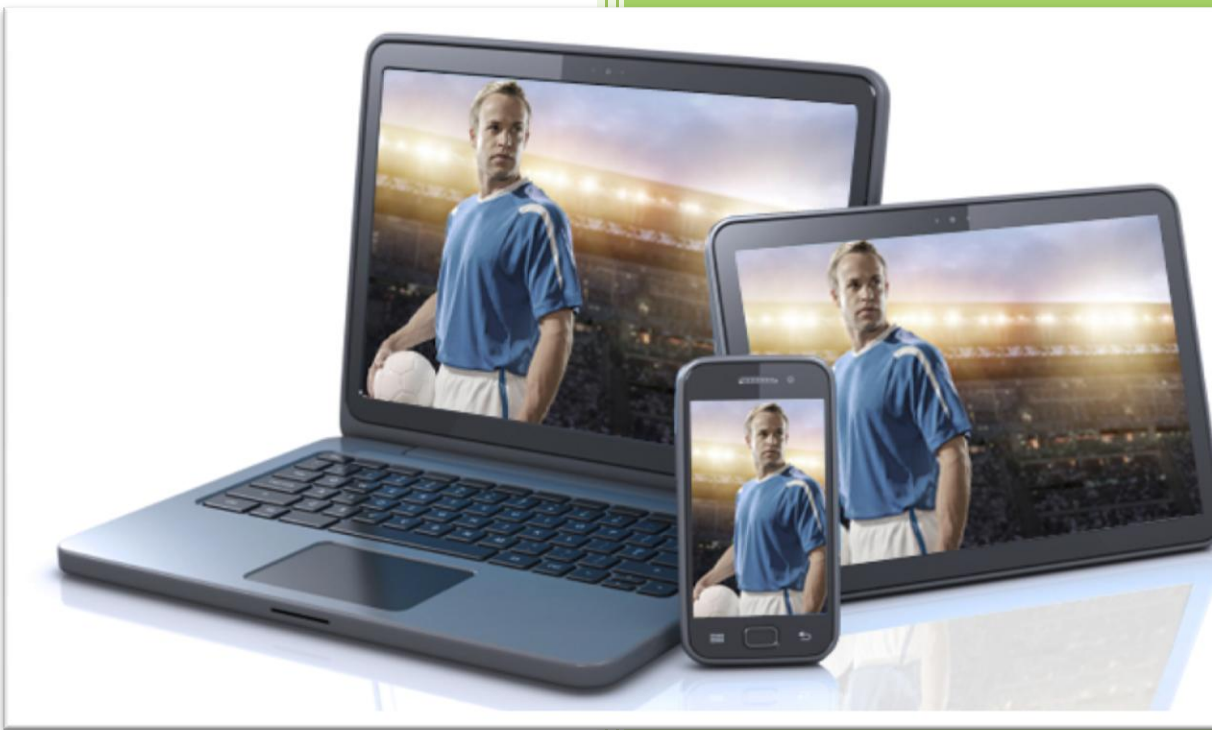
VideoFlow
seeing is believing

Broadcast Quality Video over the Public Internet



By Adi Rozenberg, CTO

Table of Contents

Chapter 1. Introduction

Now that transmitting video content over IP is growing in numbers and maturity, broadcasters, network operators and content distributors are leveraging the benefits and cost saving of the IP era. Accessibility to IP networks is fast and easy. Add new services or additional deployments immediately with short notice. Long acknowledged as the lowest cost transport network for video streaming to the home, the public Internet has enabled services like YouTube, Flicker and many others to offer video streaming directly to the home viewer. However, using the Internet to stream broadcast quality video 24/7 poses an immense challenge. Riddled with inherent complexities such as packet loss, jitter fluctuation and general statistical behavior, the public Internet makes multicast streaming a serious challenge. Viewers have high expectations. They demand the highest level of quality 24/7; therefore, any operator that streams video over the public Internet must understand the challenges and to act upon them to provide the best SLA and QoE.

The original purpose and design of IP networks was to handle data transfer where the criterion for success is complete delivery and not necessarily timely delivery. When transmitting data, IP networks can handle uneven deliveries. Even occasional packet drops can be tolerated by data delivery applications because these applications are built to handle late arrivals and protocols exist (e.g. TCP) to resend the missed packets.

