Preserving Video Quality in IPTV Networks

Abstract – Growing numbers of service providers are implementing video services over Internet Protocol (IP) networks, and discovering the unique challenges of providing a high quality-of-experience (QoE) to subscribers. Delivering consistent QoE in packet-switched communication networks can be a complex proposition due to the high sensitivity of video traffic to packet loss, as well as to jitter and delay. Preserving video quality in IP Television (IPTV) networks that rely on copper access lines poses an even greater challenge. Service providers need intelligent mechanisms in core and distribution networks to prevent congestion which deteriorates video quality, as well as intelligence between the aggregation network and the user set-top-box (STB) to repair errors, speed up channel change times, and monitor the quality of the subscriber experience. The authors propose a series of core and aggregation layer approaches, collectively referred to as Video Quality of Experience (VQE), to address these issues. The proposed VQE approach encompasses on-path video connection admission control (CAC) employing Resource ReSerVation Protocol (RSVP) in the core and aggregation layers, and a real-time signaling mechanism operating between the provider aggregation edge and the subscriber STB to address bit errors, channel change time, and packet monitoring. This article discusses this VQE approach in detail, and highlights the advantages of extending quality control and monitoring capabilities from the core network to the provider edge.

Index Terms – IPTV, RSVP, Resource Reservation Protocol, DSL line errors, channel change time, IPTV packet monitoring.

Introduction

Consumer consumption of network bandwidth continues to grow exponentially. The Internet Innovation Alliance in Washington, D.C., suggests that, by 2010, the average U.S. household will use 1.1 terabytes of bandwidth each month – meaning that 20 homes will generate more traffic than the entire Internet did in 1995. [1] The most significant factor driving this bandwidth growth is increased transport of video over IP networks.

Growing numbers of service providers are turning to video services as a means to expand revenues and market share. As more service providers roll out video offerings, the ability to meet and exceed customer expectations for video quality will become a critical service differentiator. Delivering high-quality video, however, is a complex proposition; particularly for service providers relying on packet-switched communication networks such as those used in the delivery of IP television (IPTV) services. This is due to the uniquely resource-intensive and packet loss-sensitive nature of video traffic.

Broadcast IPTV video, and especially video-on-demand (VoD) services, mandate high-quality, real-time connections and considerable bandwidth. An IPTV stream requires approximately 2-4 Megabits per second (Mbps) for standard-definition (SD) video using the Motion Picture Experts Group 4 (MPEG-4) compression standard, and 8-12 Mbps for MPEG-4 high-definition (HD) video. To deliver a high-quality user experience, the European Telecommunications Standards Institute’s (ETSI) Digital Video Broadcast (DVB) standard [2] recommends a maximum of one video artifact per one-hour movie, which translates to a packet loss rate of 10^{-7}. IP video distribution, however, is volatile, erratic, and subject to a wide range of distortions, artifacts, and degradations during

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

acquisition, compression, processing, transmission, and reproduction, especially under peak network load conditions.

IP video streams are also highly sensitive to packet loss. Even a very minimal packet loss in an IPTV stream can result in significant degradation in video quality. (A single dropped I-frame in an IP video stream causes the user's screen to literally freeze for several seconds, until the next I-frame arrives and the screen can be refreshed.)

Finally, video quality in IPTV networks tends to operate as a negative feedback loop: As service providers deliver better quality, they can attract more customers. The more customers the service attracts, however, the more congested the network can become – and the more video quality can degrade. These problems are compounded by the fact that many IPTV networks rely on digital subscriber line (DSL) access links, which typically employ twisted copper in the last mile to the customer home. Copper access networks are highly susceptible to interference from many sources and thus are subject to significant packet loss and delay.

While a variety of issues can affect video quality in IPTV networks, we identify four issues as the key causes of unsatisfactory subscriber QoE: network congestion, bit errors on access lines, slow channel change times, and limited ability to monitor per-subscriber video quality. We propose a set of standards-based core and aggregation-layer techniques to address each of these issues, collectively referred to as Visual Quality of Experience (VQE). This VQE approach encompasses two key components to address quality issues associated with both VoD and multicast video services:

1. On-path VoD connection admission control (CAC) in the network core and aggregation layers to prevent network congestion
2. A standards-based signaling mechanism operating between the provider edge (PE) aggregation router and the subscriber set-top-box (STB) to perform error repair, accelerate channel change times, and provide packet monitoring and QoE reporting

Together, these VQE techniques can provide an end-to-end quality control and monitoring capability for IPTV service providers that extends from the core network to the aggregation edge, and all the way to the subscriber STB. Ultimately, these capabilities allow service providers to:

- Improve video quality, increasing customer satisfaction and strengthening the service provider's brand
- Reduce network congestion and guarantee a consistent QoE to all subscribers
- Make efficient use of all available bandwidth in the network
- Reduce access line signal-to-noise ratio and bit error rate requirements for IPTV services, expanding the addressable market for their services
- More accurately and proactively isolate quality issues, reducing costly help-desk calls and truck rolls

Video Connection Admission Control

Background

One of the most significant challenges in delivering high-quality IP video is ensuring adequate bandwidth in the aggregation network to support the traffic load without congestion. Reserving bandwidth for broadcast (multicast) IPTV traffic is a relatively simple task, as bandwidth requirements are determined solely by the number of channels offered, independent of the number of subscribers viewing those channels. Supporting VoD sessions, however, in which each unicast stream requires dedicated bandwidth, is a more complex problem.

Unlike conventional Internet/web data traffic, unicast VoD streams are inelastic and cannot readily adapt to network congestion, whether due to oversubscription of a link or to an outage. As discussed, VoD streams are also large (requiring as much as 12 Mbps for HD video) and intolerant to packet loss and jitter. Since all subscribers on an aggregation link typically share a class-based Quality-of-Service (QoS) queue, the moment the aggregate VoD load exceeds capacity – even by a single session – video quality degrades for all subscribers on that link. This problem is compounded in resilient aggregation networks in that, in the event of a failure (whether due to a trunk or ring failure, a node failure, or even a scheduled upgrade), all sessions converge on and oversubscribe the remaining reduced-capacity path.

It is simply not cost-effective for a service provider to engineer a congestion-free residential metro or aggregation network that can support concurrent VoD connectivity to, for example, 25,000 customers connected to an aggregation router. At the same time, given the delay-sensitive nature of video traffic, service providers cannot oversubscribe the aggregation network as would be possible when supporting other types of traffic, such as high-speed Internet services.

