Introduction
IPTV service providers not only should find new customers for their services but also they need to keep them as customers in the long term. For this goal they have been looking for ways to identify impairments to the perceived quality of experience. Today this is known that the only way to achieve this, is to have a virtual “eye on the network” to check what is going on inside the network. However current network infrastructure doesn’t satisfy service providers. They usually don’t know about the user’s connection type (wireless, wired, power-line...) and user’s connection quality (lossy, noisy, poor wiring...). Totally there is not deep visibility to home network and finding origin of impairment is challenging.

MPEG2-TS: RTP vs plain UDP
MPEG2-TS format is the normal choice for media transport over network. However TS is an application layer protocol and we should decide how to transmit multimedia content over transport layer. TS is not originally designed for IP networks. In below layer, UPD is also has some deficiencies for this purpose, including lack of feedback. For solving this problem, another application layer protocol is added in between. RTP protocol is specially designed to come up with this weakness by providing an extra application level framing. First, TS packet is encapsulated by RTP packet and after that is delivered to UDP protocol. This strategy combines benefits of low overhead UDP and needs of multimedia and has superior performance over plain UDP. RTP works hand in hand with RTCP. RTP carries multimedia content and RTCP provides feedback on the quality of service.
**IPTV Delivery Architecture and RTP/RTCP**

The proposed architecture for improving QoE over IPTV is depicted in this picture. FT (feedback target) are inserted in middle of network. Like original RTP/RTCP protocol, RTP multicast connection is used for transmitting media content from DS (distribution source) to receivers (red lines). Moreover unicast RTCP connections are used for returning feedbacks (blue lines). Feedback reports include information like fraction of packet lost, jitter or information for allowing senders to calculate RTT. But in new idea, RTCP connections are made between receivers and FTs (like R71 & FT3) or between FTs (like FT1 & FT2) or between FTs and DS (like F1 & DS).

**IPTV & RTCP**

As mentioned, IPTVs have their own needs. In IPTVs, sometimes it is desirable to have more frequent RTCP packets (early report). Here three useful use-cases for having more RTCP reports are mentioned. These three have support form architecture in Fig.2.

1. Retransmission: send a NAC for retransmitting lost RTP packet.
2. Rapid acquisition of multicast sessions: rapid channel change.
3. Codec control: receivers ask to change codecs settings, change bitrate, etc.

**IPTV: Feedback Targets**

FTs suggest these functionalities:

- **Eye over network:** An FT itself can join a multicast session and provides its own feedback. By means of FTs, service provider has an “eye over network”. FTs can be considered as a measurement probe to monitor test points inside the network.
- **Feedback aggregation:** FTs can collect reports from downstream network, aggregate them and send a concise report to upstream network. This provides scalability of RTCP frequency rate. Depending on condition, different parts of network can have their own RTCP report rate.
- **Rapid acquisition:** Buffering recent media content (like last 5 seconds of TV channels) in FTs and use them to quickly react to user’s request to change the channel. Joining to new multicast session is ongoing in background while user watches that 5 seconds.
• Fault tolerance: Buffering recent media content (like last 5 seconds of TV channels) in FTs and use them to retransmit the lost packets locally.

• Fault isolation: Locating fault position in local network. Parts of network that generate more fault reports, are more likely to be faulty. Path segments can be monitored too by FTs at different distance (like F1 & F2 in Fig.2). Home networks also can be monitored by FTs, but there are some privacy issues. Customers don’t like to let strangers know about their private network configuration.

• Automation in fault detection: no need to find the source of problems manually (by repair staff).

References