Video on the other hand requires that packet delivery be timely and reliable, since video buffers need to be fed consistently. MPEG decoders do not handle missing data well, which leads to problems for those sending the video and for end-users who do not experience the quality they expect. With the increased desire to use the cost-saving Internet, there is an increased awareness of the problems that packet loss and network jitter can cause when using IP networks. The reality is that content distributors cannot ignore the resulting drop in the quality of experience for the viewer any longer.

Since the public Internet has become the new highway for video streaming, initial installations have used offline methods of streaming. They stream the video from local video servers offering services like video on demand (VOD) or over the top (OTT), which uses TCP/IP to overcome the statistical nature of the Internet. However, the TCP protocol is not suitable for high quality 24/7 real time video streaming as any packet loss may result in decreasing the usable video stream's bandwidth, which affects the quality of the stream. Standard video gateways and other equipment, such as decoders, cannot tolerate the variability in packet loss and jitter. A new solution is necessary to overcome these challenges.

Another major hurdle to overcome is the Internet's inability to pass multicast streams because network elements are very likely to block them along their path from source to destination. Generally, multicast video streaming is reserved for the last mile where the path is set to allow it. Most solutions stream only unicast video, converting them to multicast streams only at the distribution points.

The current solution for multicast video stream is to use a Virtual Private Network (VPN), which is normally offered by an Internet Service Provider (ISP). This VPN provides some assurance to uplink bandwidth and in some cases some degree of service level. However, the VPN cannot provide active protection against packet loss as bandwidth and service level are managed by prioritizing packets passing through the VPN.

Chapter 2. The Public Internet Challenge

The statistical nature of the public Internet is the result of changes in traffic profiles during the day, week, and month. This traffic fluctuation may cause temporal congestion, packet loss, packet reordering and large amount of packet jitter.

The public Internet tends to generate occasional jitter and delay variation, which may cause severe delay to the packet arrival time causing the packet to lose its place in the receiver buffer. For video streams, a severely delayed packet is considered lost packet. Most network operators cannot provide assurance against packet loss even if the stream is running over a well-engineered VPN tunnel. This is because the network (or link) is shared with other services or applications, all of whom require different bandwidths from time to time. The ubiquitous solution to reduce the occurrences of this issue is similar to the one for congestion and packet drop. This solution is over-provisioning bandwidth to allow the service to run with “wider” shoulders.

Congestion and packet dropping tend to generate bursts of loss, but the duration can be either very short or very long. For example, congestion and packet drop will occur if traffic exceeds allowable buffer limits. Reducing the probability of congestion and packet drop requires either adding more bandwidth and higher end equipment to allow better performance or reducing the traffic bandwidth to provide sufficient margin for eliminating short-time transients exceeding the allowable buffers limits. These types of solution are expensive to both the network operator and the content distributor, because it involves higher capital expenses for both bandwidth and equipment. In addition, the added bandwidth cannot be used for any other application without raising the risk of increasing packet loss. The typical bandwidth provisioning is 20-30% of the original stream. For example, a distributor would secure 12-13Mbit of bandwidth for a 10Mbit stream.

Re-order errors and packet duplication are less frequent. In this instance, the “lost” or ”duplicated” packet arrives late to the destination and is treated as an out-of-sequence event. The problem may become more severe if it is influenced by network jitter, which may cause the packet to arrive too late for processing/decoding. The common solution to handle this type of event is to use RTP streaming. This is a well-established industry solution supported by most broadcast and network equipment manufacturers. The equipment manufacturers must consider the jitter buffer size. Studies show that network jitter may reach 160-240ms and in some cases, it has reached 500ms on multi-hop connections. Therefore, any solution requires a combination of RTP and deep buffering capabilities to absorb the impact of jitter or delay variation events. The buffer should be able to handle 1000ms drop in traffic and shield the receiver from such drop.

Environmental effects like electrical impulse noise tend to cause uncorrelated short burst errors in the order of 1-20ms. The most common approach to reduce this effect is to increase protection at the physical layer. Normally, this is done indirectly by allowing a large noise margin and other parameters resulting in lower effective throughput on the channel.