Service providers must therefore engineer the network based on expected peak VoD load. The highly dynamic nature of subscriber VoD usage, however, makes such predictions difficult. Even using sound estimates based on past usage, situations are likely to arise (whether due to unexpected usage spikes or to a network failure that reduces capacity) in which more subscribers are requesting VoD sessions than current network capacity can support. As network capacity approaches oversubscription, some mechanism is needed to prevent new users from pulling more VoD streams until the capacity is available to support them, and to provide a graceful denial to subscribers, comparable to a busy signal on a telephone network.

The most effective solution is to employ some signaling intelligence in the network to perform per-flow admission control and deny the initiation of new VoD sessions until the necessary network bandwidth can be re-captured (i.e., until a current VoD user goes offline), and then allocate those resources dynamically to new users. Such a mechanism also should ensure that in the event of a network failure that causes re-routed sessions to oversubscribe the remaining path, some subset of those established sessions are torn down to preserve the quality of the remaining sessions.

Ideally, this admission control mechanism should meet six key requirements:

1. It should be accurate, allowing distribution network elements to communicate directly with the VoD server and make CAC decisions based on real-time bandwidth availability on the actual path that will support the VoD session.
2. It should be efficient, allowing service providers to allocate all available bandwidth to VoD sessions without requiring unused capacity to be held in reserve.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

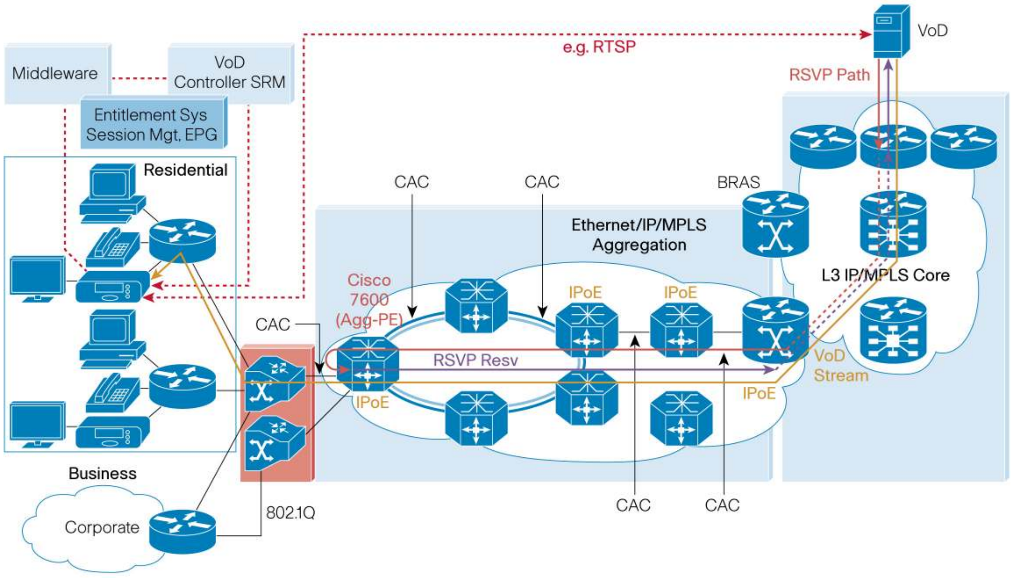
3. It should employ intelligent resiliency mechanisms that adapt to failures gracefully, re-establishing admission-controlled VoD sessions on new paths without tearing down large numbers of sessions unnecessarily.
4. It should be topology-independent, allowing it to interoperate with complex network topologies that have redundant and load-sharing paths in the transport layer of the network.
5. It should be network-based and STB-independent, interoperating with deployed STBs without requiring them to run any CAC-specific protocol.
6. It should be standards-based, relying on standardized Layer-3 forwarding mechanisms that do not require extensive integration with system middleware and can interoperate with any standards-based equipment deployed in the access layer of the network.

We propose an on-path VoD CAC approach based on the Internet Engineering Task Force (IETF) Resource ReSerVation Protocol (RSVP) [3] to perform essential video admission control functions and meet these requirements.

On-Path RSVP CAC

The proposed CAC solution employs standardized RSVP for signaling, sent by the VoD server (or a component on its behalf) before the beginning of the video session. At a high level, this approach operates as follows: The subscriber issues a command to the STB to select an on-demand video stream. The request goes through the PE aggregation router and on to the VoD server. The VoD server then issues an RSVP message, which follows the video entitlement management message (EMM) from the middleware application server to the subscriber, traversing the exact path that the VoD session will use, while tracking any real-time changes in the core and distribution layers. Along the path, each video distribution element performs a network bandwidth accounting function. The routers allow the VoD session if sufficient bandwidth is available to support the video stream, and deny the request if it is not. When a stream is denied, the router sends an RSVP-CAC message back to the VoD server, which in turns sends the subscriber a graceful denial message (e.g., a busy signal) in concert with the video middleware application client-server software. [4] Fig. 1 illustrates this approach in a typical service provider network.

Figure 1. On-path RSVP CAC Signaling for VoD Session



This model employs an on-path CAC approach. "On-path" refers to the fact that the admission control request and confirmation are explicitly signaled in the network (via RSVP) along the actual path that the new VoD session would follow. RSVP-based on-path CAC can be seen as a fully distributed admission control method, in that admission control decisions are made by the network elements themselves, without any external mechanisms required. The on-path RSVP CAC approach contrasts with "off-path" admission control methods that concentrate CAC intelligence in a centralized server.

On-path RSVP CAC offers the following advantages:

- *Accuracy* – The bandwidth reservation for each session occurs along the exact Interior Gateway Protocol (IGP) path the VoD session will use
- *100 percent bandwidth efficiency* – If a link has the capacity for 1000 VoD sessions, for example, RSVP will always accept the 1000th session and reject the 1001st.
- *Resiliency* – In the event of a topology change (due to network failures, router upgrades, addition of links, etc.) reservations automatically re-establish along the newly re-routed IGP path of the VoD session, without having to re-signal CAC or rebuild the entire connection. RSVP on-path VoD CAC co-exists with Multiprotocol Label Switching (MPLS) Fast Re-Route (FRR) link and node protection to restore connectivity (including CAC reservations) within 50 milliseconds (ms) of link or node failure. In networks that do not run FRR, RSVP CAC provides native Fast Local Repair features to dynamically re-establish reservations after a failure.
- *Flexibility* – RSVP CAC allows service providers to extend CAC end-to-end from the video head-end (VHE) to the last-mile router, within any network topology, regardless of where video content is sourced.
- *STB interoperability* – RSVP CAC functions entirely within the core and aggregation layers. It requires no integration with STBs, and can be implemented even in environments with older, previously deployed STBs.
- *Minimal processing requirements* – RSVP CAC has minimal impact on router central processing units (CPUs), making it suitable for very large deployments.
- *Ease of implementation* – RSVP CAC functions are localized to the network and require only that network elements support a subset of the fully standardized RSVP protocol.

