.com SIP/2.0
    Via: SIP/2.0/UDP 134.102.18.1
    From: <sip:zioMauro@dominio.com>; tag = 4711
'''//identifica l'originatore della richiesta ''
    To: Michele <sip:utente@domain.com> '''//identifica la
destinazione logica di una richiesta''
    Call-Id: 12345678@134.102.18.1 '''//è un valore costante
che identifica l'invito''
    Cseq: 49 Invite '''//ordina le transazioni (..la prossima
richiesta avrà Cseq=50)''
    Content-Length: 117 '''//il body consiste in 117 byte ''
    Content-Type: application /sdp '''//tipo di media
descritto secondo il protocollo [[SDP]]''
    Subject: felicitazioni! '''//l'oggetto del messaggio''
    Contact: sip:zioMauro@134.102.18.1:4050 '''//l'indirizzo
al quale si desidera ricevere richieste''
    transport = udp '''//specifica il protocollo di trasporto,
nell'esempio [[User Datagram Protocol|UDP]]''

    v = 0 '''//indica la versione in uso''
    o = jack 7564657 9823872 IN IP4 134.102.18.1 '''//l'owner
della risorsa con un ID di sessione''
    c = IN IP4 134.102.18.1 '''//tipo di rete, la versione del
protocollo IP e l'IP stesso ''
    t = 0 0 '''//tempo di start e di stop''
    m = audio 4754 RTP/AVP 0 '''//tipo di media, num. di
porto, protocollo di trasporto e formato ''
    a = rtpmap: 0 PCMU/8000 '''//attributi audio\video.. se ce
ne fossero ''
    s = festa '''//subject della sessione''
```

Le risposte, analogamente a HTTP, sono rappresentate da un codice di stato di tre cifre di cui la prima identifica la tipologia di risposta (es. 4XX= Request Failure: la richiesta non è andata a buon fine).

Ulteriori dettagli sul protocollo SIP possono essere trovati nel documento RFC (Request For Comments) 2543: se ne trova una sua copia online all'indirizzo http://www.ietf.org/rfc/rfc2543.txt

» 1.7 IAX

IAX è un acronimo che sta per Inter Asterisk eXchange. È il protocollo de facto utilizzato da Asterisk, il server PBX (Private Branch eXchange – praticamente una centrale telefonica per uso privato) open source della Digium utilizzato in questa tesi e descritto nel prossimo capitolo.

IAX ora è comunemente indicato come IAX2, la seconda versione del protocollo IAX, in quanto il protocollo originale IAX è obsoleto.

IAX può essere usato con ogni tipo di media stream, incluso i video, ma è rivolto principalmente al controllo delle chiamate vocali su rete IP.

Il principale obiettivo del protocollo IAX fu quello di minimizzare la larghezza di banda necessaria per la trasmissione dell'informazione prestando particolare attenzione al controllo, alle chiamate vocali individuali e al supporto nativo per l'utilizzo trasparente su reti con NAT. La struttura di base del protocollo IAX permette di miscelare i segnali e più flussi di dati su un singolo flusso UDP tra due computer. Lo IAX è un protocollo binario ed è organizzato in modo da minimizzare l'overhead (cioè l'intestazione aggiuntiva presente nei pacchetti, per poterli adeguatamente trasmettere) in particolare riguardo i flussi voce.

Il protocollo è di tipo peer-to-peer sia per quanto riguarda la segnalazione che per i media stream. Ciò significa che piuttosto che esaminare comandi in formato testo, IAX utilizza solo dati binari, essendo questo il modo naturale con cui le macchine comunicano tra loro.

Tutte le segnalazioni hanno luogo nel livello data link. Toni doppi e multifrequenziali sono spesso trasmessi attraverso lo stesso percorso con tutte le altre segnalazioni in modo da poterli ritrasmettere in modo affidabile all'altro terminale.

Il trasporto delle informazioni non utilizza il protocollo RTP: il progetto base di IAX prevede di fare il multiplexing della segnalazione e dei media strema attraverso una singola associazione UDP tra due host. A differenza di altri protocolli, la cui architettura prevede la separazione tra i componenti di controllo e quelli relativi ai media stream, qui, nella struttura IAX, viene utilizzata la stessa porta UDP, la 4569.

Dunque, come abbiamo già detto, IAX è un protocollo binario: la ragione per cui si scelse questa strada è legata principalmente all'efficienza in banda, in particolare per le chiamate vocali (basti pensare che con IAX è possibile triplicare il numero di chiamate che si possono effettuare rispetto ad altri sistemi più complessi, come H.323 o SIP: per esempio, utilizzando IAX e il codec G.729 è possibile effettuare almeno 103 chiamate con una banda di 1 Mbit). Altri benefici sono la robustezza contro gli errori da 'buffer overrun', la risoluzione della maggior parte dei problemi che si possono presentare nell'integrazione di piattaforme VoIP con firewalls e routers NAT. e una implementazione molto compatta.