Chapter 3. VideoFlow 3V Technology

The VideoFlow innovative DVP product line provides an innovative state-of-the-art solution for streaming over the public Internet. The DVP technology is a Client Server architecture optimized for video streaming over the public Internet. VideoFlow's DVP products provide seamless solution comprised of the following technologies:

- VPN tunnel to stream multicast
- VideoFlow Error Correction (VFEC) for recovering 100% of packet loss
- VideoFlow's Adaptive Buffering (VFAB) compensating for packet jitter

The DVP is capable of creating a VPN tunnel between the Server (Protector) and the Client (Sentinel). The VPN tunnel enables multicast streaming across the public Internet. Since the VPN is created by the DVP, there is no need for additional network equipment or special services offered by the Internet Service Provider (ISP). This reduces both capital expenses and operating expenses. In contrast to other existing VPN solutions, VideoFlow's DVP will protect the quality of the video stream by applying VFEC and VFAB technologies. VideoFlow's VPN can run numerous streams in parallel over the public Internet making it a perfect solution for multicast users. Network equipment will not block video streams passing through the VPN tunnel. The Protector is able to create several VPN tunnels to different Sentinels enabling point to multipoint connections.

VideoFlow's innovative packet recovery technology guarantees 100% protection against packet loss using a robust algorithms suite that is transparent to the original transmitter and receivers, offloading the original sender for better scalability. VideoFlow uses patent-pending, state-of-the-art VideoFlow error correction (VFEC), a unique on-demand packet recovery technique. VideoFlow's patented packet recovery has multiple layers of protection techniques, all designed with a single goal, which is to recover lost packets using minimum bandwidth.

VideoFlow DVP product line offers a built in configurable buffering capacity ranging from 10ms-2000ms for each stream. The Buffer size design handles bursty traffic on one hand and lack of traffic on the other. The DVP can use the buffered video to play out jitter-free video despite high jitter figures, which characterize the public Internet.

In addition, VideoFlow's DVP guarantees reliability by invoking auto-box redundancy. The auto box-redundancy scheme is comprised of two identical sets of Protector and

Sentinel. One set is active while the other remains “hot” in standby mode. If the active set fails, the hot standby kicks in without missing a beat to offer the ultimate content protection.

Furthermore, the DVP uses a standard RTCP channel for bidirectional communication between the server and its clients. This solution protects both unicast and multicast video content against single and bursty packet loss.

VideoFlow’s DVP is the only solution that both delivers and protects multicast video over the public Internet, which is a major advantage for distributors. VideoFlow’s 3V technology enable operators to deploy assured service using less bandwidth to stream video, thereby, reducing the cost of network elements like routers for opening VPNs and eliminating the need to use expense ISP provided premium services like their VPNs.

Chapter 4. The Economy of Quality Video

The key to selecting any solution is a sound business case. While savings vary from deployment to deployment, the potential return on investment can be summarized as follows:

- Reduce Network Costs by using the Internet

  The Internet is being hailed as the next great thing in video streaming. While it does have drawbacks, such as random and unforeseen packet loss, the cost of using the Internet is much lower than other B2B solutions. VideoFlow's DVP enables multicast video streams over the public Internet with VPN, guaranteeing 100% protection against packet loss with VFEC and protection against excessive jitter with VFAB. All three technologies have been optimized to require the lowest possible bandwidth overhead while enabling the highest possible video quality.

- Reduce OPEX and CAPEX

  VideoFlow's DVP product line enables all types of distributors to use the public Internet as a viable transport for broadcast quality video 24/7 at a fraction of the cost of today's solutions. VideoFlow's VPN, VFEC, and VFAB integrated 3V technologies eliminate the need to add redundant network equipment and does not require customers to lease premium services like VPN from their ISP.

Chapter 5. Conclusion

Broadcasters, network operators and content distributors who want to use the public Internet to provide high quality video 24/7 have long faced serious challenges. Now, VideoFlow offers a simple, cost-effective solution that enables them to broadcast quality, jitter-free multicast video streaming over the public Internet. The VideoFlow DVP solution reduces expenses traditionally coupled with multicast streaming by reducing overhead expenses for additional bandwidth, the need for expensive VPN services and the need for high-end network equipment.