RSVP CAC Operations

The following section details the steps involved in a typical RSVP CAC operation for both a successful and unsuccessful VoD session request:

1. The STB relays the customer request for a new VoD session via an application-layer Real Time Streaming Protocol (RTSP) [5] setup command to the VoD server. (Depending on the network, other steps may occur before this, such as the STB communicating with the VoD middleware or session manager to obtain the address and other parameters of the VoD server.)
2. Before accepting the VoD session request at the application layer, the VoD server requests the corresponding bandwidth reservation in the network by generating RSVP Signaling (e.g., an RSVP Path message) which travels downstream toward the STB. The Path message traffic specification (TSPEC) contains the bandwidth required for the VoD session (e.g., 4 Mbps).

3. At each hop, IGP routes the Path message downstream toward the requesting STB. RSVP-enabled routers at each hop process the path message and install a corresponding Path soft state.
4. When the Path message reaches the aggregation PE router, the router activates the RSVP Receiver Proxy function on its DSL access multiplexer (DSLAM)-facing interface to terminate the Path message and generate a corresponding RSVP reservation request (Resv) message. (Note: at this point, the RSVP path message is not forwarded to the DSLAM or requesting STB. It is terminated on the egress interface of the aggregation PE router.) The Resv message contains the VoD session bandwidth encoded in the Resv flow specification (FLOWSPEC), which is the same value as in the Path TSPEC (e.g., 4 Mbps).
5. The RSVP Receiver Proxy function hands the Resv message over to the regular RSVP module on the PE aggregation router. The RSVP module then performs processing of the Resv message exactly as if it had been received from the downstream STB, and performs admission control on the egress, or DSLAM-facing interface. If this admission control decision is successful, RSVP creates a corresponding Resv soft state and forwards the Resv message upstream to the previous RSVP hop.
6. As per normal RSVP operations, the Resv message gets routed back upstream toward the VoD server along the exact same path as was followed by the Path message. (To ensure this, each RSVP router explicitly addresses the Resv message to the RSVP Previous hop, based on the previously established Path state.)
7. At each RSVP hop, the router performs admission control on the downstream link from that hop and makes an admission control decision based on the available bandwidth on that egress interface. The router allocates the requested bandwidth (e.g., 4 Mbps) from the global RSVP pool of the interface and installs the Resv soft state.

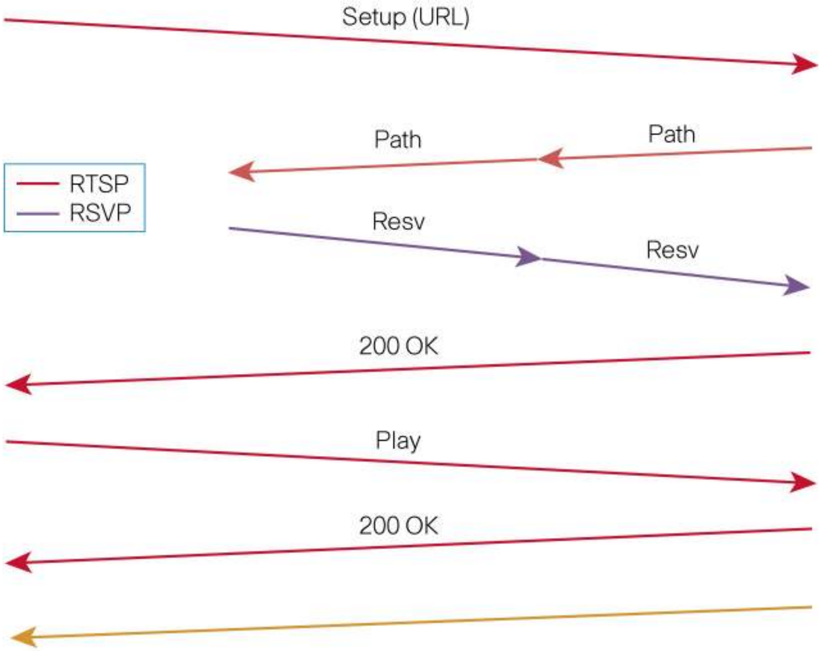
If the admission control decision is successful at every hop, the following occurs:

1. The VoD server receives the Resv message confirming the successful reservation of the bandwidth (e.g., 4 Mbps) for the VoD session across the aggregation network.
2. The VoD server then confirms to the requesting STB, at the application layer, that the new VoD session is accepted (sending a RTSP status code 200, i.e., “OK,” to confirm RTSP setup).
3. The STB responds with a RTSP “Play” command to the VoD server.
4. The VoD server recognizes that the corresponding RSVP reservation is already in place and responds again with a RTSP status code 200 indicating the “Play” command was executed successfully.
5. The VoD server begins unicasting the corresponding media stream to the subscriber.

