

Internet Engineering Task Force
Internet Draft
[draft-ietf-avt-mux-rtp-00.txt](#)
Aug 21, 1998
Expires: Feb 21, 1999

AVT Working Group
B. Subbiah, S. Sengodan
Nokia Research Center.

User Multiplexing in RTP payload between IP Telephony Gateways

STATUS OF THIS MEMO

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress''.

To learn the current status of any Internet-Draft, please check the ``[1id-abstracts.txt](#)'' listing contained in the Internet-Drafts Shadow Directories on [ftp.is.co.za](#) (Africa), [nic.nordu.net](#) (Europe), [munni.oz.au](#) (Pacific Rim), [ds.internic.net](#) (US East Coast), or [ftp.isi.edu](#) (US West Coast).

Distribution of this document is unlimited.

ABSTRACT

This draft proposes a method to multiplex a number of low bit rate audio streams (upto 256) into a single RTP/UDP/IP connection between IP telephony gateways. Audio samples from different users are assembled into an RTP payload thus reducing the overhead of RTP/UDP/IP headers. To identify users sharing a single RTP/UDP/IP connection, a 2 byte MINI-Header is proposed. A channel negotiation procedure to assign and release channels on a single UDP connection between gateways is described.

1 Introduction

IP telephony gateways provide an interface between the existing circuit switched telephone networks (such as PSTN and GSM) and the packet switched IP data networks. In a traditional IP telephony application, telephone calls between PSTN/GSM users interconnected by a pair of IP telephony gateways are carried by separate RTP/UDP/IP connections. Codecs at the IP telephony gateway which compress incoming PSTN/GSM speech samples generate packets with sizes ranging

from 5 to 20 bytes per speech sample. For example, G.723.1 (the most popular IP telephony codec and the IMTC VoIP Forum's mandatory low bit-rate codec), generates a 20 byte speech packet at 30 ms intervals

[4]. Many codecs used in cellular environments generate packets of size less than 10 bytes per speech sample. Small size packets are subject to a large overhead when transferred using the Real time Transport Protocol (RTP). The RTP/UDP/IP overhead is 40 bytes (12+8+20) for a single speech packet. For example, a 10 byte packet transferred via RTP/UDP/IP has an overhead of 80%.

In addition, for each call request a single UDP/IP connection (a pair of UDP ports) is established between the gateways. This not only limits the number of audio streams between the gateways to the number of available UDP port pairs, but also requires a large state (memory) to be maintained at the telephony gateways, thereby making these gateways less scaleable.

Another disadvantage of the traditional RTP/UDP/IP method in a gateway scenario is the possibility of congestion at intermediate routers in the IP network. In the RTP/UDP/IP method, each individual speech packet is transmitted as a single IP packet, which results in large number of small sized IP packets between gateways. This is a potential situation for congestion at intermediate IP routers. Congestion in IP networks results in packet loss and UDP does not have any re-transmission mechanism to recover lost packets. Also, real time applications such as speech are intolerant to delay caused by re-transmission.

In this draft, we propose a mechanism that enables several streams (upto 256) to share a single RTP/UDP/IP connection between IP telephony gateways thereby reducing the overhead, lowering the possibility for congestion at IP routers, and making such gateways more scaleable. This method is suitable for IP telephony gateways that interconnect PSTN/GSM users through IP networks. In a cellular environment, it can also be used in cellular trunking, links that interconnect Base Station (BS), Base Station controller (BSC), and Mobile Switching Center (MSC) of a Radio Access Network (RAN). Individual user packets multiplexed in an RTP payload are identified using a 2 byte MINI-header. The channel association between gateways for a single user can be carried out by one of the three mechanisms described later in this draft.

2 User multiplexing in RTP payload

It has been observed that, at any given time there are multiple active users between IP telephony gateway pairs that interconnect PSTN/PBX/GSM clouds. This is also true in the case of cellular trunking between a Base Transmission System (BTS) and BSC/MSC. At present, IP telephony gateways establish and maintain a separate RTP/UDP/IP connection for each call request. In the above scenarios, a large number of connections originate and terminate between two

gateways interconnected by an IP network. This is an ideal situation for multiplexing a group of users in a single RTP/UDP/IP connection.

The mechanism for user mux in RTP that is proposed in this draft decreases the overhead by multiplexing two or more (up to 256) low bit rate connections (compressed speech) in a single RTP/UDP/IP connection. To enable such multiplexing, a 2 byte header called

MINI-Header is prepended to each mini packet before it is assembled with other mini packets into an RTP payload. To identify a single user among the number of users sharing the same RTP connection, each user is assigned a unique Channel Identifier (CID) which is negotiated during connection setup. The CID negotiation procedure is carried out by a control signaling which may be based on one of the three methods(CNP, SIP and H.225) described in [section 3](#).

