Control over VoIP traffic from IP endpoints

Azfar Aslam

Systems & Standards Engineer, Converged Networks Solution, Lucent Technologies, Eng-D RE UCL

Abstract: This paper discusses an issue of control over Voice over IP (VoIP) traffic originating from IP endpoints like dial-up customers, and private IP networks. This issue is of major concern to the telephony service providers migrating from the circuit switched technology to packet based IP technology, as they would like to control the voice traffic in their networks for several reasons including accounting and Quality of Service. This paper proposes a versatile solution, based on the RTP gateway concept developed by the Advanced Technologies division of Bell-labs [1,3].

1 – Introduction.

As the telephony service providers evolve their networks from the traditional circuit switched technology towards the packet based IP technology, they would like to maintain a level of control over the IP networks just as they do with the traditional TDM networks: The level of control which allows a service provider to admit or reject calls based on several parameters. These parameters include, and are not restricted to: Network congestion, call priority, bill payment, network integrity etc. The Current trends show that the initial transition from the circuit switched to packet switched telephony is based on the 'transit' solution, i.e. two PSTN segments connected via an IP backbone. This enables a telephony service provider a smooth transition, whilst allowing it to exploit its investment in the legacy systems. In this phased approach, call admission into the IP network takes place at the media gateways, which are controlled by SoftSwitches. It is therefore possible to control the VoIP traffic volume entering the IP network based on the information from the media gateways and SoftSwitches. This information could be critical in network planning and performance, including the QoS.

It is however not always practical to control the VoIP traffic entering an IP network originating from an IP endpoint, such as a 'dial-up' PC user or from a corporate LAN, due to the reasons explained in section 2. The resulting 'rogue' VoIP traffic however has an impact on the network resource usage, is not regulated, and can have a severe impact on the QoS. It may, therefore, be desirable to control this traffic to:

- Control the amount of traffic flowing in the network.
- Allow only registered users to make calls (essence of this paper).
- Charge for it – generate extra revenue.

The last point may however not be possible to impose on the IP customers until the Internet is regulated. This may actually prove to be a catch 22. The service providers may not be able to charge VoIP endpoints (as defined in the context of this paper), until the regulations allow them; and the regulators may not be allow it to happen until the service providers can demonstrate that they have a significant level of control on the VoIP traffic flowing through their networks, and can provide a QoS. **"You cannot regulate anything you cannot control."**

2 - The problem Statement.

The question then arises that how can a service provider control VoIP traffic originating from the IP endpoints**. It is a two-fold problem because there are two levels of control required in IP communications**: Call/Bearer Control and Media flow control – a shift from traditional telephony paradigm. To understand this, an analogy to a local Exchange (LE) functionality can be made, where the LE authenticates/authorises a subscriber and allows it access to network. The Call Control (CC) is tightly coupled with the bearer and there cannot be a bearer access /media flow until the call control authenticates it. The tight coupling implies the relationship between call control (signaling) and a physical line, Channel, Time Slot or circuit. Once authenticated, the call signaling takes place in the network for the requested service, and the resources are provided accordingly. In the case of VoIP on IP networks, the concept of tight coupling between the CC and bearer is no more. The concept of association between **call control and physical channel** is replaced by logical association between one communicating node to another – Connectionless communications!

The call control signaling may take place on one TCP logical channel, the bearer signaling may take place on another logical channel, whilst the media flow takes place on a separate logical channel.
In the VoIP solutions so far, such as H.323 and SIP, the control over communication at an endpoint is limited to the control over Call Control signaling with the aid of Gatekeeper and Proxy functionality. I.e. a VoIP client software is configured such that it must register with a gatekeeper/proxy server, and authenticate itself to gain

access to a service. This allows a service provider/network administrator to control the VoIP communications on its network. This may be necessary for resource provisioning and billing purposes. So far, the Gatekeeper and proxy server play a similar role as a LE.
Note: so far, the discussion is based on VoIP endpoints, and does not include VoIP traffic flowing between media gateways, under the control of gatekeeper/proxy-server/SoftSwitch.