Fig. 2 illustrates a successful admission control decision.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 2. Successful On-path RSVP CAC Signaling



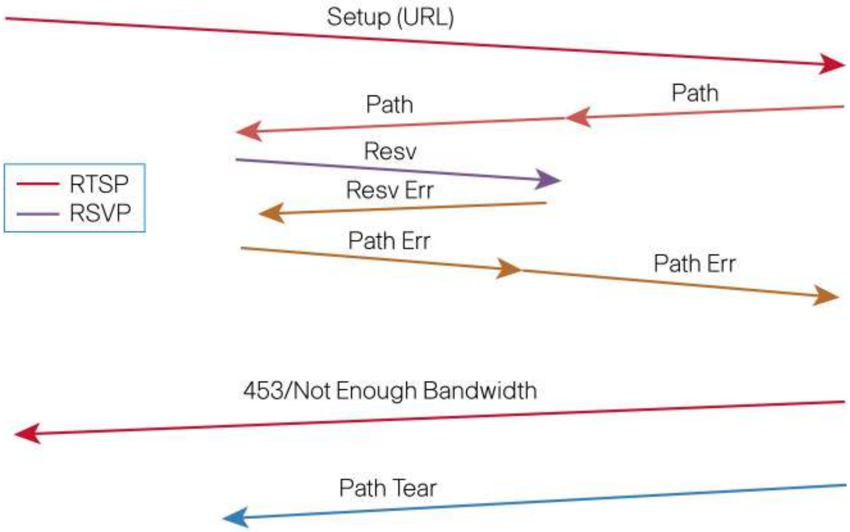
Alternatively, if a router at any hop upstream from the PE aggregation router performs admission control on its downstream link and finds insufficient remaining bandwidth for the new session, the admission control for the new VoD session fails, and the router does not install this reservation. In this scenario, the following occurs:

1. The router sends a Resv Error message back downstream toward the PE aggregation router indicating that admission control for the reservation has failed. (All other existing reservations are not affected by this failure and remain in place.)
2. The RSVP Receiver Proxy function in the PE aggregation router processes the Resv Error message, and sends a Path Error message containing the error code “Admission Control Failed” back upstream to the VoD server to provide explicit notification of the CAC failure. (Currently, RSVP operations are entirely receiver-driven, so the current RSVP standard only allows the use of this error code in a Resv error message, not a Path error message. The Transport Area (TSV) Working Group of the IETF has standardized an extension to RSVP to expand this functionality.) [6]
3. On receipt of the Path Error message, the VoD server recognizes that admission control failed, and sends a RTSP status code 453 (i.e., “Not Enough Bandwidth”) to the STB.
4. The STB recognizes that the VoD request was denied because the network is busy, and the VoD middleware displays a meaningful, user-friendly message to the subscriber, such as “Sorry, the network is currently busy. Please try your request again later.”
5. The VoD server injects a Path Tear message (addressed to the STB, just as the original Path message was) to immediately clean up all the RSVP soft states in the network for that failed reservation and free up any bandwidth which may have been reserved by the RSVP Receiver Proxy function on the downstream interface of the PE aggregation router.

Fig. 3 illustrates an unsuccessful admission control decision.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 3. Unsuccessful On-path RSVP CAC Signaling



Through this process, RSVP VoD CAC provides a highly efficient mechanism for extending admission control intelligence from the VHE to the last-mile router, and preventing network congestion to preserve subscriber video quality.

Responding to Network Failures

In the event of a network failure that causes re-routed VoD sessions to oversubscribe the remaining path, RSVP CAC provides features to dynamically tear down a subset of established sessions to preserve the quality of the remaining sessions. In addition to meeting the sub-50-ms convergence times that service providers require, RSVP provides the intelligence to tear down only those reservations that cannot fit on the new path and preserve those that can. RSVP dynamically re-establishes reservations around the failed link without requiring all VoD sessions to be torn down and rebuilt end-to-end.

RSVP CAC co-exists with MPLS Traffic Engineering (TE) FRR, allowing new paths to be established dynamically after a failure within 50 ms, with no impact to CAC. For networks that do not run TE FRR (or as a backup resiliency feature in networks that do), RSVP also provides a Fast Local Repair feature, which is enabled by default once RSVP is enabled.

To accomplish this intelligent resiliency, RSVP re-subjects every reservation affected by a route change during reconvergence to admission control. RSVP maintains sessions that can fit on the new path and tears down sessions that cannot, and in both cases, provides proper notification to the VoD server. This process occurs within a few seconds of reconvergence – meaning that users are subjected to a maximum of a few seconds of QoE degradation as a result of oversubscription after reconvergence.

RSVP Pre-Emption Features

A basic RSVP CAC implementation will effectively control VoD sessions to eliminate network congestion. Some service providers, however, may wish to exercise additional control over the priority in which requested VoD sessions are accepted or denied, or established VoD sessions are torn down in the event of a reconvergence. RSVP VoD CAC supports this pre-emption priority feature. [7]

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

RSVP CAC pre-emption features allow each reservation to be associated with a preemption priority. In the event that not all reservations can be established through a given link, the RSVP admission control algorithm will admit reservations in accordance with their preemption priority. For example, if all the RSVP bandwidth on a link is already reserved by established reservations with a low preemption priority, and an establishment request arrives for a new reservation with a high preemption priority, then RSVP will bump one low priority reservation (or as many as needed) to make room for the new reservation. Similarly, if the RSVP bandwidth on an interface is reduced for some reason and all currently established reservations no longer fit, RSVP will bump as many reservations as needed, starting with those with the lowest pre-emption priority.

Service providers employing RSVP VoD CAC can use these preemption features to provide granular prioritization across different types of content and build a system that intelligently responds to resource shortages according to a variety of operational priorities. For example, service providers can associate a lower pre-emption priority with free VoD content and a higher priority with paid content. In normal circumstances, both free and paid content would be supported. In special circumstances, however, when bandwidth becomes scarce, free VoD sessions would always make room for revenue-generating paid sessions.

To use RSVP preemption, the VoD gear responsible for initiating RSVP signaling (either the VoD server or the session manager) need only include a POLICY_DATA object containing a Preemption Priority Policy Element in the Path messages. This POLICY_DATA object will be echoed back inside the Resv by the RSVP Receiver Proxy and then honored by every RSVP router processing the Resv message.