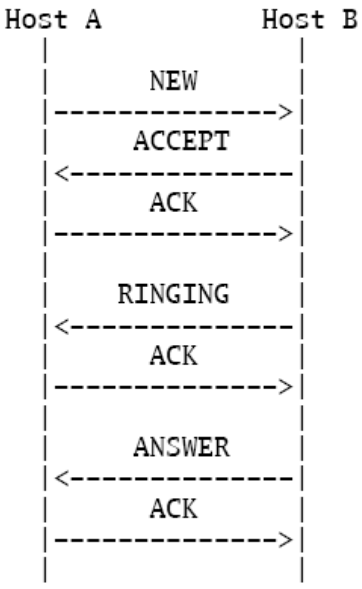

Fig. 7 – semplice chiamata tra due host

La figura sopra illustra il flusso basilare di messaggi tra due host allo scopo di dar vita ad una chiamata. L'host A inizia la chiamata inviando un messaggio NEW all'host B, che risponde con un messaggio ACCEPT, seguito da un ACK, cioè un riscontro, da A a B.

Segue un messaggio RINGING, con cui B informa A che il suo telefono sta squillando. Anche qui c'è un ACK inviato da A a B, come conferma della ricezione del messaggio RINGING. Infine, quando la cornetta è sollevata, l'host B invia un messaggio di risposta (ANSWER) ad A, che conferma con un ACK. A questo punto una comunicazione full-duplex (cioè nelle due direzioni) è instaurata tra A e B.

In IAX, la più piccola unità di comunicazione è il frame.

I **Full Frame** possono essere usati per inviare segnalazioni, e informazioni audio e video attendibili (dunque è previsto l'invio di ack). Ci sono due tipi di informazioni di controllo che sono trasmesse attraverso i full frame: i Control Frame (si occupano della sessione di controllo, come per esempio il controllo dei dispositivi connessi ai terminali IAX) e gli IAX Control Frames (si occupano della gestione dei terminali).

I **Mini Frame** sono usati per trasportare media stream con un minimo overhead: hanno un header di soli 4 byte per ciascun pacchetto (1 bit di tipo frame, 15 per il numero di origine chiamata, 16 di timestamp) e in questo modo aumenta il numero di chiamate che possono essere gestite a parità di banda.

Va notato che le Mini Frame sono trasmesse in rete in modo 'unreliable', ossia non si prevede un ack di una Mini Frame inviata da parte del nodo ricevente. Intervallate alle Mini Frame vengono trasmesse le già citate Full Frame, che sono di dimensioni maggiori ma vengono 'confermate' del nodo ricevente.

Ciò permette anche un meccanismo di controllo dello stato delle connessioni. Se uno dei due nodi dopo un certo periodo di tempo (15 secondi) non riceve più Full Frame dall'altro, gliene invia una di 'ping'

per verificare che sia attivo. Dopo un certo lasso di tempo ne invia ancora, e dopo un predeterminato numero di tentativi presume che l'altro nodo si sia scollegato e chiude la connessione UDP.

Sono previste anche funzioni di trunking di più canali nella stessa comunicazione: IAX unisce i dati di più canali in un unico insieme di pacchetti, riducendo non solo il numero degli header, ma anche quello dei pacchetti. Questa funzione, particolarmente importante nelle reti wireless è interessante se si vuole affiancare alla chiamata VoIP uno scambio di media stream diversi, come ad esempio il video.

Meglio ancora, il protocollo IAX è così semplice e lineare che permette l'implementazione di un terminal adapter analogico (ATA) dell'intero stack IP, dello stack IAX, dell'interfaccia TDm, dei cancellatori di echo e del Caller ID.

Un dispositivo ATA include un jack Ethernet e uno telefonico, e converte un telefono analogico in un telefono IP. Può essere realizzato con hardware a costo minimo: un microprocessore a 8 bit, 4 KB di RAM e 64 KB memoria flash basta a collegare un telefono analogico a una rete VoIP basata su IAX, occupandosi di tutto lo stack protocollare, della cancellazione dell'eco, dell'interfaccia TDM e della generazione del Caller ID. In questo modo un telefono VoIP potrebbe arrivare a costare una decina di euro, un prezzo finalmente concorrenziale con quello dei terminali analogici.

» 1.8 Servizi 3G su reti IP e il QoS

I due organismi di standardizzazione, 3GPP e 3GPP2, prevedono che i servizi di terza generazione si stabiliranno completamente su reti IP. Comunque questa prospettiva sarà realizzabile solo tra qualche anno.

Il punto saliente del problema è che la rete Internet non è sufficientemente robusta per le applicazioni sensibili al ritardo.

Una trasmissione in tempo reale, infatti, deve essere caratterizzata da:

- Ritardi d'arrivo dei pacchetti contenuti.
