Adaptive Bitrate Streaming

Monitoring and Quality Control

Monitoring and quality control of Adaptive Bitrate Streaming platforms is as important as the ABR systems themselves, according to test, measurement and monitoring solutions specialist Tektronix.

Content Providers, Broadcasters and Operators are all seeking to provide multiscreen video or TV Everywhere, as it is also sometimes called. This is intended to deliver streaming video services to PCs, laptops, smartphones, tablets and TVs.

Streaming to such a wide range of devices is complex. Each type of device has its own unique demands. The data rate an IPenabled television needs to present an acceptable picture is far greater than that necessary for a smartphone. In addition, the networks that some of these devices use can suffer from dynamically changing characteristics.

The underlying technology used with multiscreen video is adaptive bitrate streaming (ABR). This essentially is the segmenting of content into small fragments of compressed content for transmission to viewing devices. This technology is not standardised in the same way that DVB Transport Streams are used in traditional TV applications.

There are several ABR implementations, each having different characteristics:

- Apple's HTTP Live Streaming
- Microsoft's Smooth Streaming
- Adobe's HTTP Dynamic Streaming
- MPEG-DASH

A recent survey identified 'quality of experience/quality of service' as the second most significant technical challenge (after bandwidth limitations) in offering OTT video. "ABR is a simple idea that is both clever but hard to implement," said Paul Robinson, Tektronix's CTO for Video. "There is a lot that can go wrong. You have to check that everything is working as you think it is. The only other way to find out when things are going wrong is to wait for subscribers to tell you, and you don't want to find out that way." Monitoring and Quality Control (QC) of ABR platforms is as important as the ABR systems themselves.

Tektronix

One of the biggest challenges of content streaming is that the networks and devices are far more varied than those found in the more controlled environments of Cable, Satellite, Terrestrial and IPTV. Different network conditions and device requirements make a highly adaptable architecture necessary.

ABR addresses this issue dividing the stream into discrete fragments of fixed time duration. These are referred to as fragments, segments or chunks. A variety of bitrates for the fragments is established commonly referred to as profiles. The device displaying the content has the intelligence to request the appropriate profile that best suits network conditions at any particular point in time. The optimal profile can change each time a fragment is requested. Any ABR system works by checking the playout devices buffer to see how full it is. If it is becoming full, the device requests a lower bitrate profile. As the buffer empties the device requests a higher bitrate profile. In theory this ensures that constant playout is maintained without the 'buffering' issues experienced with traditional progressive streaming systems.

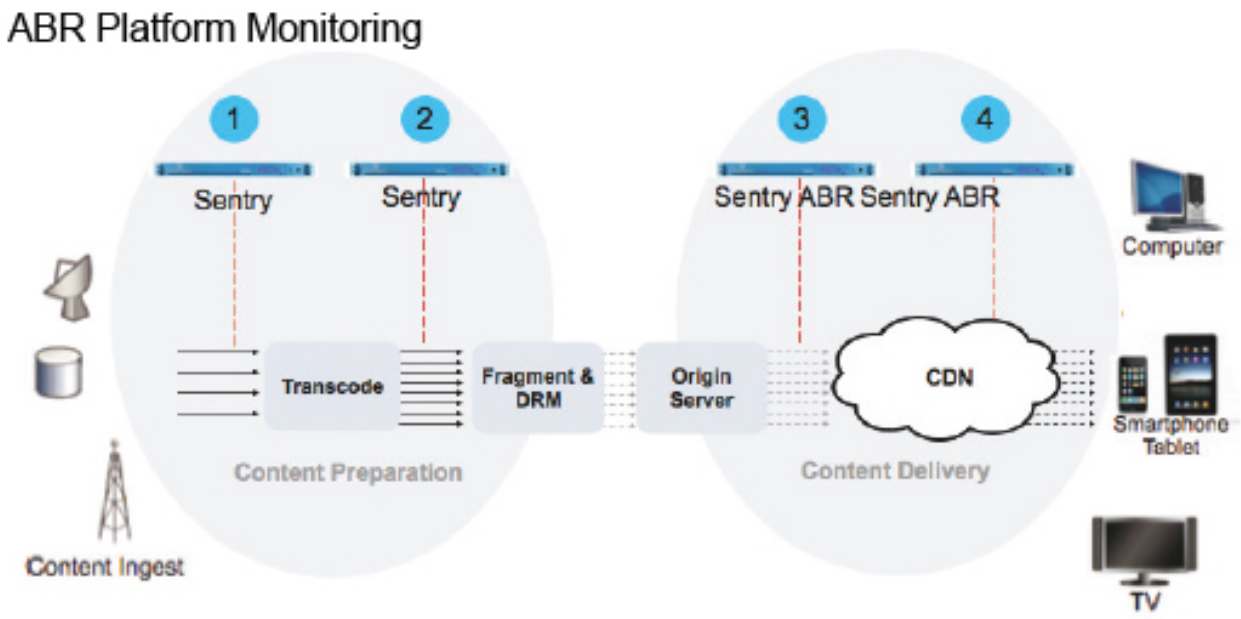
Ensuring subscriber satisfaction with such a complex architecture requires monitoring QoE and QoS at multiple points in the network to ensure that the content is of appropriate quality and that the delivery network is actually capable of delivering the content.