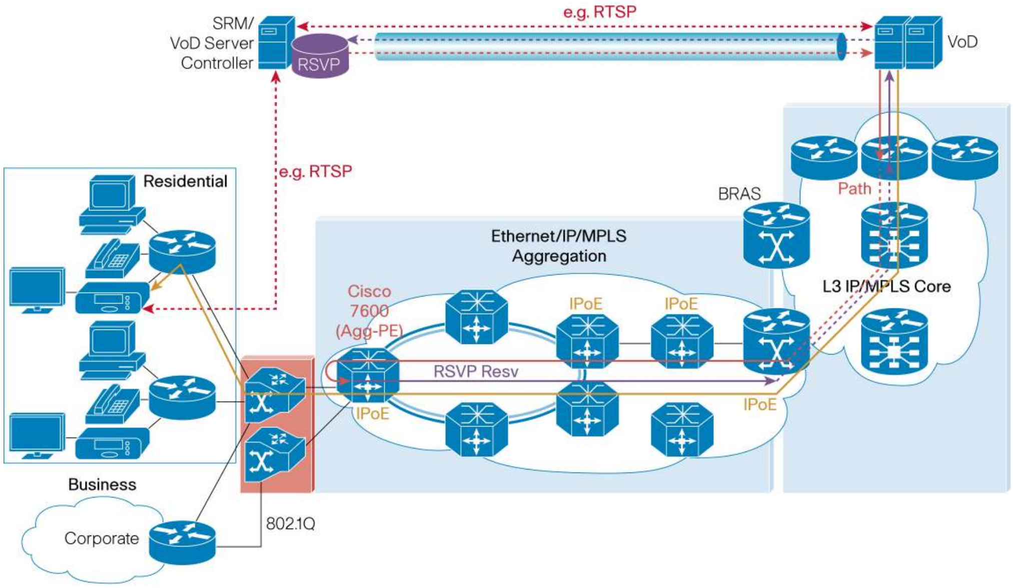
Implementing RSVP on VoD Equipment

Service providers have two options for implementing the RSVP protocol stack on VoD equipment to perform RSVP admission control. The first option is to deploy RSVP directly on the VoD server. In this scenario, RSVP messages are synchronized with VoD streaming. (The example scenario described above is based on this implementation.)

If deploying RSVP directly on the VoD server is not feasible (for example, if the VoD server cannot easily support RSVP), service providers can deploy RSVP on a centralized session resource manager (SRM). In this scenario, the SRM is remotely connected via a Generic Routing Encapsulation (GRE) tunnel to the first-hop router (FHR) that is directly connected to the VoD server. Fig. 4 illustrates the RSVP CAC process in a network with RSVP deployed on a centralized SRM.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 4. RSVP on SRM



Since Path messages generated by the remote session manager must follow the same path through the network as their corresponding VoD sessions, the session manager injects Path messages into the network at the FHR by tunneling them into the GRE tunnel to the FHR. To the FHR then, it appears that the RSVP Path message has been generated by the VoD server, and RSVP VoD CAC proceeds as described in the example above.

Deploying On-Path RSVP VoD CAC

To support on-path RSVP CAC, IPTV networks must meet two key requirements. First, every network element, from the video distribution router connecting the VoD servers to the aggregation routers in central offices, must support native Layer-3 forwarding intelligence. Second, because RSVP is an IP-based protocol and follows the exact path of VoD streams, the network must transport VoD sessions natively over IP or over MPLS Label Distribution Protocol (LDP) in the Global Table.

IPTV services typically are delivered over “triple play” (voice, broadband Internet, and video) networks. As a result, service providers must account for the handling of both VoD traffic, which demands more rigorous treatment, and other types of Internet and business traffic which do not. Following are three RSVP CAC deployment models describing a native IP aggregation network, a hybrid network that transports video as native IP and MPLS/LDP for non-video traffic, and a network that transports all services (including video) over MPLS/LDP:

- *Pure native-IP aggregation network* – In this scenario, the network carries all traffic as native IP and applies CAC to VoD sessions.
- *VoD over IP + Internet/business traffic over MPLS* – In this scenario, the network also carries VoD traffic as native IP and applies CAC. Non-VoD traffic, however, is carried over MPLS/LDP either in Virtual Routing and Forwarding (VRF) tunnels or in the Global Table. MPLS/LDP selective advertisement ensures that prefixes used for VoD traffic are not label-switched.
- *VoD over MPLS* – In this scenario, the network uses MPLS/LDP for all traffic, including business/Internet traffic and VoD sessions. The network carries VoD traffic over MPLS/LDP

in the Global Table and applies RSVP CAC. However, the network transmits the IP version 4 (IPv4) Path messages for the corresponding VoD flows as native IP packets without MPLS encapsulation. This allows for RSVP processing at every hop, even if the VoD media packets themselves are encapsulated in MPLS.

RSVP CAC Scalability

On-path RSVP-based CAC is highly scalable. While RSVP has had a reputation for scalability issues in the past, this perception is due to the previous generation of RSVP's (RSVP IntServ) model for QoS enforcement. RSVP IntServ required maintenance of a separate scheduling state (e.g., a separate queue) in the data path. The current RSVP CAC approach is based on the "RSVP over Diffserv" model. In this model, the router maintains a soft state per reservation in the control plane, but relies purely on normal Diffserv mechanisms in the data path, allowing it to scale to hundreds of thousands of reservations per device. [8]

With RSVP over Diffserv, RSVP does not perform any policing nor separate queuing (neither per flow nor aggregate) for admitted flows. It operates purely in the control plane and is solely responsible for performing admission control of flows over a configured bandwidth pool.

Extending RSVP CAC to Core Networks

Large service providers tend to distribute VoD content to multiple locations and often overprovision their IP/MPLS core networks, so RSVP VoD CAC is not typically required in the core network. RSVP CAC can, however, extend across the entire end-to-end network and deliver benefits even in core networks. For example, while oversubscription may not be a concern in the immediate future, service providers typically have little visibility into video traffic in core networks, and no efficient means of accurately monitoring VoD bandwidth utilization. Extending RSVP CAC to the core network can provide an intelligent mechanism for accomplishing this, while supporting VoD bandwidth control capabilities that may be employed in the future.

The chief requirement for providing RSVP CAC in core networks is core platform support for IPv4 RSVP CAC. If the core network meets this requirement, RSVP provides a MPLS TE Tunnel Based Admission Control (TBAC) feature to support aggregation of RSVP reservations over MPLS TE tunnels, and extend CAC end-to-end across the provider network. [9] RSVP also supports TBAC in VRF tunnels [11].

Access Line Bit Error Repair

Background

While the CAC section above focuses on unicast VoD services, service providers also face challenges delivering a high QoE for multicast TV, especially over the copper wiring that is common in the last mile of IPTV networks. The most significant concern for such service providers is the amount of overall line errors that can occur on subscriber access lines.