2.1 – Present solutions

The above model of control begins to breakdown when a user uses a non registered VoIP client for VoIP communications. It doesn't have to register and authorise itself from a gatekeeper/proxy to make VoIP calls. It will however require to be authenticated if it makes a call from IP network to PSTN via a media gateway, which is under the control of a gatekeeper/SoftSwitch. But for any other VoIP communications on IP network, including the Internet, it does not need any authentication. To counter this situation, Call Control level firewalls have been introduced which analyse all the packet flowing through an interface in the network and detect the Call Control traffic. The role of these firewalls is described in section 3. These firewalls have only been implemented for H.323 on commercial scale so far, and not for SIP. These firewall enable a service provider/network administrator to block the unauthorised VoIP communications, but only at a Call Control level. This solution could mean deployment of both the H.323 and SIP firewalls in IP networks, but it would still fail if the VoIP client software employs a non standardised protocol for call control signaling.
As it can be seen from the above discussion, efforts have been made only to control the VoIP traffic from a VoIP endpoint at call control level to large extent. No direct efforts have been made to control the VoIP traffic at media level. And to demonstrate full control over VoIP traffic, a service provider/network operator needs to be able to control it at media level, as well as Call Control level.
This paper addresses the issue of lack of control at media level.

3 – The Proposed Solution.

As mentioned earlier, the VoIP traffic consists of three logical components: Call Control, Bearer Control, and Media flow itself on the transport (IP) network. The call and bearer control signalling usually takes place on TCP, whereas, the media flow takes place on RTP/UDP. It is this differing nature of the application and transport protocols which can be used to provide VoIP traffic control in conjunction with Firewalls and Routers in an IP network.
Firewalls are policy enforcement mechanisms that allow certain type of IP traffic to go through a network segment, whilst blocking other types of traffic. Taking the example of a corporate IP network, firewalls are deployed to block UDP traffic entering a network, due to several reasons including network security and integrity, which is outside the scope of this paper. The firewalls can coexist with routers or as separate entities located adjacent to a router, inside the network boundaries.

Extending the above example of the corporate network, a firewall/Router would typically be configured such that the two way VoIP call Control signalling (using SIP, H.323) transported over TCP would be allowed to traverse through it, whereas, the UDP (voice stream) would only be allowed to go out of the network, but not enter the network, i.e. one way communications, as shown in the fig 1.
The solution proposed here extends this fundamental ability of a firewall/Router to block certain type of traffic to control VoIP traffic in a network.

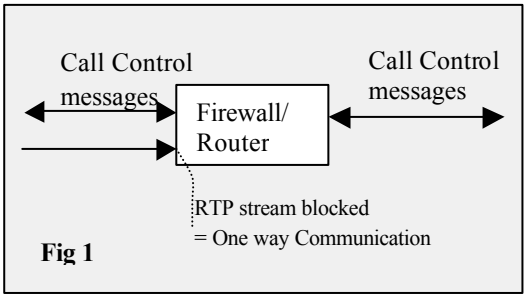

Fig 1

The routers in the IP networks have 'Access Control Lists' (ACLs), which is a list of policies a router enforces on its interfaces to the network. For example, a router can be configured such that it can block the RTP or UDP or both types of traffic. The ACL control allows a network administrator to control Application level protocol, such as RTP; or transport level protocol, such as TCP to be blocked or allowed through an interface. This control can further be enhanced based on several other parameters including originating and terminating IP addresses. It maybe useful to note here that not all the routers can support stateful firewalls, which can block the application level protocols/traffic, such as RTP. Some Routers/firewalls can only block transport level protocols/traffic, such as UDP.
Ideally, a service provider would like to be able to dynamically control the RTP (VoIP) traffic flowing at a node (router), via some call control communications with a router, on a per call basis (like a telephone switch) – but in practice, it is not possible due to the limitations of present day routers. Therefore, we propose the next best solution: an RTP gateway. This solution works with any call control protocol (SIP, H.323, BICC), and solves some of the other issues related to VoIP.

4 - RTP Gateway

An RTP gateway is an addressable device which can be controlled by a SoftSwitch via the **Megaco protocol**. It sits adjacent or parallel to a firewall, working as a proxy for RTP media streams. The firewall is configured such that it allows the RTP traffic originating or destined for the RTP gateway, while blocking all other incoming and outgoing RTP streams. This enables the call control signaling to take place between the end user and the SoftSwitch, allowing for registration, call authentication and call set-up etc. When the call is admitted, the SoftSwitch informs the end user to send its media to the RTP gateway. Because this RTP stream is destined for the RTP gateway, the routers/firewalls allow it to traverse through the network. This creates the first leg of the call. The SoftSwitch then requests the RTP gateway to create the second leg of the call to the terminating address (note: the terminating address may not be same as called address), and requests the RTP GW to connect the two call legs together. This mechanism will ensure that VoIP calls that are authenticated only by the SoftSwitch will be allowed onto the network, all other calls will be blocked, as only the SoftSwitch will control the creation and deletion of call legs. This also means that no user will be able to use just any VoIP client software to make free calls on the IP network, without registering with the service provider.