2.1 MINI-Header

The format of a MINI-Header is shown in Figure 1:

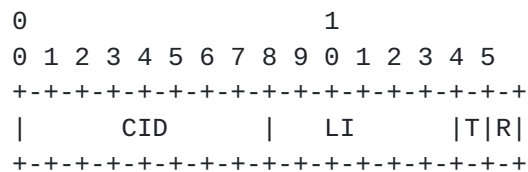


Figure 1: Format of a MINI-Header

The length of the MINI-Header is 2 bytes, which includes a Channel Identifier(CID), Length Indicator (LI), Transition bit (T) and a Reserved bit (R). The purpose of each field is described below:

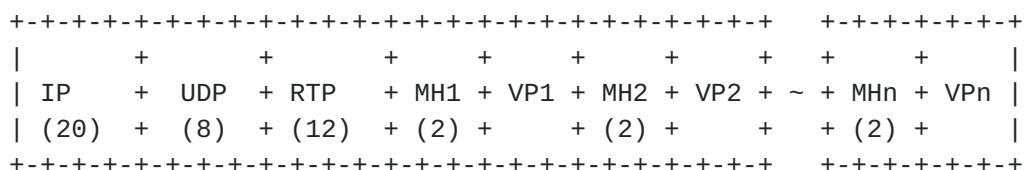
- Channel IDentification (CID): This 8 bit field allows a maximum of 256 users to share a single RTP/UDP/IP connection. When the total number of users exceeds 256, a new RTP/UDP/IP connection is established.
- Length Indicator (LI): This 6 bit field allows a maximum payload size of 64 bytes.
- Transition bit (T): The transition bit is used to facilitate dynamic re-negotiation of mini-packet processing. Notification of such changes occurs by toggling the bit.
- Reserved bit (R): The use of this bit is being explored at this moment.

It has been observed that an 8 bit CID is sufficient for multiplexing since there are enough speech samples at any instance. Most of the codecs generate packets less than 40 bytes per speech sample that can be easily accommodated with a 6 bit LI field. While the presence of a Sequence Number (SN) field and a Marker (M) field in the mini-header could be useful at the receiving gateway, we believe that the presence of these fields is not critical. The SN field in the RTP

header can guarantee the order of packet (RTP packet) arrival at the receiver. If the packet multiplexing order at the transmitter is maintained then there is no need for SN in the MINI-Header from the standpoint of in-sequence arrival of packets within a single RTP/UDP/IP connection. Moreover, a Header Error Control (HEC) field to protect from transmission errors has been left out because UDP checksum could be used for the same purpose.

2.2 RTP Payload Format

A speech sample (voice packet) received from a user is converted to a mini packet by adding the 2 byte MINI-Header. The CID selection and channel negotiation procedures are carried out before the packet is assembled. These procedures are described in [section 3](#). The assembly of mini packets into a single RTP payload with RTP/UDP/IP header is shown in Figure 2. The mini packets follow the RTP header and each mini packet is delineated by the 2 byte MINI-Header. This arrangement of a MINI-header followed by payload allows variable sized packets (≤ 64 bytes) to be assembled without the knowledge of the payload itself. Moreover, this scheme requires a very simple de-multiplexing algorithm at the receiver. The RTP payload received by the remote gateway is de-assembled to recover the individual mini packets until the payload becomes empty. The packets are then delivered to the respective users based on the channel association carried out during the call setup phase.



*MH - Mini Header, VP - Voice Packet

Figure 2. RTP payload format with user multiplexing

2.3 Packet assembly timer

While assembling mini packets into an RTP payload, there is a need to control the waiting time (delay) between the placement of the first packet in the RTP payload and the transmission of the complete IP packet to the remote gateway. Without a timer, packets placed at the beginning will be subjected to a large delay. This problem occurs when there is a large interval between successive packet arrivals at the multiplexing end. To solve this problem, we propose a timer called `TIMER_MUX` to control the maximum delay a mini packet may be subjected to during the RTP payload assembly. The `TIMER_MUX` is initialized when the first packet is placed in the RTP payload and upon the timer expiry the RTP/UDP/IP packet is transmitted. There are instances when the RTP/UDP/IP packet needs to be transmitted without the expiry of `TIMER_MUX`. The higher the `TIMER_MUX` value the better the bandwidth efficiency. However, a higher `TIMER_MUX` value means additional delay for voice packets.

2.4 Packet Size

The assembly process of mini-packets into an RTP payload should not only consider the TIMER_MUX value but should also take into account the size of the resulting IP datagram. The size of the resulting IP datagram should not exceed the maximum transmission unit (MTU) of the

IP network. Hence, when the IP network is the public Internet, the size of the IP datagram should not exceed 1500 bytes. It has been determined that an IP datagram of size less than 1500 bytes usually goes through the Internet unfragmented.