- Jitter d'interarrivo ridotto.
- Adeguate risorse di rete (in particolare ampiezza di banda: se la capacità del collegamento è inferiore all'ampiezza di banda richiesta le code all'interno dei router tenderanno a crescere creando ritardo nell'arrivo dei pacchetti e aumentando la probabilità di perdite).

Assicurare ciò significa garantire agli utenti la cosiddetta qualità del servizio (QoS).

» 1.8.1 Jitter

La commutazione a pacchetto implica che i datagrammi, che non compiono percorsi fissi e sono soggetti alla congestione della rete, non arrivano tutti con il ritmo costante col quale sono stati inviati, il che provoca una distorsione nel segnale.

Questo fenomeno di ritardo variabile è appunto il **jitter** ed è necessario ristabilire la frequenza di arrivo dei pacchetti per riottenere un segnale sufficientemente adeguato. È necessario quindi disporre, di una memoria tampone (buffer) in cui accodare i pacchetti e dalla quale attingerli poi in modo sincrono.

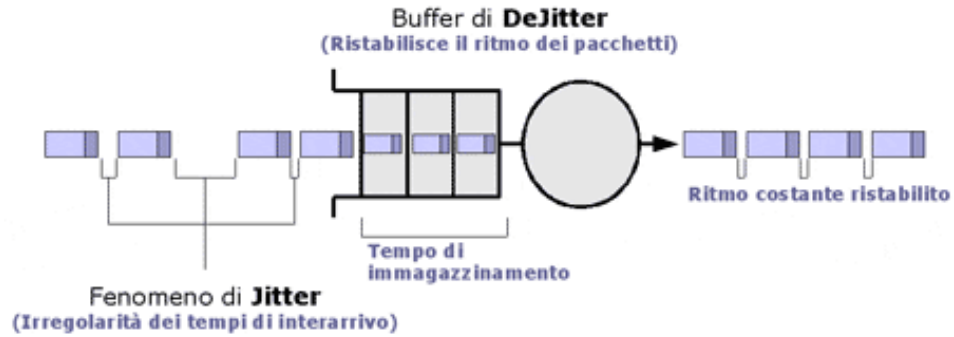

Fig. 8 – Jitter e memoria tampone

Questo sistema di buffering implica un ulteriore tempo di attesa, il tempo di dejitter appunto.

L'introduzione di RTP e l'uso di UDP garantiscono, comunque, delle performances sufficienti nell'attenuazione degli effetti del jitter e della temporizzazione/sincronizzazione e gli algoritmi di compressione dell'audio sono molto efficienti forniscono un buon rapporto tra compressione del segnale e fedeltà: il problema, a questo punto, rimane legato alla disponibilità di banda in caso di congestioni dovute al traffico di rete.

» 1.8.2 Integrated Service e Differentiated Service

Per mitigare il rischio di una perdita di qualità dovuta a colli di bottiglia nella rete sono state ideate le strategie, **IntServ**/**RSVP** e **DiffServ**, che garantiscono priorità ad alcuni flussi di informazioni, agendo sui router che implementano e gestiscono le politiche di instradamento (routine).

IntServ sta per «Integrated Service». È una architettura che introduce delle classi di servizio associate a flussi di pacchetti. Ciascun flusso è associato all'applicazione che ne fa richiesta, è distinguibile ed ha delle particolari richieste di qualità.

Per stabilire la qualità dei flussi viene sfruttato RSVP (resource ReSerVation Protocol): un protocollo che serve a prenotare le risorse di rete necessarie ed a renderle diponibili per un certo tempo.

Anche se lavora proprio sopra il livello IP, RSVP non è un protocollo di trasporto in senso stretto, in quanto non trasporta informazioni. Piuttosto serve agli host per prenotare risorse di rete e ad ogni router, presente sul percorso del flusso, a mantenere e aggiornate le informazioni sulla qualità del servizio.

IntServ differenzia i flussi su tre classi di servizio

- Best effort - i pacchetti subiscono lo stesso trattamento del routing tradizionale. Viene applicato a tutte le classiche applicazioni Internet: HTTP, FTP, e-mail, etc.
- Carico Controllato - per applicazioni con richieste poco esose, che tollerano la perdita dei pacchetti o ritardi consistenti (ordine di pochi secondi). Per esempio lo streaming.
- Garantito - per applicazioni che richiedono tempi di risposta molto stretti e vincoli di banda. Per esempio VoIP.

Una volta che il pacchetto arriva su un router IntServ viene classificato e il router valuta se instradarlo, lasciarlo in attesa o scartarlo a seconda della congestione e della classe di servizio assegnata al pacchetto.

IntServ è una architettura molto efficace: con RSVP si generano dei circuiti virtuali con risorse garantite all'interno della rete a pacchetto. Il limite lo troviamo nella scalabilità.