Consider the following exa mple which provides a simplistic view of the above mechanism. For simplicity, SIP protocol has been used for call control signaling, however, any other call control protocol would be valid. See fig 2. This example shows a call originating from a SIP user agent 'A' destined for user agent 'B'. The call control signalling takes place via the SoftSwitches, whereas, the media flows through a RTP gateway.

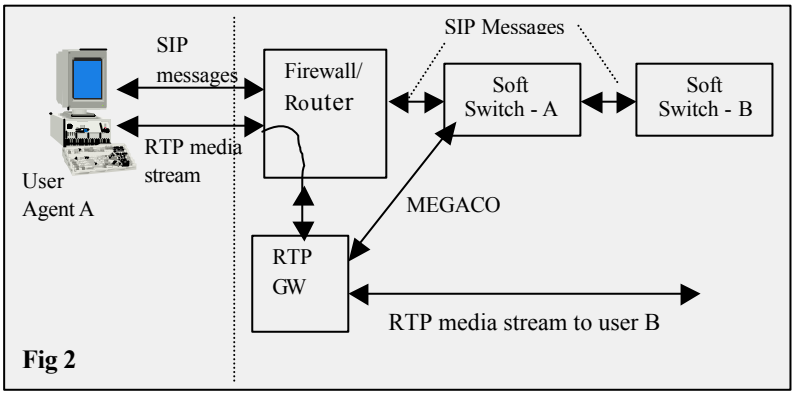

Fig 2

1. User Agent A sends INVITE message to User Agent B, via its home SoftSwitch-A (SS-A). SS-A analyses the call request, authenticates and finds route to SS-B.
2. Before sending the call request to SoftSwitch-B, SS-A requests the RTP gateway, via Megaco, to create two terminations (call legs): T1, T2. T1 termination to send and receive media from user A; T2 termination to send and receive media from user B.
   The '**RecvOnly'** information for user A is available from its SDP, leading to a '**SendOnly'** mode set up at the RTP GW. The transport descriptor (IP address and port number) for user B is not available at this time, so a '**RecvOnly'** mode is created at the RTP GW.This allows for early media flow from user B to user A.
3. RTP gateway then replies to SS-A that the reservation has been successful.
4. SS-A sends the INVITE message to the relevant SoftSwitch, SS-B. SS-A replaces the original '**RecvOnly**' SDP transport descriptor of user A, with the '**RecvOnly'** transport descriptor of RTP GW.
5. SS-B sends a 180 Ringing response back to SS-A. it is assumed here that the SDP transport descriptor of user B is sent with the 180 response – This may however arrive with 200 OK response.