Most service providers have built out their networks to deliver 10^{-6} packet loss across broadband subscriber lines, which is acceptable for high-speed Internet services that are more tolerant of packet loss and can take advantage of Transmission Control Protocol (TCP) retransmission characteristics. Video traffic, however, requires a much more rigorous standard to achieve acceptable QoE. In the worst cases, typical DSL bit error rates of 10^{-7} can translate to packet loss rates of 10^{-3} – or an artifact every minute.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Incoming IPTV packets will be dropped if they fail cyclic redundancy checks (CRC) on the receiving DSL modem, routing gateway, or STB. Bit errors also can be caused by electrical impulse noise as packets traverse DSL transmission lines, or may result from poor building wiring – especially common in aging multi-tenant dwellings. Although DSL offers Layer-1 error mitigation features, these techniques were not designed to cope with the effects of sustained bursts typical of impulse noise.

Forward Error Correction (FEC) capabilities in DSLAMs support basic error repair functions, but current FEC employs very limited repair algorithms that cannot provide the granularity demanded by highly loss-sensitive traffic such as video. (More advanced FEC algorithms that allow for partial packet reconstruction are currently in development, however, and may be available in the future.) In addition, current FEC transmission is extremely inefficient with high overhead – a significant problem in video services that are bandwidth-intensive to begin with.

In light of these issues, service providers need some intelligent signaling mechanism operating between the STB and the PE aggregation network that can monitor for errors, request packet retransmissions, fulfill those requests within the time constraints of the STB’s jitter buffer, and splice re-transmitted unicast packets with the “live” multicast stream.

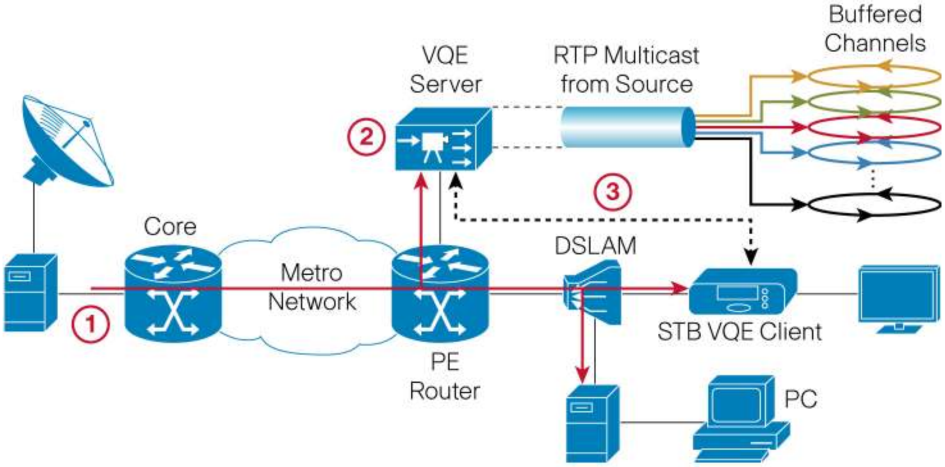
As part of its VQE approach, we propose a client-server signaling mechanism that employs Real-Time Transport Protocol (RTP) video encapsulation and RTP selective unicast transmission to provide these services. [10] Drawing on intelligence localized in both the subscriber STB and the service provider’s intelligent network edge, such a mechanism provides an ideal solution for dynamically recognizing and addressing access line errors. (This mechanism can also provide the technology foundation for accelerating channel change times and performing IPTV packet monitoring, as discussed in sections IV and V.)

Bit Error Repair Operation

The bit error repair capability within VQE (as well as the channel change time and monitoring functions described in later sections of this paper) is based on a client-server model. The server portion is deployed at the intelligent edge of the network, i.e., the Video Switching Office (VSO) or Central Office (CO). The client software resides in the subscriber STBs. At the highest level, the VQE client and server components work together in the bit error repair function to detect any dropped packets, request retransmission, and splice re-transmitted packets into the multicast stream. Fig. 5 illustrates this client-server mechanism at a high level.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 5. VQE Client-Server Model



As discussed, this VQE model requires video traffic to be encapsulated in RTP. This allows each IPTV packet within a given multicast group or channel to be assigned a unique RTP sequence number. This sequence number is at the core of the VQE mechanism's ability to identify specific dropped packets, request their retransmission, and re-order video packets in the STB's jitter buffer to splice in re-transmitted packets.

To support VQE error repair functions, the VQE server should be configured to receive all broadcast channels (e.g., to join all multicast groups). The server joins multicast groups using Internet Group Management Protocol (IGMP) "join" requests, like any other IP host. The VQE server maintains a dedicated circular buffer for each channel/multicast group and caches a few seconds of program content from each. This cached data is used to service error repair requests from downstream VQE clients.

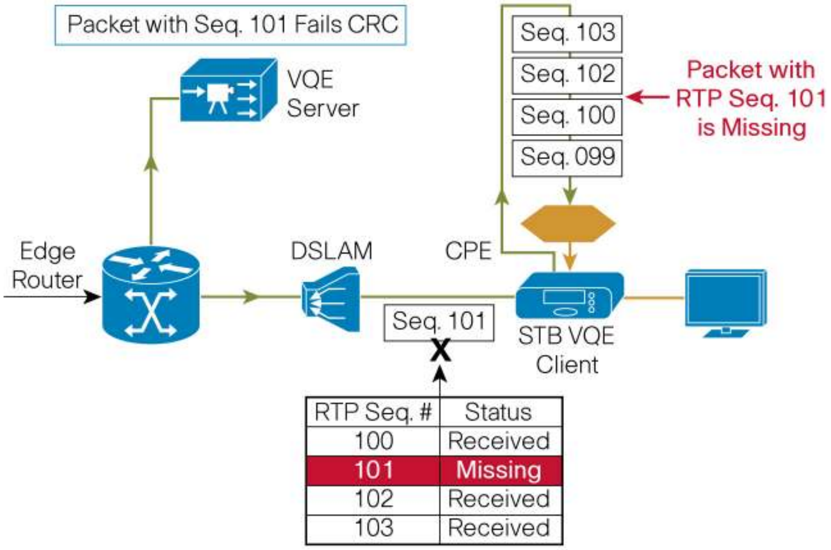
The error repair operation proceeds as follows:

1. The video source transmits multicast packets encapsulated in RTP to the subscriber STB.
2. The VQE client software in the subscriber STB tracks the sequence numbers of incoming RTP video packets. When it detects a missing sequence number (for example, if a corrupted packet has failed the STB's CRC error check and been discarded), the client requests retransmission of that packet from its associated VQE server, using standardized Real-Time Transport Control Protocol (RTCP). [10] The client may request a single packet or multiple packets in a single transaction.
3. Upon receipt of the request, the VQE server locates the appropriate channel cache, copies the requested RTP packets, and transmits them to the requesting client.
4. The receiving client splices the "repair" packets into its jitter buffer according to the RTP sequence numbers, re-ordering packets within the window defined in the RTCP standard.
5. The client also provides a de-jitter function (using the RTP time-stamp information provided in each packet) so that packets handed off to the STB's MPEG Transport Stream (TS) de-multiplexing/decoding stage are free of network-induced jitter.