2.5 UDP connection

Implementation details of sharing a pair of UDP ports among different users and reusing the same port numbers for persistent UDP sessions are beyond the scope of this document.

3 Control signaling for user multiplexing

The user plane and control plane between gateways is shown in Figure 3. The control plane signaling is needed because peer Mux controllers are required to negotiate a channel for an incoming call request on an existing or on a new UDP connection. The control signaling is transferred using a common persistent connection, which may be either connection oriented (TCP) or connectionless (UDP). The user plane association (CID allocation on a UDP connection) is made after a successful connection setup. In this draft, we describe three different approaches to establish and clear a CID association. The user plane data is carried over RTP/UDP/IP layers in a manner similar to the audio and video transport over IP networks. The description of the signalling and control operation is not meant to be comprehensive.

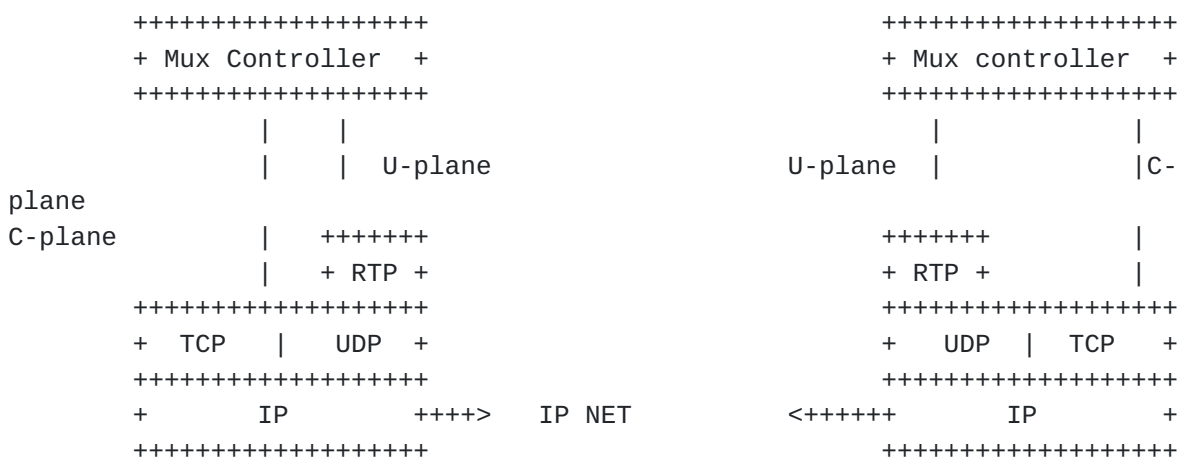


Figure 3. Control plane and user plane in a user multiplexing scenario

3.1 CID selection

Irrespective of the choice of the signaling mechanism between the MUX controllers, the CID selection procedure at each of the MUX controllers MUST be done as follows:

- 1) Arrival of a new call from a PSTN/GSM user triggers a CID assignment sequence at the MUX controller of the local gateway. After establishing which remote gateway can handle the call, the local MUX controller checks for the existence of an RTP/UDP/IP connection to the remote MUX controller. If there exists a UDP connection with free CIDs, then a CID is chosen and reserved for that call. If there is no UDP connection between the gateways or if all the existing connections are full (i.e., no free CID), then a new RTP/UDP/IP connection is established. Once the CID selection is done, a notification message that consists of CID, calling user ID, called user ID, local and remote UDP port numbers is transmitted. Such transmission may occur either in the initial notification message (during call setup) or in the notification message for capability exchange that occurs after call setup.
- 2) Upon receiving the message containing the CID, the MUX controller at the remote gateway checks its CID table associated with the UDP connection. The status of CIDs is maintained in a CID table, which is associated with each UDP connection between any two gateways. If the CID indicated in the notification message has not already been assigned, then the remote MUX controller makes an entry in its CID table assigning the CID to a call between the pair of UDP ports as indicated in the notification message. If the UDP port at the remote gateway is not already open, then the MUX controller opens the UDP port. Table 1 shows a sample CID table used at a gateway for a single UDP connection.

CID	CID status	Local UID	Remote UID
5	Assigned	6172300000	9127363736
10	Reserved	6175464636	8263737474
20	Idle		
200	Idle		

Table 1. CID table for a single UDP connection

3.2 CID collision

During the CID negotiation procedures, there is a possibility that the same CID is selected by both ends for their own call requests. Both gateways transmit channel request messages with the same CID without the knowledge of the other gateway. After receiving the request, both sides are unable to allocate the CID since it has been

reserved for their local call request. This problem is otherwise known as CID glare. We propose to use a method that is fair to both ends in CID assignment procedures. In this method, one side is assigned to allocate CIDs from the top of the CID table and the opposite side from bottom. However, CID collision occurs when a single CID is available at both ends. Even in such a case, fairness can be achieved by an assignment based on the even and odd value of CID. The arbitration of which side starts from top can be resolved using IP address of the gateways. For example, the gateway with the higher IP address starts from the top and the other gateway starts from the bottom.