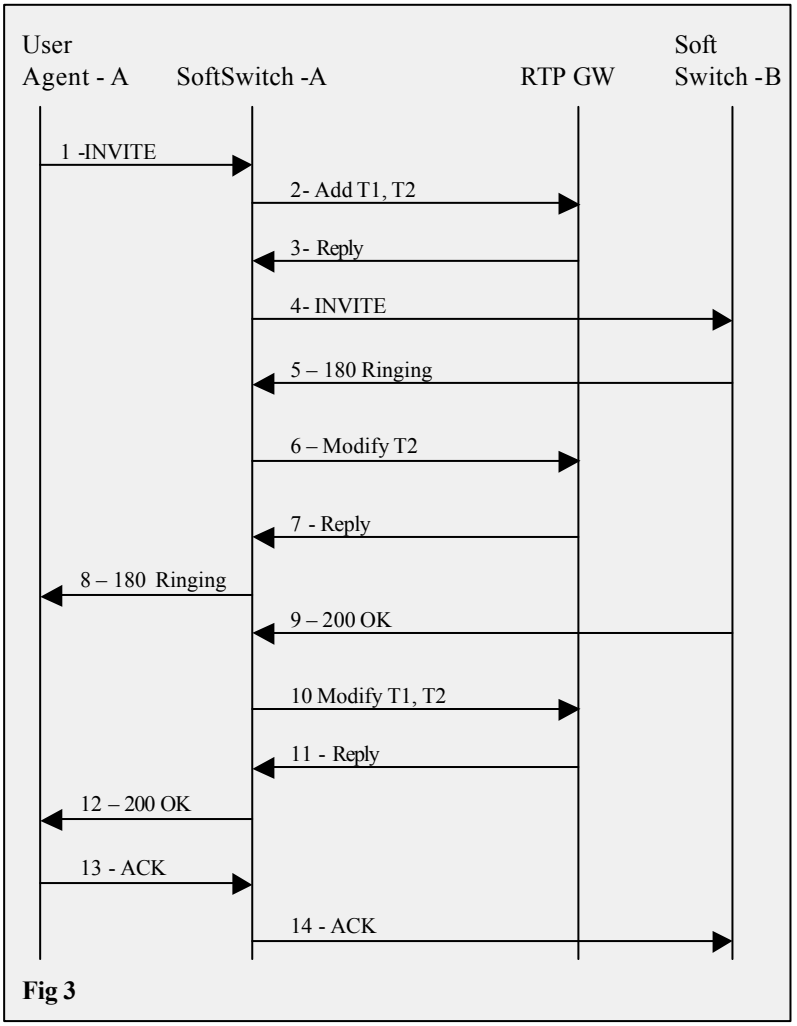

Fig 3

6. SS-A requests RTP GW to modify the T2 termination by providing it with user B's transport descriptor ('**RecvOnly'**). This enable a '**SendOnly'** mode setup towards the user B.
7. RTP gateway makes the required modifications, and informs the SS-A of the successful modification.
8. The SS-A modifies the SDP transport descriptor it received from user B, by replacing user B's '**RecvOnly'** transport descriptor with the RTP GW's '**RecvOnly'** transport decriptor. It then sends the 180 Ringing response to user A, with the modified SDP message.
9. User B sends 200 OK, Call Successful, response.
10. SS-A informs RTP GW to update the '**SendOnly'** and '**RecvOnly'** modes with '**SendRecv'** modes, to allow for a bidirectional media stream.
11. RTP GW replies to SS-A with 'successful' update response.
12. A 200 OK success message is sent to the user A.
13. User A sends an ACK message to SS-A.
14. SS-A sends an ACK message to SS-B.

It is worth mentioning here that for simplicity sake, the RTP GW with SS-B is not shown.

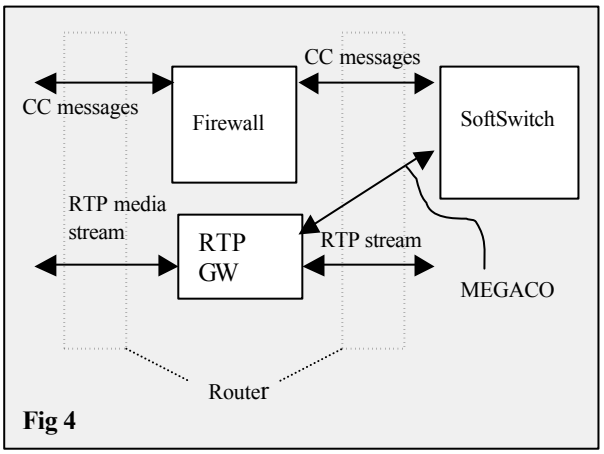

Fig 4

5 – Other advantages of the RTP GW solution

5.1 - Interconnect functionality/Call handover.

An RTP GW could also act as an Interconnect gateway to another Network/Service provider domain, to hand over calls with certain QoS features from one network to another. More on the interconnect funtionality can be found in [2].

5.2 - Physical location

The RTP gateways can be located anywhere in the network, with the exception of cases where statefull firewalls are not availble in a network segment, i.e. a firewall can only block the UDP traffic. In such scenario, the RTP GW would be located parallel to the firewall, and RTP/UDP traffic would be bypassed from the firewall, as shown in fig 3.

5.3 - n to n support.

One RTP gateway could serve several IP endpoints, and provide service to more than one SoftSwitches – a feature most useful for load distribution purposes. In practice however, a service provider may chose to dedicate a RTP GW to one SoftSwitch.

5.4 - QoS support

As the loading increases on the RTP gateways, the softswitch could decide to either drop the calls, or use another RTP gateway in the network. This is one of the major advantages of not restricting the location of RTP GWs.
This solution is not restricted to voice calls only, but also supports other multimedia capabilities too.
This mechanism supports some other QoS enabling mechanisms in IP networks, which are outside the scope of this paper.

5.5 - Security

As the communication through the RTP GW can only be allowed by the sofswitch, and provided a security mechanism is available between RTP GW and SoftSwitch, this should not compromise the IP network security. Therefore, the network administrator should not be concerned about bypassing the RTP/UDP traffic from the firewall, provided there is a secure communications mechanism in place between SoftSwitches and RTP gateways.

6 - Conclusion

This paper presents a scalable solution to gain control over the VoIP traffic flowing through an IP network. It is a scalable solution which can be extended beyond a network domain.

7 – References

[1] http://voip.nl.lucent.com/~sijben/review/draft-sijben-rtp-gateway-00v7.doc). (internal)
[2] ET DTS 5003 – TIPHON QoS architecture (ETSI online account required)
[3] http://www.ietf.org/internet-drafts/draft-ietf-midcom-requirements-02.txt