Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 13, Issue 8

Managing Customer Quality of Experience (QoE) with Active Assurance for IP Video

By: Wesley Hicks

Service providers are seeing an explosion in the growth of IP based video services in their networks. Driven by increasing demand for online content sources such as YouTube, HBO GO or the NFL Network and by the emergence of 4K HD content, their networks have seen a 3-fold growth in IP based video traffic from 2014 to 2019. According to Cisco's Virtual Networking Index, IP video, which consists of both IPTV services offered by the communications service provider (CSP) and over-the-top (OTT) video offered by third party content providers, is now projected to make up as much as 84 percent of all consumer IP traffic by 2019 with OTT expected to be around 83 percent of that number.

With video services becoming an essential part of the CSP offering, and given the increasingly competitive market for service providers of all kinds, the question becomes how do these providers ensure a high quality of experience (QoE) for multiple IP video delivery methods, delivered across their network to retain and growth their customer base?

What is over-the-top video

By now, everybody has experienced video delivered over the internet. Whether it was a YouTube video clip, a TV show streamed on-demand from one of the major networks' website or a movie from Netflix, video delivered over the internet and streamed to your smart TV, computer, or mobile device, has become an essential part of the service bundle. But how is OTT video different from the more traditional Internet Protocol TV (IPTV) service offered by service providers?

Traditional IPTV is a carefully planned and engineered service where the video distribution network is built specifically to address transport issues such as capacity, latency and jitter, and scaled to meet the anticipated demand. The service is broadly distributed throughout the providers' network and uses traditional Internet Group Management Protocol (IGMP) techniques to allow customers access to their subscribed channel lineup. Since the network is multicast and engineered for quality of service (QoS) and, since this video is a live streamed service, it is acceptable to rely on UDP-based transport services. Packets lost or corrupted during transport are simply discarded. By carefully engineering the network, packet loss can be minimized; however, network issues such as equipment failures, maintenance activities, software upgrades, or in the case of hybrid or virtual networks, dynamic optimization of VNF instances and traffic routing, will always exist and can all lead to service quality issues.

OTT video, on the other hand, does not use a purpose-built network; rather, it leverages the public internet to deliver the video content. The service relies on internet protocols to deliver video in much the same way as other web based content. OTT video is delivered 'on demand' as a unicast service using TCP based transport which means it is subject to re-transmission of lost or corrupted packets. To avoid impacting the video service in the event of packet loss and re transmission, OTT video is delivered as a segmented file so that content is delivered to the users' device in advance of the viewing – commonly referred to as buffering. In this way, any lost or corrupted packets can be re-transmitted before they are required, ensuring a smooth video service.

The other interesting challenge that OTT brings to the CSP is that, unlike a traditional IPTV service

that is offered by the CSP and engineered for QoS, OTT is typically offered by third-party content providers and distributed through content distribution networks (CDN) and across the CSP network. Not only does the third-party provider represent a loss of potential revenue to the CSP, but if the OTT service is not performing well, it is often the CSP that gets blamed for it, damaging their brand reputation even though the issue may very well not have been in their network.

Delivering OTT Video

As mentioned, OTT video relies heavily on content distribution networks (CDN), such as Akamai or Amazon, to position high value or popular content closer to the end users. Leveraging CDNs allows the content provider to ensure a better quality of service by shortening the delivery path, hence minimizing any latency related to transport, and by distributing the file sharing load across multiple servers, reducing any impact from high user demand.As well, OTT video distribution leverages adaptive bit rate (ABR) encoding of the segmented video files so that the service can tradeoff network performance and video quality to maximize the users experience. If network issues are such that the segmented files cannot be downloaded fast enough to keep the video operating smoothly, then a lower bitrate version of the files is requested allowing the video playout to continue smoothly, albeit at a lower quality resolution.

Monitoring the video service

Video services, much like voice services, are dependent on a low latency, error free connection to ensure a high quality of service. Being able to continuously monitor the quality of a video signal being received by a customer is critical to maintaining a good quality of experience. Failure to do so will likely result in the loss of both customers and revenue.

There are several ways of monitoring the quality of a video service, depending on the type of video being used. Traditional broadcast video, the kind you might get from a satellite TV provider or over-the-air transmission, rely on passive monitoring only. For these methods, it is sufficient to have a test set with an appropriate receiver which can then analyze the received signal for such things as signal strength, encoding errors, and missing channels. Since these traditional methods broadcast "all channels, all the time", there is no need for the test set to request content. Key performance indicators (KPI) for the received broadcast signals can be generated and sent to a video operations center to allow the provider to see how the service is behaving and take appropriate action if warranted.

IP video services, on the other hand, are not broadcast services. They rely on signaling from the receiver to request specific content. Additionally, because the distribution is packet based, IP video is susceptible to a variety of other service quality and network issues; therefore, in addition to assuring the video and audio content of the received signal, IP video services, including IPTV and OTT video, need to employ active monitoring to request specific content from the application server and verify the receipt of that content before it can analyze the quality of the video received.

Additionally, because IP video relies on internet protocols for streaming live traffic, in the case of IPTV, or delivering video file segments, in the case of OTT, any testing strategy also needs to account for the content encoding as well as the decoding. OTT video further complicates this because of its reliance on ABR encoding, video file segmenting and the use of CDNs for distribution. To address all these IP video issues, the CSP needs a comprehensive active video assurance strategy to ensure complete visibility of the service, whatever video technology is being used.

Best practices in IP Video distribution and monitoring dictate that testing of video services should be done wherever the content is encoded, received, stored and watched. Doing this not only ensures the delivered video product is of good quality, but if there is an issue, isolating the location and cause is much quicker and the service network can be modified to bypass issues.

In the case of OTT video, monitoring should also take place at the video origin server, where the content is encoded and segmented, as well as at various points along the distribution path,

including at the hand-off to the CDN, the hand-off to the local CSP, the hand-off to access network, and the hand-off to the customer.

Similarly, IPTV video services need video and audio assurance at the point of content origination and should also include delivery assurance at all key network interface points to fully monitor the delivery of quality services to the customer.

To ensure a complete and robust monitoring solution, the family of video assurance equipment used should be able to support not only all the variations of video distribution technology, but should also provide a common surveillance platform to manage the entire video assurance strategy and provide the CSP with a unified view of the health of their video service, regardless of technology.