3.3 Channel Negotiation Procedures (CNP)

CNP is a new control signaling specifically proposed for the user multiplexing application between IP telephony gateways that interconnect PSTN/GSM clouds. The function of CNP is to negotiate a CID for a call through a set of messages similar to standard signaling protocols. Since CNP is targeted for a specific application, we do not anticipate the need for complex signaling procedures similar to H.225/H.245 [5,6]. However, H.225/H.245 could be adapted to suit the requirements of the user multiplexing in RTP method. CNP consists of a set of messages that include assign, assign_confirm, release, release_confirm and reject. An additional message "messages_transfer" is also proposed in case there is a need to transmit control messages of a particular user (call control messages) during the active session of a call. A detailed study on the format of the CNP messages and their parameters will be reported later.

The following is the sequence of events that occur in a channel negotiation phase:

- Assign: Upon arrival of a new call from a PSTN/GSM user, a CID is assigned based on the procedure described in the previous section. An "assign" message is then transmitted to the remote gateway containing the local UDP port number, remote UDP port number, CID number, calling and called user, and an UUI field to carry any call control signaling (PSTN and SS7).
- Assign_confirm or reject: The remote peer recovers the information within the "assign" message and does local processing as described in the previous section. If the call can be accepted then the local Mux controller updates its local CID table and replies with an "assign_confirm" message. If the remote gateway experiences a problem in allocating the connection, say due to CID collision, then it transmits a "reject" message. Upon recei-

ving the "assign_confirm" message, the local Mux controller confirms the CID assignment by updating the CID table and notifying the local user.

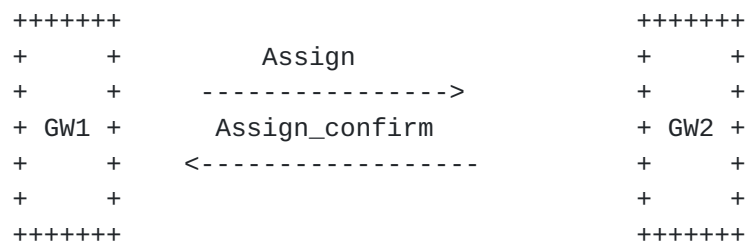


Figure 4: CNP Confirm sequence

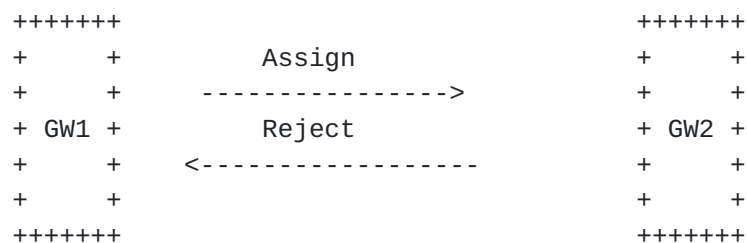


Figure 5: CNP Reject sequence

[3.4](#) Use of H.225/H.245 for channel negotiation

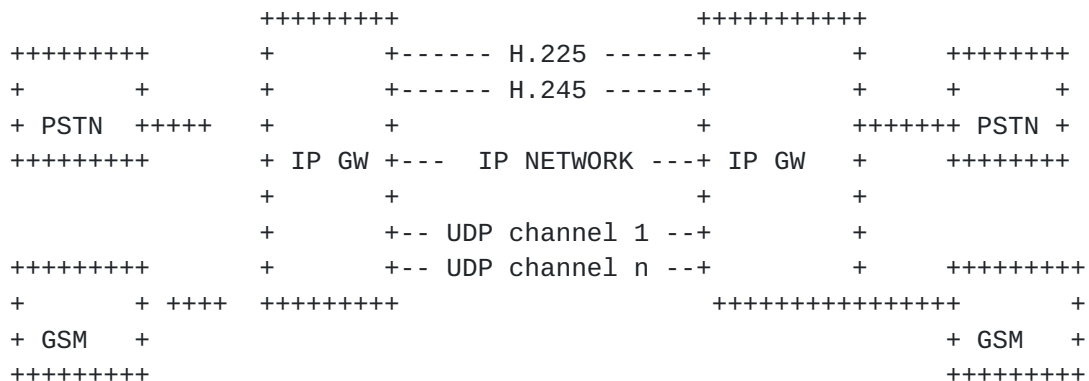


Figure 6: H.225/H.245 in an IP telephony gateway

ITU-T has standardized H.225[5] and H.245[6] as the call signaling protocol and call control protocol respectively to be used within the ITU-T standard H.323[7]. H.225 and H.245 may be used for signaling and control purposes between the gateways. When this is the case, persistent H.225 and H.245 connections exist between a pair of gateways. All voice connections between the two gateways should use the same H.225 and H.245 connection for call signaling and call

control purposes.