Ogni router mantiene informazioni sui percorsi di tutti i flussi e per funzionare tutti i router dovrebbero supportare il protocollo RSVP. Queste condizioni diventano difficili da mantenere su reti di grandi dimensioni.

DiffServ sta per «Differentiated Service» e a differenza di IntServ, non richiede ai router di memorizzare le caratteristiche di servizio per ogni flusso.

All'ingresso nel dominio DiffServ, ovvero sui router di contorno (edge routers), ad ogni pacchetto viene assegnato un codice PHB (per Hop Behaviour). PHB stabilisce il comportamento che i router assumono riguardo al flusso ad ogni hop (cioè da un nodo all'altro nella rete).

Purtroppo occorreranno ancora alcuni anni per il completo sviluppo del protocollo IPv6 e il raggiungimento di un'affidabilità del 99.999%, che assicureranno la totale migrazione ad IP per le reti 3G.

Una rete ibrida tra IPv6 e IPv4 non è sufficiente, c'è bisogno di una rete completamente IPv6.

Le problematiche da affrontare sono molte, tra cui: interoperabilità tra le versioni IPv6, maturità del protocollo, necessario upgrade, sviluppo e completa accettazione dell'indirizzamento IPv6 nel mondo.

» 1.9 Il sistema ITU-T H.324

Lo standard ITU-T H.324 è una raccomandazione generale sviluppata tra il 1994 e il 1998 che include diversi componenti:

- Un multiplexer, definito nella raccomandazione ITU – T H.223;
- Un modem V.34;
- Un sistema di comando, controllo e segnalazione definito nella raccomandazione ITU – T H.245;
- Codec audio e video;
- Protocolli opzionali per altre applicazioni, come la condivisione di dati (per esempio la suite ITU – T T.120);
- Supporto opzionale per la codifica.

Ad una applicazione H.324 non sono richiesti tutti questi elementi funzionali, ad eccezione del modem v.34, del multiplez H.223 e del

system control protocol H.245, che sono obbligatori per tutti i terminali H.324.

Comunque, H.324 raccomanda che i terminali supportino il codec audio G.723.1, i codecs video H.261 e H.263. Inoltre, ai terminali H.324 che offrono conferenze real – time audio-grafiche, è richiesto di supportare la suite protocollare T.120.

» 1.9.1 3G-324M

Per risolvere i problemi delle reti IP wireless, le aziende produttrici hanno adottato la specifica 3G-324M.

3G-324M supporta lo streaming real-time per comunicazioni multimediali wireless a banda larga instradando il traffico su reti a commutazione di circuito invece che su rete IP. Per questo motivo lo standard ha tutte le garanzie di un protocollo ideale per lo streaming real-time multimediale, che include un ritardo fisso, un basso overhead dei codec e il non sovraccarico degli header IP/UDP/RTP.

Lo standard 3G-324M deriva da quello dalla ITU H.324, sviluppato per le PSTN e il protocollo v.34 per il modem. H.324 è un protocollo pesante per il setup e la chiusura di una sessione di videoconferenza su una linea telefonica analogica, per cui è stato modificato per reti wireless 3G, permettendo a reti a commutazione di circuito di supportare applicazioni sensibili al ritardo tra terminali 3G.

Il protocollo non utilizza indirizzamento ma solo il vecchio metodo E.164 come base per il W-CDMA per la localizzazione delle parti e verificare che la chiamata tra i due terminali (i peers) sia iniziata.

» 1.9.2 I sottoprotocolli di 3G-324M

Lo standard 3G – 324 M utilizza molti sottoprotocolli.

Tra questi, analizzeremo più da vicino i seguenti:

- Error Resilience Services and Concealment
- H.223 Multiplexing/Demultiplexing
- H.245 Call Control Channel
- 3G-324M Adaptation Layers
- H.245 Call Control Channel
- Voice Channel – adaptive multi – rate (AMR) e G.723.1 codec
- Video Channel – H.263 e MPEG-4 Simple Profile Codec

» 1.9.2.1 La prevenzione degli errori: l'Error Resilience e Concealment

3G-324M opera in ambienti wireless dove è presente un alto BER (bit error rate) durante tutta la sessione. H.223 è la specifica che definisce il multiplex tra il bit stream sottostante e i canali per il controllo di chiamata, l'audio, il video e i dati.

I problemi con H.223 sono i seguenti:

- Errori sui bit che corrompono l'HLDC (high – level data link control) bit stuffing;
- Emulazione dei flag nel payload;
- Flag corrotti;
- Errori nell'header del mux-pacchetto (pacchetto multiplato)
- Errori nei bit del payload

Al livello base H.223, il protocollo HLDC effettua la suddivisione dei pacchetti multiplati in frame. Questo protocollo è comunemente utilizzato in molte reti dati, tuttavia, un livello HLDC a lunghezza variabile non è considerato robusto rispetto agli errori di trasmissione.