Fig. 6 illustrates the VQE client recognizing a missing packet. Fig. 7 shows the synchronization of the re-transmitted packet.

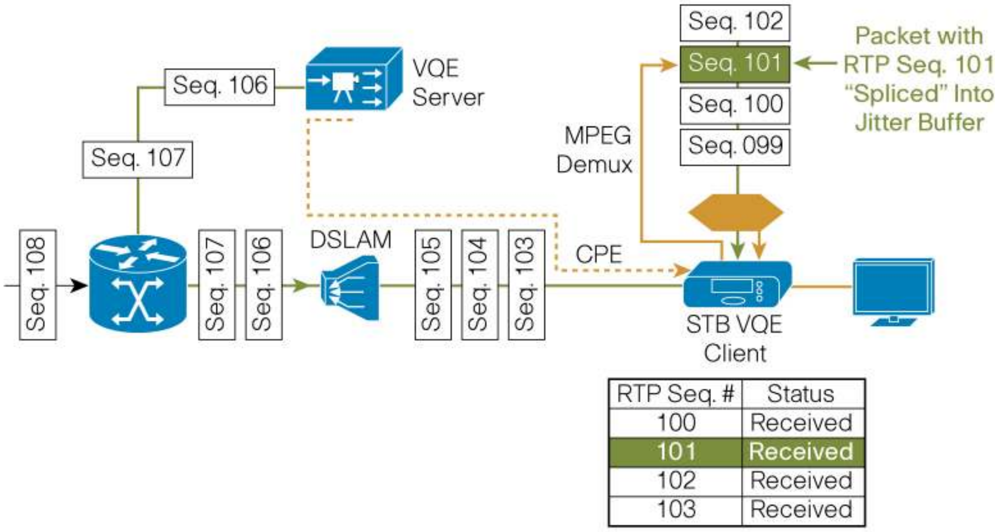
© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 6. Bit Error Repair – Stage 1



RTP Seq. #	Status
100	Received
101	Missing
102	Received
103	Received

Figure 7. Bit Error Repair – Stage 2



RTP Seq. #	Status
100	Received
101	Received
102	Received
103	Received

The entire transaction should take, on average, about 100 ms to complete, although transaction time is dependent on the round-trip delay between the VQE client and server. Since the operation happens prior to the MPEG TS de-multiplexing/decoding stage, and since typical IPTV STBs employ 250-ms jitter buffers, the transaction should be transparent to the subscriber from an audio/video quality perspective.

Ultimately, this VQE function results in a highly reliable error repair capability, allowing service providers to address one of the chief culprits of poor IPTV video quality and deliver a better QoE to more subscribers.

Network Requirements for VQE Error Repair

As discussed, the chief network requirement for VQE error repair is support for RTP and RTCP. The VQE server also requires a direct Layer-3 connection to the PE aggregation router for the

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

purpose of joining and leaving multicast groups. An IP multicast path is also required between the VQE server and client for signaling and transmission of data packets.

Beyond these requirements, this VQE error repair technique calls for some minimal communication with application-layer middleware. Both the VQE server and VQE clients must receive continually updated channel lineup information (per-channel IP multicast addresses, RTP and RTCP port numbers, unicast addresses, etc.).

Standards-Based Rapid Channel Change

Background

As service providers continually add channels and VoD content to compete for subscribers, users switch between channels more frequently than in the past. Subscribers expect to receive the same, virtually instantaneous channel change time (CCT) to which they have grown accustomed with analog and digital cable services, and they expect an immediate response to their viewing requests. CCT delays in IPTV systems, however, can be both longer and more variable than digital cable – both of which issues can detract from the overall subscriber QoE.

These increased CCT delays can result from a number of factors, including:

- *IGMP signaling delay* – Unlike the traditional cable model, in which the STB receives all offered channels concurrently, IPTV STBs typically must communicate with the upstream multicast source (e.g., transmit a IGMP “leave” request for the current channel and a “join” request for the new channel) for each channel change. The IGMP “leave” and “join” messages sent by the STB either flow directly to the PE aggregation router or are processed by an intervening IGMP snooping device such as a DSLAM. IPTV networks should support “fast leave” to minimize IGMP signaling delay, but the signaling process does cause some inherent CCT lag.
- *Conditional access system (CAS) key acquisition delay* – A typical CAS encrypts digital services using entitlement control messages (ECMs) and EMMs. A STB must receive and decrypt the correct ECMs and EMMs in order to generate the final keys needed to decrypt and display a particular video stream. Any delay in this process can add to the CCT delay.
- *MPEG decoding delay* – When an STB completes a IGMP “join” request and begins receiving the new multicast stream containing MPEG TS packets, it must acquire program-specific information (PSI) frames in order to determine the desired TV channel. The time it takes for the decoder to receive the program-allocation-table (PAT) frame determines the time it takes for it to display programs. MPEG specifications indicate a decoder must receive a PAT every .5 seconds.
- *I-frame acquisition delay* – To reduce the amount of bandwidth required for digital video transmission, compression methods such as MPEG package the video frames of a digital video stream into various types of standardized MPEG frames. These frame types are known as I-frames, P-frames, and B-frames, named for the type of MPEG frame prediction used in performing their encoding. The I-frame serves as the reference picture that begins each “Group of Pictures” (GOP) – a discrete packet of 12-15 frames from which the MPEG decoder generates the visible video frames. The time it takes the STB to acquire the I-frame is proportional to the size of the GOP. In typical digital cable broadcasts, this delay is approximately .5 seconds. IPTV systems, however, tend to use more compression to reduce bit rates – which increases the size of the GOP, leading to longer I-frame acquisition times.

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

A common misconception is that IP multicast signaling delays are the chief culprit in increased or variable CCT delay. In fact, multicast “leave” and “join” signaling typically constitutes just 8 percent of total CCT, or 100 ms combined. The biggest factor in CCT delay is actually I-frame acquisition delay, which can last 500 ms or longer, and typically constitutes 39 percent or more of total CCT, depending on the compression and the STB.