When a new call arrives at a gateway from the circuit switched side (PSTN/GSM), a SETUP message is transmitted from the initiating gateway to the terminating gateway on the persistent TCP call-signaling channel (H.225 channel). The User-User-Information-Element (UUIE) of the SETUP message includes the parameters that are needed for connection setup as indicated in the H.225 document [9].

For the purpose of user multiplexing between gateways, the setting of the UUIE fields in the SETUP message MUST be as follows:

- h245Address: This field is set to the TSAP address of the call control TCP channel (H.245 channel) at the initiating gateway that will be used for call control purposes of this voice stream. Initiating gateways should use the same call control channel for all voice streams. However, the initiating gateway may wish to open a new call control channel when the number of voice streams using the same control channel exceeds a certain threshold value. When the initiating gateway wishes to use a new call control channel, the TSAP address of the new H.245 channel is included in this field.

If the remote gateway responds with a CONNECT message upon receiving the SETUP message, the UUIE fields within the CONNECT message MUST be set as follows:

- h245Address: This field is set to the TSAP address of the call control TCP channel (H.245 channel) at the responding gateway that will be used for call control purposes of this voice stream. Remote gateways should use the same call control channel for all voice streams when an initiating gateway has used the same existing call control channel. If a remote gateway wishes to use a new call control channel when the initiating gateway has indicated the use of an existing call control channel in the SETUP message, then the remote gateway must send a FACILITY and a RELEASE message. However, if an initiating gateway has indicated the use of a new call control channel, then the remote gateway must use a new call control channel. The TSAP address of the new call control TCP channel at the remote gateway is included in this field.

Upon receiving the CONNECT message from the remote gateway, the call control phase (H.245) begins. The capability exchange messages determine the choice of codecs and the security parameters if any to be used between the gateways. In addition, the capability exchange also indicates the capability for performing multiplexing. In the openLogicalChannel (and openLogicalChannelAck) message, in addition to indicating the TSAP address, the CID is also indicated.

++++++		++++++
+ +	SETUP	+ +
+ +	----->	+ +
+ GW1 +	CONNECT	+ GW2 +
+ +	<-----	+ +
+ +	CapabilitySet	+ +
+ +	----->	+ +
+ +	CapabilitySetAck	+ +
+ +	<-----	+ +
+ +	OLC	+ +
+ +	----->	+ +
+ +	OLCAck	+ +
+ +	<-----	+ +
++++++		++++++

Figure 7: H.225/H.245 exchange sequence

++++++		++++++
+ +	SETUP	+ +
+ +	----->	+ +
+ GW1 +	FACILITY	+ GW2 +
+ +	<-----	+ +
+ +	RELEASE	+ +
+ +	<-----	+ +
++++++		++++++

Figure 8: H.225 Facility/Reject sequence

3.5 Use of SIP for channel negotiation

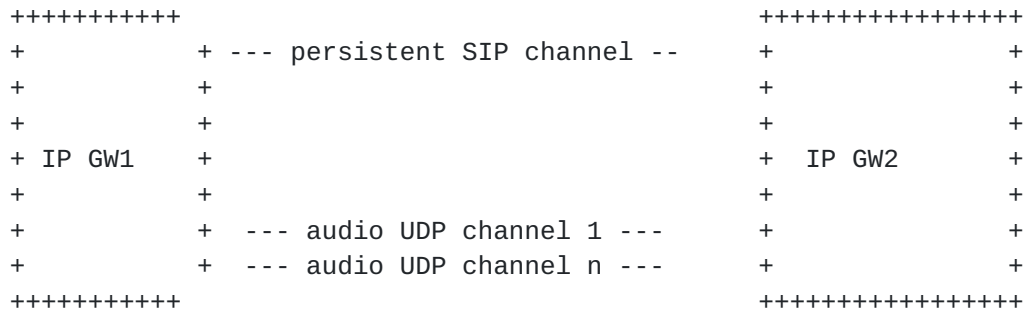


Figure 9. SIP in IP telephony gateways

Session Initiation Protocol (SIP) can be used as the control signaling protocol between the two gateways [11]. In this case, the gateway that receives a call from the circuit switched side is the SIP client, while the remote gateway is the SIP server. The series of messages that are exchanged are described below. These messages are exchanged on the persistent signaling connection existing between the two gateways. Such a persistent connection may either be TCP or UDP.