Primo problema: il codificatore HLDC, infatti, aggiunge come stuffing un bit '0' dopo ogni 5 bit '1' contigui nel payload; se errori di trasmissione rovinano la struttura del frame, allora il decodificatore HLDC può perdere la sincronizzazione con i dati.

Secondo problema: dopo alcuni bit errati, è molto probabile l'emulazione dei flag nel payload. Tale emulazione, dovuto alla brevità dei framing flag stessi, distrugge la struttura dei pacchetti multiplati e può spostarli in posizioni con corrette.

Terzo problema: l'alterazione dei framing flag, che porta alla concatenazione o perdita di pacchetti multiplati.

Per risolvere questi problemi, l'ITU-T introdusse in H.223 una struttura gerarchica a livelli multipli: livello 0,1 e 2 affinché sia garantito un elevato error resilience (cioè evitare il più possibile la propagazione dell'errore).

- Il livello 0, livello base H.223 definito dall'originale H.324, attualmente non effettua error resilience;

- Il livello 1, definito i H.223 annesso A, sostituisce all'HLDC un framing più robusto, grazie all'uso di una sequenza di 16 bit, senza biti di stuffing. Il vantaggio risultante è un netto abbattimento delle probabilità di emulazione dei flag nei payload, di fronte però ad un maggior rischio di flag corrotti, poiché più lunghi.

- Il livello 2, definito in H.223 annesso B, aggiunge un header (con informazioni sul multiplexing e sulla lunghezza del frame) al pacchetto multiplato, mentre il framing è lo stesso del livello 1.

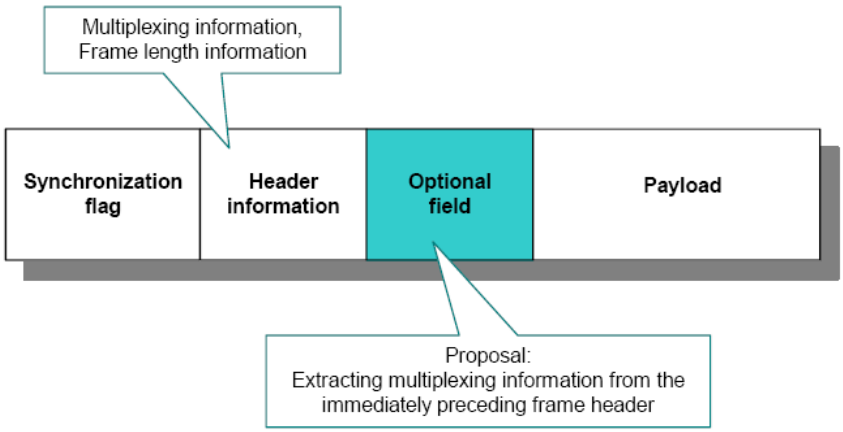

Fig. 9 – Multiplexing del Frame previsto dall'H.223 Annesso B

La specifica 3G-324M definisce, nell'annesso A, il trattamento di un BER basso e nell'annesso B di un BER moderato come supporto obbligatorio per l'error resilience. In più i codec, AMR obbligatorio e MPEG-4 raccomandato, forniscono un ulteriore mezzo per l'error resilience, al fine di minimizzare la degradazione della qualità causata dagli errori sui bit.

In un videotelefono mobile la sfida più grande riguarda i codec video poiché è noto che il video compresso è molto sensibile agli errori di trasmissione.

Nella comunicazione multimediale mobile l'error resilience è fondamentale, per la rivelazione degli errori e il loro trattamento immediato.

Queste soluzioni non riducono gli errori come la tecnica FEC (Forward error correction) e ARQ, automatic repeat request) ma possono ridurre i danni sulla qualità nella decodifica del video.

» 1.9.2.2 H.223 Multiplexing/Demultiplexing Protocol

Il protocollo 3G-324M viene inizializzato dopo l'apertura di un canale a commutazione di circuito tra le due parti comunicanti.

H.223 per il multiplexing è il primo protocollo ad essere instaurato tra le parti. Dopo l'inizializzazione di questo protocollo, il processo di multiplexing deve essere sincronizzato. Inoltre è importante instaurare il controllo di chiamata (H.245) per l'apertura del primo canale logico (channel 0).

La funzione base del protocollo di multiplexing è di effettuare l'interleaver dei media stream multiplati insieme come video, audio, dati e segnali di controllo (H.245) in un singolo stream, in modo tale da essere inviato su un canale di trasmissione, 3G-324M, come protocollo per effettuare la multiplazione, utilizza l'estensione mobile della ITU-T H.223 del livello 2.

