Introduction
As a relatively new technology and service, IPTV still lacks a lot of quantitative metrics for measuring performance. This is, in part, because most IPTV deployments are still small in total numbers of subscribers, lacking the scaling necessary to adequately measure performance. As a result, a carrier faced with architecting their IPTV system and network has little or no empirical data to guide them to the best approach. And, unlike the DOCSIS standards for cable systems, Telco carriers are given a variety of ‘options’ within the scope of IP standards for implementing IPTV with no specific reference point to the functional specification and design yielding the highest level or performance. This gray area can often times be capitalized on by equipment vendors to support and promote designs and architectures that allow them to sell the most equipment, rather than best serve the needs of the IPTV service provider.

From a technology perspective, IPTV appears a complex system and architecture to implement. It requires a digital IP head end system, middleware, conditional access, on demand streaming video servers, access systems, switches and routers along with IP set tops and terminations end points. It is the integration and interoperation of all these elements that constitutes IPTV service deliver, along with other sub-system such as Emergency Alert, Caller ID/TV and ad insertion. From the perspective of the paying subscriber, though, the quality and performance factors for television viewing boil down to a few basic and simple factors. First, how good is the quality of the picture? Second, how fast do channels change and can I always get the channel I want? Third, how reliable is the service availability? And fourth, how much content or programming do I get? The technical bells and whistles behind the service matter like to the end customer, and their choice to maintain the service or discontinue it will usually most often be predicated on one of these four factors.

For the foreseeable future, broadcast television programming is the core service for television viewing. Interactive, on demand ‘push’ based unicast video is growing in use and importance, but unlikely to change the service model near term to where live broadcast television is replaced. Therefore,
multicast video is the main feature of IPTV (and cable) services, with most operators today offering an average of 150 program channels, many as high as 200. In IPTV, broadcast video is controlled and delivered using Internet Group Multicast Protocol, or IGMP. IGMP is also responsible for channel changing with IPTV. The head end content processor, middleware, conditional access system and set tops all use IGMP as the trigger for IP video delivery. IGMP, therefore, has the biggest single influence as well as impact on IPTV service performance and quality.

Within the IP standards adopted for IPTV, IGMP may be used in either a bridged or routed mode for multicast of video streams at the access end. In a bridged mode, the access node performs a Layer 2 snooping function, allowing a device, generally the network router in the core network, to perform the Layer 3 IGMP multicast control and set up/tear down of channels. In a Routed access network, the access node has its own IGMP proxy function built-in. Therefore, multicast control and channel changing occurs at the access node, and is distributed across the network. Both methods are supported fully in standards, and both accomplish the same functions, the difference being where in the network the intelligence and control exists.

Zhone, as part of its open standards platform philosophy, supports both bridged and routed IGMP multicast in its MALC access platform, and has customers using both methods. Although the choice is up to each customer, the customer needs to understand the performance criteria and impacts of each option in order to make the right decision, and this paper is written to offer some comparisons functionally between using bridged and routing for IGMP, along with a clear understanding of performance as networks and subscribers scale. Unlike a number of vendors who support one method, Zhone can offer a neutral assessment since the ultimate choice rests with the customer since both methods are supported.

**IGMP explained**

Internet Group Multicast Protocol, or IGMP, is the method defined in standards for broadcast TV channel changing mimicking a cable system environment in simple form. IGMP is not a new standard, and is a protocol that has been around for some time for use with Internet data. IGMP is normally software feature set used in a core router, designed to allow a central device to send simultaneous sessions to subtending hosts within a specified multicast group. Multicast is performed through a simple join or leave message, notifying the router a host wants to receive a multicast or drop from a multicast. As it applies to broadcast video, a set top, via the remote, sends a join when a channel request is made and a leave when the channel is left. This constitutes a channel change.