As with the case of H.225, the description here is not meant to be exhaustive but is merely for illustration. Issues such as locating the remote gateway by the use of proxy or redirect servers, among other things, are not discussed here.

When a new call comes into the initiating gateway from the circuit switched side, an INVITE message is sent from the calling gateway (SIP client) to the called gateway (SIP server). The fields of the INVITE message are set as follows:

- Request-URI: This field contains sip:phonenumber@remotegateway. For instance, if the number being called is +1-781-359-5112 and the remote gateway that can handle this call is gw1-boston.research.nokia.com, then the Request-URI has a value sip:+1-781-359-5112@gw1-boston.research.nokia.com.
- Session Description: The session description includes the capability of the initiating gateway with regard to supported

codecs, supported security parameters etc. Also included in the session description is the Channel Identifier (CID), the source UDP port and the destination UDP port.

Upon receiving the INVITE message, the remote gateway returns the following messages in the sequence indicated:

- TRYING: This message indicates to the calling gateway that the remote gateway has received the INVITE message successfully and that the remote gateway is trying to establish contact with the user. This is also an indication to the initiating gateway not to retransmit the INVITE message.
- RINGING: This message indicates that the user has been contacted and that his phone is ringing.
- SUCCESS: This message indicates that the user has answered his phone.

The SUCCESS message is sent by the remote gateway only if the CID value indicated in the INVITE message is acceptable to the remote gateway. Upon receiving the SUCCESS message, the initiating gateway returns an ACK message back to the remote gateway. This is illustrated in Figure 10.

If the CID indicated in the INVITE message is not a valid one, the remote gateway returns an ERROR/FAILURE message back to the initiating gateway as indicated in Figure 11.

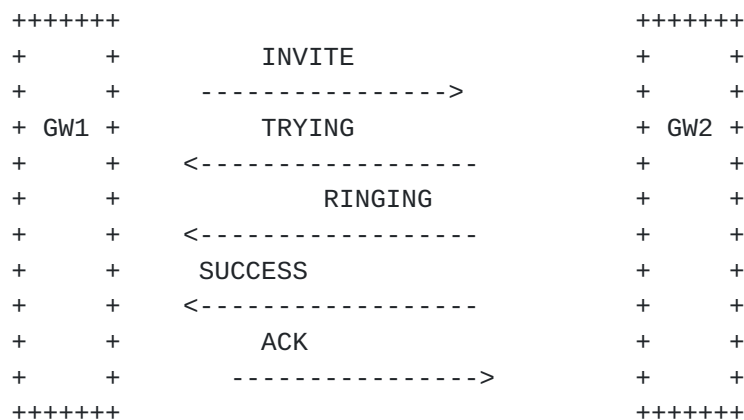


Figure 10: SIP Confirm sequence

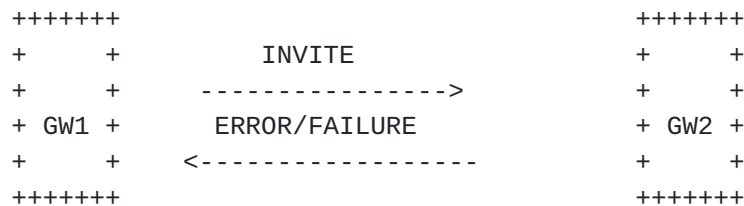


Figure 11: SIP Reject sequence

4 Transmission errors and packet loss

Protocols such as ATM, IP and AAL2 specify a Header Error Correction (HEC) to detect errors in the headers, whereas UDP offers both header and payload protection. The UDP checksum field in the UDP header is calculated for the entire UDP packet including the header and payload bytes. The MINI-header used for user multiplexing is 2 byte long and does not have any HEC field. The reason is that the mini packets are encapsulated within a UDP payload thus protected by the UDP checksum. The presence of the RTP sequence number in the RTP header facilitates to identify packet losses at the RTP level. Since each RTP packet contains a number of mini packets, packet loss at individual level becomes difficult. However, it is our understanding that the SN for individual mini packet is not necessary.

5 Application scenarios

Some of the most obvious scenarios, in which the proposed method is beneficial, are shown in Figure 12. Traditional telephony system such

as PSTN interconnected by IP telephony gateways is an ideal scenario where user mux method improves the bandwidth efficiency in the IP

network. This method can also be used in the Radio Access Network (RAN) of a cellular network. In cellular trunking, mux controller is a part of the BS and BSC/MSC connected by IP networks. User aggregation can be applied between BTS and BSC as well as between BSC and MSC.