H.223 ha uno schema flessibile adatto per una gran varietà di media frame anche a lunghezza variabile. Nella sua estensione mobile, si ottiene una sincronizzazione del canale e un controllo più forte contro gli errori senza perdere di flessibilità. Ci sono 3 modalità – livello 0, livello 1 e livello 2 – che vengono scelti in base al grado di error resilence richiesto.

- ➔ **Multiplexing level 0** – è identico alla specifica H.223, e si occupa di raggiungere multiplexing e QoS (qualità of service) appropriate per ogni tipo di dato multimediale. Il livello 0 è costituito da un adaptation layer e un mux layer, fig. 10. Il mux layer assembla i pacchetti di dati multimediali multiplati in un singolo stream, in accordo con un multiplex pattern (modello) selezionato tra 16 possibili. Il multiplex pattern può essere definito arbitrariamente attraverso la procedura di negoziazione della sessione. L'informazione di header è fissata al controllo con un flessibile meccanismo di multiplexing.

L'header è formato da: un multiplex code (MC) di 4 bit, un marcatore di pacchetto (PM) di 1 bit, e 3 bit di parità header error control (HEC). I campi dei 3 bit HEC si occupano di trovare gli errori nei bit MC, utlizzando un CRC (Controllo a Ridondanza Ciclica) a 3 bit. Per delimitare i mux – packet data unit (PDUs) vengono inseriti 8 bit di flag di sincronizzazione ('01111110') nell'HLDC (High Level Data Controller) e poi viene effettuato l'inserimento (stuffing) di uno '0' ogni cinque '1', per evitare possibili rischi di emulazione degli 8 bit di flag all'interno del pacchetto.

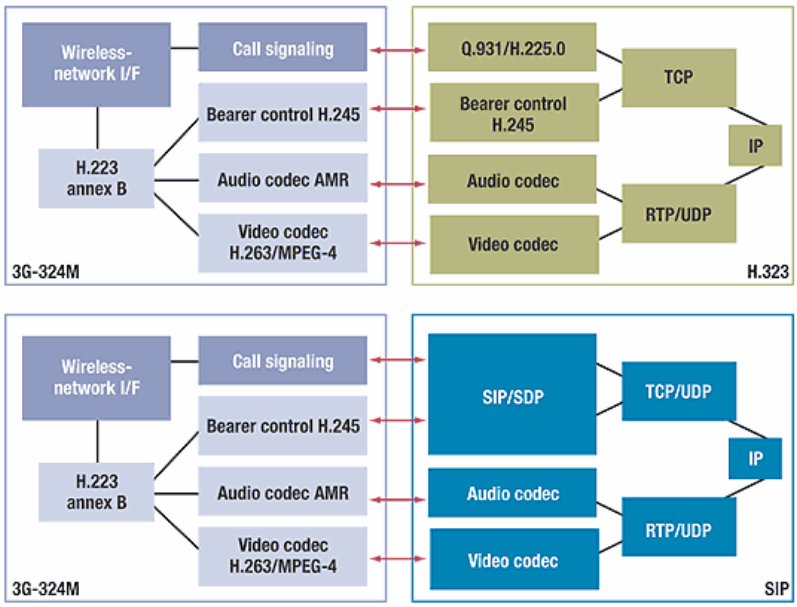

Fig. 10 – Confronto tra H.323/SIP e 3G-324M

➔ **Multiplex level 1** – impiega per la sincronizzazione una sequenza PN a 16 bit anziché gli 8 bit di flag visti prima, allo scopo di migliorare la sincronizzazione del mux – PDU attraverso un canale con errori. Non è consentito lo stuffing per abilitare ricerche di flag di 8 bit. Questa modifica migliora notevolmente la ricerca di flag su canali con errori con una piccola probabilità di emulazione del flag in caso di conflitto.

➔ **Multiplex level 2** – aggiunge al mux – PDU un'informazione sulla lunghezza del payload e un controllo FEC nell'header, per migliorare la sincronizzazione e l'error resilience. Inoltre può aggiungere un campo header opzionale che include MC/PM/HEC per il frame precedente, per migliorare l'error resilience contro errori a burst, con un effetto simile alla diversità temporale.

» 1.9.2.3 3G-324M Adaptation Layer

Nella specifica 3G-324m sono definiti 3 tipi di adaptation layer in accordo con il tipo di dati (video, voce o dati): adaptation layer 1 (AL1), 2 (AL2), e 3 (AL3).

Esaminiamoli in dettaglio:

- **AL1** è progettato per il trasferimento dei dati e il controllo delle informazioni, non ha alcuna capacità di rilevare o correggere errori.
  Quindi è il livello superiore ad effettuare un necessario controllo degli errori, includendo anche la possibilità di una ritrasmissione.
  Il controllo di chiamata H.245 è utilizzato obbligatoriamente appena il bit stream multiplexing è sincronizzato tra le parti comunicanti e poi per canali dati opzionali. Questo AL assume che il livello superiore effettuerà il controllo degli errori.