IGMP, however, is not an ideal protocol for broadcast video and channel changing since its purpose was not originally intended for this use, but rather adopted for IPTV applications. Its main weakness is that it is a stateless protocol with no means of authentication. The router upstream of hosts has no idea of who sends an IGMP join or leave nor does it keep track of that status of joins and leaves being passed by hosts. This poses several problems for IPTV. First, with no ‘policing’ of joins and leaves, it is possible to have joins and leaves get out of balance due to dropped packets and errors. It is not uncommon to have a leave message dropped and channels (multicast streams) remain active although no longer in use. Imagine a popular channel like ESPN being multicast to a number of subscribers. Several subscribers decide to change channels and the leave request is dropped between the set top and router. ESPN remains stream even though no longer being watched. Over a period of time, rather than being a single instance of ESPN being multicast, there are a number of separate instances being streamed concurrently. Joins are less of an issue, when they are occasionally dropped it results in a channel change not occurring and the subscriber having to push the remote control button again.

The second issue is security of content. IGMP allows no means of correlating a join or leave to a device or subscriber and therefore cannot control who accesses
content itself. Therefore, studios concerned with digital piracy of content fear IPTV using IGMP can allow access to digital content by hackers and thieves. The centralized router is not intended to maintain the proper database to match IGMP requests to individual devices and their authorization to request multicasts.

IGMP implementation is oft times characterized as “It isn’t a problem until it breaks, then I will know I have a problem”. For a carrier, this means lab evaluations and field trial tests of IPTV will generally work well because scalability is not part of the measurement criteria. It may not be for several years, when a significant subscriber base is attained, that the hidden problems of multicast performance come to light. The, the carrier is forced to add more equipment and re-vamp its network to compensate for the performance problems. In the initial implementation stage, factors such as costs or ease of provisioning may direct a decision, with scaling and performance an assumed constant until the problems actually occur.

This is not to imply that every IPTV service provider will have problems or see performance issues. Many Telco’s offering IPTV today are small rural Telco’s who will never reach a subscriber base largest enough to see performance degradation. At the same time, though, performance cannot be quantified based strictly on the number of subscribers, number of set tops, or number of channels. Human factors, such as the sophistication on the subscriber to always use the Electronic Program Guide (EPG) versus ‘channel surfing’ via the remote control can weigh the equation. There are so many permutations that it is almost impossible to develop a set of metrics to determine performance affecting thresholds. Smaller operators may experience problems in many cases, although larger carriers serving more metropolitan markets will most likely be most severely impacted.

**Tracing the roots of IPTV**

Initially, video over phones lines was performed a Switched Digital Video (SDV) using ATM rather than IP. Since no IPTV standards yet adopted, suppliers used a combination of cable standards and proprietary means to build the video system. DSM-CC was used as the channel change protocol.

IPTV has a reputation in the industry as being unpredictable in performance and problematic based on some well publicized failures with early deployments.

When Zhone developed its MALC Broadband Loop Carrier access platform, it too recognized the value of delivering IPTV and controlling it at the access edge. Zhone studied IGMP and concluded that a combination of dense mode multicast with
IGMP proxy would yield optimum performance for IPTV. The notion of distributing multicast at the edge of the network, and controlling it as close to the subscriber as possible seemed to make sense for IGMP in IPTV just as it was proven for DSM-CC in SDV. When the IPTV standards emerged, the easiest path for implementation was Layer 2 IGMP snooping using bridging for multicast, however, and because most access vendors implemented it that way, it was deployed. The notable IPTV failures were largely caused by a combination of this implementation coupled with scaling of the deployment to a point where problems occurred.

To compare performance and scalability, let’s use two customers as acast study. The first, a non Zhone customer using IGMP snooping at Layer 2 bridging. The second (Consolidated Communications Incorporated), a Zhone MALC customer, implementing IPTV using IGMP proxy with Layer 3 routing. The non Zhone customer put in a number of DSLAM’s for triple play, using their core Router to perform IGMP multicast at Layer 3. In lab and field tests, it worked fine, as it did for almost 2 years. But, as they approached 3000 subscribers (with each subscriber having 2 or 3 set tops in the home), suddenly channel changing became unpredictable during peak viewing hours. Instead of a second or less to change a channel, it would take anywhere from 3-6 seconds per channel change. On several occasions, channel changing just stopped entirely. After extensive research and investigation, the problem was traced to the core router, which was the source for initiating all multicast. By design, the core Router has a lot of interfaces (ports) and a great deal of imbedded IP software functions, but a relatively small processor for transactions. IGMP multicast, which involves a series of join and leave commands, tend to build rapidly during peaks, especially if channel surfing occurs frequently.