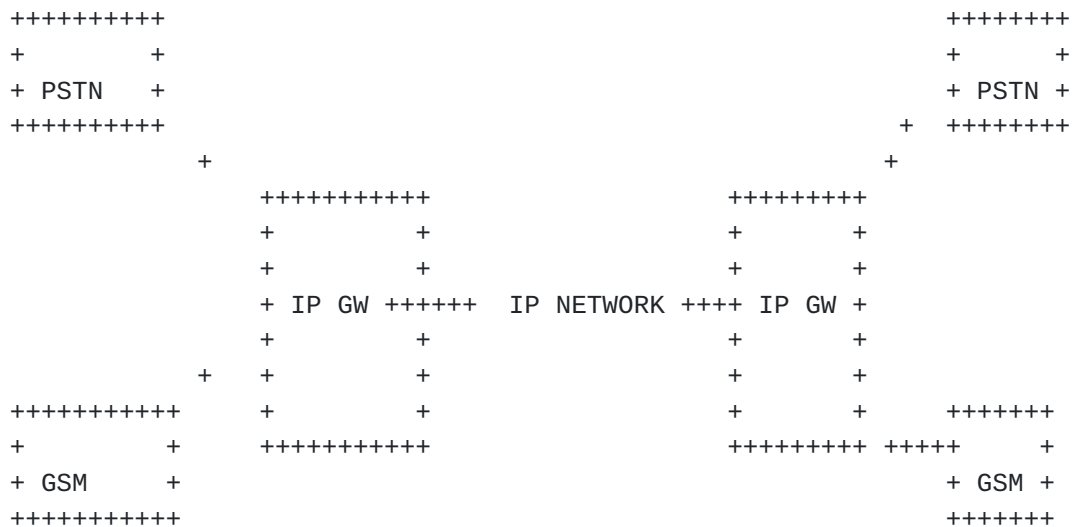


Figure 12. Application scenario of User mux in RTP

6 Security Considerations

There are no security considerations beyond those addressed in RTP itself. The multiplexing protocol can make use of whatever encryption and authentication schemes are present in RTP, SIP, H.323 or other relevant protocols. For instance, the multiplexed media stream could be secured by securing the UDP ports using IPSEC. The signaling and control channels could be secured either by the use of IPSEC or TLS. Application level security as specified in SIP and H.235 may also be incorporated.

7 Comparison of User mux in RTP and traditional RTP/UDP/IP

The important reason for multiplexing small size packets into a single RTP payload is that the RTP/UDP/IP overhead for each packet can be reduced. For example, the RTP/UDP/IP overhead is 66.7% in case of 20 byte G.723.1 packet and 80% for a 10 byte G.729 packet. Considering that IP telephony gateways transfer 100s of user at any given time, the total bandwidth requirement including the overhead is very high. The bandwidth requirement for a traditional scheme (RTP/UDP/IP) is compared to user mux in RTP and the results are shown in Table 2. The results indicate that the bandwidth requirement to

transport same number of users through user mux is very low compared to the traditional IP telephony (RTP/UDP/IP) method.

# users	No Mux (G.723.1)	User Mux (G.723.1)	No Mux (G.729)	UserMux (G.729)
10	159	68.9	400	128
30	477	185.5	1200	320
50	795	302.1	2000	512
70	1113	418.7	2800	704
90	1431	535.3	3600	896
110	1749	651.9	4400	1088
130	2067	768.5	5200	1280
150	2385	885.1	6000	1472
170	2703	1001.7	6800	1664
190	3021	1118.3	7600	1856
210	3339	1234.9	8400	2048
230	3657	1351.5	9200	2240
250	3975	1468.1	10000	2432

Table 2. Bandwidth requirements in Kbps for user mux and IP methods

A comparison of percentage overhead for two different speech codecs is shown in Table 3. The overhead due to RTP/UDP/IP is constant for both codecs. User mux in RTP method is able to multiplex small packets into a single RTP/UDP/IP payload thus reducing the overhead to minimum. The overhead comparison on both codecs proves that user mux in RTP is very efficient in reducing the overhead.

#Users	Mux(G.729)	IP (G.729)	Mux(G.723.1)	IP (G.723.1)
10	37.5	80	23.07692308	66.7
30	25	80	14.28571429	66.7
50	21.875	80	12.28070175	66.7
70	20.45454545	80	11.39240506	66.7
90	19.64285714	80	10.89108911	66.7
110	19.11764706	80	10.56910569	66.7
130	18.75	80	10.34482759	66.7
150	18.47826087	80	10.17964072	66.7
170	18.26923077	80	10.05291005	66.7
190	18.10344828	80	9.952606635	66.7
210	17.96875	80	9.871244635	66.7
230	17.85714286	80	9.803921569	66.7
250	17.76315789	80	9.747292419	66.7

Table 3. Comparison of % overhead due to IP and user mux in RTP

8 Advantages of user multiplexing in RTP

The first advantage of using the proposed method between IP telephony

gateways is the bandwidth efficiency. The second advantage of sharing a single RTP/UDP/IP is that the number of UDP connections is reduced between gateways. For example, in the proposed user multiplexing method a single UDP connection can be shared by a maximum of 256 users. The third advantage is that the less chances for traffic congestion at intermediate IP routers, because the proposed method reduces the number of IP packets by multiplexing mini packets in a single RTP payload. Despite the multiplexing effect, user multiplexing in RTP does not cause any problems in the IP network since RTP payload (mini packets) is transparent to the intermediate IP routers. The user mux method requires minimal effort on standardization and could be implemented as an add-on module to the existing telephony gateways.