Once again, we propose the VQE model to address this issue. The same VQE client-server intelligence operating between the STB and the provider edge used to repair bit errors can be extended to circumvent I-frame acquisition delays and accelerate CCT, and ultimately, to improve overall subscriber QoE.

VQE Rapid Channel Change Operation

As with error repair, the VQE rapid channel change transaction employs standardized RTP and RTCP to perform signaling between the STB and the video aggregation network, and optimize CCT. They key to accelerating CCT in this model is that the VQE server begins unicasting the IPTV packets to the client STB at the same time as the network is processing the IGMP “leave” and “join” requests to begin normal multicast streaming of the new channel. The STB can begin processing the unicast packets immediately, and then synchronize the display with the multicast stream once it becomes available. This capability greatly reduces the time a subscriber waits before the image is rendered on the TV screen.

The rapid CCT transaction proceeds as follows:

1. When the subscriber changes channels, the STB-based VQE client requests IPTV packets for the new channel from its target VQE server, again using RTCP messages. In parallel, the client also issues an IGMP “join” request to the video source for the required channel.
2. Upon receipt of the rapid CCT request, the VQE server locates the appropriate channel cache, identifies the location of IPTV packets carrying the most recent I-frame for that channel, and transmits a short unicast burst of packets, starting with the I-frame, to the requesting client.
3. Because the incoming burst from the VQE server contains an I-frame, the STB decoder can immediately begin processing the MPEG information upon receipt of the unicast burst. The STB play-out buffer fills, and the MPEG decoder activates and renders the screen with the video.
4. After a short time, multicast packets begin arriving at the STB. The STB VQE client monitors the RTP sequence numbers from both the unicast and multicast streams. As soon as it identifies an overlap, it sends a RTCP message to the VQE server to cease unicast streaming.

This rapid CCT process can improve the responsiveness of channel changes from several seconds to around one second (depending on the efficiency of the STB’s buffer management and I-frame capabilities), providing a notable improvement in overall subscriber QoE.

Preventing Network Congestion During Unicast Bursts

While service providers must strive to accelerate CCT in IPTV networks, they also must ensure that the combined multicast + unicast bandwidth consumed by the VQE rapid CCT transaction does not exceed the available bandwidth. The proposed VQE rapid CCT mechanism includes rate-shaping features to prevent congestion in the access network that might otherwise be caused by the transaction.

To support this capability, the VQE server performing the CCT transaction sends unicast data in a two-phase burst. In Phase 1, the unicast burst begins at a higher rate that exceeds the normal unicast streaming rate up to a pre-determined excess rate, configured by the service provider. In Phase 2 – after the initial unicast burst but before normal multicast streaming begins – the unicast burst rate decreases to a level that will allow combined unicast + multicast streaming to proceed without exceeding available bandwidth.

This rate-shaping capability allows service providers to set excess video rates on a per-subscriber basis, providing greater flexibility and scalability in deploying rapid CCT VQE mechanisms.

Video QoE Monitoring and Reporting

Background

It is not enough to deploy mechanisms for delivering higher video quality if a service provider has no means of measuring subscriber QoE. This concern is more than academic; accurate video quality information is critical to effective traffic modeling and traffic engineering. Implementing mechanisms to monitor video quality, however, has traditionally been a complicated endeavor. Moving forward, to satisfy demanding customers and differentiate their offerings based on video quality, service providers will require straightforward and easy-to-obtain information about per-subscriber video flows.

As in the error repair and rapid CCT scenarios, service providers can employ the RTCP signaling mechanisms in the proposed VQE client-server model to address this requirement.

VQE Monitoring and Reporting Operations

Since each STB-based VQE client supports RTP, each client supports RTP’s rich packet-level statistics-gathering capabilities. Statistics include cumulative information on loss, jitter, and delay of RTP streams. The proposed VQE mechanism draws on those statistics for standards-based monitoring and reporting.

In operation, the VQE client transmits a compound “Receiver Report” packet [10] to a target VQE server (not to the RTP source). These compound packets can be sent periodically, or as part of every bit error repair or rapid channel change request. The VQE server in turn sends the compound Receiver Reports via a standards-based TCP interface to a network analysis tool.

With these continuous RTP signaling capabilities, service providers can proactively monitor per-subscriber video quality from the VHE to the STB, and generate accurate reports of per-subscriber QoE information. This allows service providers to more easily isolate problems, such as narrowing down the source of a quality issue to the DSLAM, the external wiring plant or the in-house wiring. Ultimately, these capabilities allow service providers to respond to quality issues proactively, and take ameliorative action for many issues without requiring an onsite diagnosis.

Conclusion

As more service providers incorporate video into their service portfolios and IP communication networks, they will face a continually growing challenge to preserve video quality and deliver excellent subscriber QoE. The proposed VQE approach described in this paper provides a standards-based, highly efficient set of techniques to inject granular QoE control mechanisms into IPTV networks. With these techniques, service providers can extend intelligent quality controls from the core network through the aggregation layer, and from the provider edge to the subscriber home to deliver consistently superior QoE.

References

[1] Internet Innovation Alliance, “Bringing Up Broadband: Higher Traffic; Higher Costs,” *USA Today*, April 27, 2008.

[2] ETSI EN 300 429 V1.2.1 (1998-04), “Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for cable systems.”

[3] IETF Request for Comments (RFC) Document 2205, “Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification.

[4] EDCS-45526, “RSVP VoD CAC: System Functional Specification.”

[5] IETF RFC 2326, “Real Time Streaming Protocol.”

[6] draft-ietf-tsvwg-rsvp-proxy-approaches, “RSVP Proxy Approaches.” A and draft-ietf-tsvwg-rsvp-proxy-proto "Protocol Extensions for RSVP Receiver Proxy"

[7] IETF RFC 3181, “Signaled Preemption Priority Policy Element.”

[8] IETF RFC2998, “Integrated Services Operation Over Diffserv Networks.”

[9] RFC4804, “Aggregation of RSVP Reservations Over MPLS TE/DS-TE Tunnels.”

[10] IETF RFC 3550, “RTP: A Transport Protocol for Real-Time Applications.”

[11] draft-davie-tsvwg-rsvp-l3vpn "RSVP in Layer 3 VPNs

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Printed in USA C11-496525-00 09/08

© 2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.