- **AL2** è progettato per il trasferimento dell'audio digitale. Effettua la rivelazione degli errori con un CRC (cyclic redundancy check) a 8 bit e supporta anche la numerazione della sequenza (opzionale), che potrebbe essere usata per rivelare perdite e cattivo recapito negli AL-PDU. AL2 trasferisce un numero intero di ottetti all'AL-SDU a lunghezza variabile. Sono previsti anche la rivelazione degli errori sulla voce e la numerazione della sequenza. Quest'ultima è a 8 bit

(SN), può frammentare gli AL-PDU e può essere usata dal livello AL2 del ricevente per rivelare perdite di AL PDU.

- **AL3** è progettato per il trasferimento del video digitale e include un controllo CRC a 16 bit per la rivelazione dell'errore, supporta inoltre la numerazione di sequenza (opzionale), che potrebbe essere usata per rivelare perdite negli AL-PDU. AL3 trasferisce un numero intero di ottetti all'AL-SDU a lunghezza variabile ed effettua la ritrasmissione, prevista soprattutto per il video. Ci sono anche la rivelazione di errori, numerazione di sequenze e ARQ.

» 1.9.2.4 H.245 Terminal Control Protocol

3G-324M utilizza il protocollo H.245 per il controllo del terminale, come era già stato utilizzato da H.323 e H.324 per reti PSTN e da H.320 per ATM.

La versione più vecchia di H.245 che può essere supportata in una implementazione di 3G-324M è la tre, comunque è fortemente raccomandato l'utilizzo di versioni superiori per disporre di un set più ricco di servizi per il controllo di chiamata, comandi e indicazioni.

3G-324M non necessita di indirizzamento come per H.323, poiché interviene su un canale già aperto tra due parti comunicanti.

Per questo si prevede la facile realizzazione di gateway (ad esempio tra 3G-324M, H.320, H323 e SIP) che garantiscano l'interoperabilità tra reti differenti.

Poiché non è utilizzato il protocollo H.323 per assicurare l'affidabilità delle operazioni, H.245 richiede il NSRP (numbered simple retransmission protocol) e il CCSRL (control channel segmentation and reassembly layer).

Quindi i terminali mobili devono supportare le modalità NSRP e SRP. Se ogni terminale inizia la sessione al livello 0, il sistema H.245 deve operare in SRP. Se invece i terminali iniziano la sessione al livello 2, viene impiegato NSRP.

D'altra parte CCSRL è utilizzato per trasportare grandi pacchetti H.245.

In più per supportare NSRP e CCSRL, il protocollo di controllo H.245 ha le seguenti funzionalità e servizi:

- **Master-slave determination** determina quale terminale è il master all'inizio della sessione. Il fatto che H.245 sia un protocollo simmetrico rende indispensabile questo passo, dal momento che il master deve prendere le decisioni in caso di conflitto.
- **Capability exchange** è la fase di scambio delle capacità di ogni terminale, e serve a stabilire modi opzionali di multiplexing, tipo di audio/video codec, modalità di data sharing e suoi parametri relativi, e/o altre caratteristiche opzionali.
- **Logical channel signaling** necessaria per l'apertura e la chiusura dei canali logici. Questa procedura include anche i parametri di scambio per l'uso dei canali logici.
- **Multiplex table initiation/modification** aggiunge o cancela le entry nella multiplex table.
- **Mode request** serve a richiedere in che modalità si sta operando dal lato ricevitore al lato trasmettitore. In H.245, la scelta dei codec e dei suoi parametri è presa dal lato trasmettitore considerando la capacità del decodificatore, così se il lato ricevitore ha delle preferenze riguardo la capacità, viene utilizzata questa procedura.
- **Round – trip delay measurement** per aver una misura più accurata

- **Loopback testing** necessario durante lo sviluppo o in alcuni campi per assicurare operazioni particolari
- **Miscellaneous call control commando and indications** serve a richiedere la modalità di comunicazione, flow control come comandi per la conferenza, indicazioni di jitter e skew, o per indicare le condizioni del terminale dall'altro lato.

H.245 utilizza l'abstract syntax notation 1 (ASN.1) per definire i parametri dei messaggi facendo in modo che siano effettivamente leggibili.

Per codificare in binario questi messaggi ASN.1 viene utilizzato il PER (packet encoding rule) per utilizzare l'effettiva larghezza di banda richiesta nella trasmissione del messaggio. Come detto in precedenza, terminata la sincronizzazione al livello di multiplexing tra le parti, il primo canale logico che viene aperto (channel 0) è H.245 call control con CCSRL e NSRP, per garantirne un'alta affidabilità e permettergli l'utilizzo di pacchetti grandi durante le operazioni.

» 1.9.2.5 Voice channel – AMR codec

La specifica 3G.324M stabilisce che l'AMR codec sia obbligatorio. Inoltre raccomanda l'utilizzo di G.723.1 usato attualmente in molti terminali H.323.