9 Comparison of three different proposals

We have found two other proposals [9,10] submitted as IETF drafts to the AVT group. We have compared our proposal with others in terms of known performance metrics. Table 4 summarizes the results of the comparison.

+							
	+	Nokia	+	Lucent	+	Hitachi+	
+							
	+		+		+	+	
+Reducing overhead	+	Very good	+	Very good	+	ok	+
	+		+		+		+
+Bandwidth efficiency	+	Very good	+	Very good	+	ok	+
	+		+		+		+
+Additional header	+	yes	+	yes	+	Not known	+
	+	(2 bytes/pkt)	+	(2 bytes/pkt)	+		+
	+		+		+		+
+Assembly and	+	Simple	+	Hard	+	Simple	+
+de-assembly	+		+		+		+
	+		+		+		+
+Max # of users	+		+		+		+
+for multiplexing	+	256	+	256	+	Not known	+
	+		+		+		+
+Mini packet size	+	Variable	+	Variable	+	Variable	+
	+	(0 ~64)	+	(req. known	+		+
	+		+	profiles)	+		+
	+		+		+		+
+Channel association	+	Required	+	Required	+	Required	+
+(signaling)	+		+		+		+
	+		+		+		+

+Padding mux	+ Not required	+ Required	+ Not req	+
+header	+	+	+	+
+	+	+	+	+
+Multiplex timer	+ Proposed	+ Not proposed	+ Not prop	+
+	+	+	+	+
+Dynamic capability	+ Possible	+ Not possible	+ Not poss	+
+ exchange	+	+	+	+
+++++				

Table 4. Comparison of different approaches on user multiplexing in RTP payload

10 Conclusion

A new method to multiplex speech samples from a number of users in a RTP payload is proposed. It is shown that this method reduces the overhead for small packets, improves the bandwidth efficiency, lowers the chances for congestion at intermediate IP routers and enhances the scalability of the gateways. A new control signaling procedure to negotiate a channel between peer gateways is also proposed. The advantages of this method justify the need for such a mechanism between gateways that interconnect PSTN and GSM users.

11 Full Copyright Statement

Copyright (C) The Internet Society (1998). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works.

However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

12 Authors' Addresses

Barani Subbiah, Senthil Sengodan
Nokia Research Center
3 Burlington Woods Dr., Ste. 260
Burlington, MA - 01803, USA

baranitharan.subbiah@research.nokia.com
senthil.sengodan@research.nokia.com

13 Bibliography

- [1] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, RTP: a transport protocol for real-time applications, Request for Comments(Proposed Standard) 1889, Internet Engineering Task Force, Jan. 1996.
- [2] International Telecommunication Union, Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction, Recommendation G.729, Telecommunication Standardization Sector of ITU, Geneva, Switzerland, Mar. 1996.
- [3] H. Schulzrinne, RTP profile for audio and video conferences with minimal control, Request for Comments (Proposed Standard) [1890](#), Internet Engineering Task Force, Jan. 1996.
- [4] ITU-T Recommendation G.723.1 (1995) "Dual Rate Speech Coder For Multimedia Communications Transmitting At 5.3 And 6.3 kbit/s"
- [5] ITU-T Recommendation H.225.0 (1998): " Media Stream Packetization and Synchronization for Visual Telephone Systems on Non-Guaranteed Quality of Service LANs ".
- [6] ITU-T Recommendation H.245 (1998): "Control of communications between Visual Telephone Systems and Terminal Equipment". ITU-T Recommendation H.246 (1998) "Interworking of H.series multimedia terminals"
- [7] ITU-T Recommendation H.323 (May, 1996): Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non-Guaranteed Quality of Service.
- [8] ITU-T Recommendation H.323 (January, 1998): Packet Based Multimedia Communications Systems
- [9] J. Rosenberg and H. Schulzrinne: An RTP payload format for user multiplexing, IETF draft, work in progress, May 1998.
- [10] K. Tanigawa, T. Hoshi and K. Tsukada: A RTP simple multiplexing transfer method for Internet telephony gateway, IETF draft, work in progress, June 1998
- [11] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg: SIP: Session Initiation Protocol, IETF draft, work in progress, July 1998.