QoE and QoS

There are two linked ways of ensuring subscriber satisfaction, Quality of Experience (QoE) and Quality of Service (QoS). They may have similar sounding names, but they are significantly different.

QoE is a relatively new area for operators. In the past, operators focused on measuring attributes related to the precision of the IP packet transport and the MPEG Transport Stream. For example, at the IP level, these QoS measures focused on delayed, out of order, and lost packets. Recent technology advances have allowed operators to use deep packet inspection to look for deeper content related problems. These QoE measures come far closer to identifying the actual experience viewers will have when they see and hear the video and audio.

The overall monitoring of ABR streams are performed at four points using a two-step process. The first step relates to content preparation and is performed at the QoE level. Monitoring is performed before and after transcoding, but before fragmentation and the addition of digital rights management (DRM). The second step relates to content delivery and is a network level QoS function that ensures content can be delivered correctly. Monitoring is implemented after the origin servers and CDN caching/streaming servers.



Content Preparation

The first important point in the monitoring and Quality Control (QC) of ABR platforms is that the ingested content must be error free when received by the operator. If there are flaws in the ingested video and audio, it is inevitable that the final service will not be acceptable.

Transport Streams that arrive at the operator's ABR head-end from its own encoders or from other broadcasters and content providers are monitored for QoE issues such as macroblocking, compression artefacts, audio silence, levels and loudness. (Point 1 in the graphic). The ingested content is then transcoded into each of the ABR profiles (the same content at various bitrates) that the operator supports. The content quality of each profile is then verified after transcode. (Point 2 in the graphic).

ABR platforms have much in common because typically they are deployed using the H.264 compression standard and as a result it is common to use the same transcoded content with each of the operator's ABR delivery platform.

Content Delivery

After transcode, each stream is fragmented into fixed time duration fragments, the content is encrypted

and Digital Rights Management (DRM) is applied. The content is now ready for delivery to subscribers using a playout device known as an Origin Server. The encryption that is a key element of DRM makes it impossible for the same level of deep packet inspection to be performed and QoE monitoring is impossible at this point. It can also be argued that as the content has already been verified prior to fragmentation and encryption, this makes checking it after that process pointless. If the content is acceptable when it is encrypted, it is impossible for it not to be in precisely the same state when it is decrypted by the subscriber's device.

After encryption, operators use QoS measures to ensure the correct content delivery of capability of the Origin Servers and CDN caching/streaming servers. This is performed at two points: After streams leave the origin server (Point 3 in the graphic) and when they leave content and caching servers, which is the last step before delivery to end users' devices (Point 4 in the graphic).

At these monitoring points, the focus turns to QoS metrics such as manifest verification, fragment load time and latency as well as ensuring that the various profile bitrates for each service are as expected. This is performed by active devices that emulate requests made by end users in order to subscribe to all services at all profiles.

ABR requires precise and exhaustive tracking of the huge number of packets that make up the various services. "When the device requests a chunk at a specific bit rate the system needs to check the manifest file and make sure that it's actually the right bit rate that is being sent," Robinson said. "If it requests a fragment at 500 kilobits per second and for whatever reason it incorrectly sends video 1 megabit at per second, the service will fail."

QoS indeed is vital to the success of ABR Streaming which uses HTTP to request each fragment in the same way that a web page is requested. This is a unicast approach in which only the stream requested is sent. This puts pressure on the system to deliver data in a precise fashion and, consequently, puts more pressure on video and audio monitoring and service assurance techniques. ABR is so complex that a very rigid and structured monitoring regime must be in place to ensure that the system is functioning correctly.

Adaptive Bitrate Streaming

Monitoring and Quality Control

In Summary

With ABR streaming services, it is important to monitor both video and audio QoE both at ingest and posttranscode for all available profiles. After fragmenting and encryption, it is important to monitor the QoS of the content delivery platform to ensure that the system delivers what the client-side player is expecting to receive. In addition, for systems offering on-demand services, it is important to verify the decodability of these assets prior to being made available for transmission. If operators perform all these steps, they will be best placed to deliver the highest possible quality video and audio programming over a robust and reliable service delivery platform.

Sentry	Sentry ABR	Cerify
Identifies QoS anomalies in the network at the IP and MPEG TS layers as well as in Quality of Experience (QoE), identifying issues that represent the bulk of trouble calls from subscribers including frozen video, tiling/macroblocking and audio disruptions or audio-level and loudness issues. In addition, Sentry includes a video artefact measurement and detection capability which enables Sentry to detect compression issues in programming while generating metrics represented as a Mean Opinion Score (MOS). Within the ABR network, Sentry is used from ingest all the way through the critical transcode process to perform comprehensive QoE analysis and artefact detection on each stream at each bitrate in real time.	Is a post-origin server monitoring device that focuses on QoS. Sentry ABR is an “active” monitoring product that proactively monitors ABR content on origin servers or CDN caching/streaming servers. It does this by actively requesting and validating program playlists / manifests that it has been configured to monitor. It then requests from the server, in turn, all of the fragments of each profile / representation for each program – calculating availability and performance metrics and generating alerts in real time.	Is the file-based on demand asset product analogous to Sentry. Cerify is a quality control software tool that does two things: First, it checks that the file has the expected video and audio content, that it is decodable and can be transcoded, and that the overall length is correct and that the video quality meets operator requirements.

12/2013 28WI-29956-0

Tektronix