L'AMR codec fu sviluppato e standardizzato originariamente dalla ETSI per i sistemi GSM, e si adatta dinamica ai bit allocati dal codificatore della voce e dal controllo dell'errore, fornendo la migliore qualità per la voce in ogni situazione e condizione del canale radio. Il codec AMR migliora l'efficacia del frequency hopping e del riuso dei pattern, permettendo una maggior percentuale di canali radio utilizzabili contemporaneamente, con un guadagno aggiuntivo di circa il 150%.

AMR fu scelto da 3GPP come codec obbligatorio per i cellulari di terza generazione. Esso include 8 modalità a banda stretta: 12.2, 10.2, 7.95, 7.4, 6.7, 5.9, 5.5 e 4.75 kbit/s. Inoltre supporta il comfort noise (CS) per una modalità di trasmissione discontinua (DTX).

Dal punto di vista dell'adattamento sul rate, l'AMR codec supporta l'unequal bit-error detection and protection (UED/UEP).

Questo meccanismo permette di avere molta più voce su una rete con perdite dividendo i bit in classi di percezione più o meno sensibili. Un frame è considerato danneggiato e non viene consegnato, se vengono trovati bit meno sensibili, stabiliti in base alla percezione uditiva umana. Un'importante caratteristiche dell'AMR, per un ambiente con un alto valore del BER come le reti wireless, è la robustezza contro i pacchetti persi, grazie alla ridondanza e alla divisione per sensibilità dei bit errati.

Un ulteriore beneficio è l'adattatività del rate per commutare agevolmente tra le varie modalità.

» 1.9.2.6 Video Channel – MPEG-4

3G-324M per il video processing richiede H.263 come codec obbligatorio e MPEG-4 raccomandato, anche se MPEG-4 è lo standard de facto utilizzato dalla maggior parte dei produttori.

Funzionalità come la prevenzione dell'errore e alta efficienza fanno di MPEG-4 un codec particolarmente adatto per 3G-324M.

MPEG-4 rispetto a H.263 è molto più flessibile e offre metodi avanzati di rivelazione e correzione di errori, che costituiscono un grande valore aggiunto per il trasporto di video su reti wireless. Entriamo più nel dettaglio in questi metodi.

MPEG-4 visual (ISO/IEC 14496-2) è un codec video generico particolarmente adatto per 3G-324M grazie all'error resilience e alta

efficienza. Quando è supportato, 3G-324M prevede che esso abbia il semplice profilo 1 livello 0 chiamato simple profile.

MPEG-4 è organizzato in profili, con i quali vengono definiti vari livelli. I profili definiscono un sottoinsieme di un certo numero di operazioni. I livelli sono relativi alla complessità computazionale. Fra questi, il simple profile effettua error resilience ed ha bassa complessità.

L'error resilience è ottenuto attraverso:

- **Risincronizzazione**: nella specifica MPEG-4, un marker di risincronizzazione riduce la propagazione dell'errore causato dalla natura del codice a lunghezza variabile (VLC) in un singolo frame. Il marker è inserito all'inizio di un nuovo gruppo di GOB insieme con l'header (multiplez block number [MBN]; parametri di quantizzazione) e HEC opzionale,così che può essere decodificato indipendentemente. Mettere il marker prima di un oggetto importante fa avere error resilience con il minimo incremento dell'overhead.
- **Allineamento dei byte**: il bit-stuffing per l'allineamento dei byte conferisce una maggior capacità di rivelare l'errore attraverso il controllo della sua violazione.
- **Partizionamento dei dati**: un nuovo codice di sincronizzazione chiamato motion marker, separa i campi di motion vector (MV) e discrete cosine transform (DCT) per prevenire che si propaghi errore tra i campi, ottenendo un effettivo post-trattamento. Quando viene trovato un errore solo nel campo DCT, il multiplexex block (MB) verrà ricostruito utilizzando il corretto MV. Questo, nel movimento naturale, risulta migliore rispetto alla sostituzione del frame precedente.
- **RVLC (Reversibile Variable Lenght Code)**: abilita la decodifica in avanti e all'indietro senza un impatto significativo sull'efficienza del codice. Ciò permette di circoscrivere la propagazione dell'errore idealmente ad un singolo MB.

- **AIR (Adaptive Intra Refresh)**: a differenza del convenzionale intra refresh ciclico, AIR impiega un motion intra refresh pesato, che dà una migliore qualità di percezione con recuperi veloci in oggetti corrotti.
- **Error detection and concealment**: gli errori possono essere rivelati attraverso eccezioni o violazioni nella decodifica per cui è applicato il post-trattamento (concealment). Questa funzionalità insieme all'audio MPEG-4 può essere utilizzata con dispositivi mobili H.324.