At some point, the processor filled and began to buffer requests, causing a slowdown in channel changing. As buffers overflow occasionally (usually in peaks), channel changing actually stopped. With the access system and network already in place, the solution rested with the router vendor. The solution was to buy a number of smaller edge routers to co-exist with DSLAM’s at the central office to offload processing on the core router. The core router then had only the edge routers to treat as hosts for IGMP multicast, rather than every set top being the host. This solved the problem, although at significant cost to add a number of video-specific edge routers to resolve the limitation of the DSLAM to only perform IGMP Layer 2 snooping.

CCI, being a larger Independent Operating Company (IOC) serving some fairly dense markets, assumed from the start the DSLAM would serve a fairly large subscriber population, with as many as 500 video subscribers with 3 streams per subscriber per node. When CCI looked at their network, it immediately decided that centralized multicast from a core router was too risky, and service quality required distributing IPTV functionality to the access edge. With Zhone’s MALC supporting both IGMP snooping (bridged) and IGMP Proxy (routed), they have the flexibility to choose they way they wished to implement it. Therefore, MALC’s were provisioned as routed IGMP multicast through IGMP proxy, and their core router was bypassed for support of IPTV. One Layer 2 switch acting as a hub was used between the access and transport network for video. In the 3 years CCI has offered IPTV there has not yet been a problem in scaling service at any node, nor any fluctuations in the levels of multicast performance.

**Bridged Mode multicast**

The advantage of bridged mode, using IGMP snooping at Layer 2 in the access node, is provisioning simplicity. It is a simple process to provision the access node to bridge multicast as a host from the central multicast Router, as the access system itself is a passive participant in the process of multicast. As long as the Router is not overloaded with IGMP requests and buffers them, channel changing works fine and performance is good. And, because the work is done in the Router, access systems do not require extensive intelligence for multicast and therefore less software is needed in its core processing.

Many Telco’s opt for using bridged mode with IGMP snooping because it requires much less complex provisioning than doing routed, and is simple to implement. Since core Routers already exist, it allows utilization of existing assets without extensive network re-provisioning. And many of the small rural IOC’s implementing IPTV today have a small enough subscriber base
to not run into performance problems that larger networks would. MALC supports bridged mode with IGMP snooping and has numerous customer implementations in this manner that have acceptable performance due to the size of the subscriber footprint.

**Routed Mode multicast**

Using Routed mode for multicast requires more extensive and complex provisioning at the access level. Between the Router and access node, each multicast route must be defined and provisioned by IP address. Once done, the central Router no longer handles IGMP requests, and the MALC now becomes the multicast router for IPTV using IGMP proxy. Multicast is no longer controlled from a central point, but controlled on a distributed basis at each access node at Layer 3. The Router performs only simple Layer 2 functions to pass multicast to MALC’s, or a simple Layer 2 switch is used in lieu of the Router.

With the main disadvantage provisioning complexity and managing multicast at each node rather than a central router, there is a number of upside benefits. IGMP proxy allows MALC to maintain multicast in a stateful environment rather than stateless as with bridged and snooping. Using IGMP tables, MALC performs active queries to determine if there are excessive leaves and assure joins and leaves are in balance, the end result being eliminating unnecessary bandwidth residing in the network. Using a provisioned Access Control List, or ACL, each subscriber line has assigned only those IP multicast addresses that subscriber is authorized to receive, therefore eliminating the possibility of pirating channels or programs a subscriber has not paid for. And going a step further, correlating a MAC address for each set top to the subscriber line and insuring that no device other than the one authorized for that line can forward joins and leaves to the network.

In routed mode, MALC can either use dense or sparse mode for multicast if bandwidth is a consideration. In dense mode, all multicast traffic will forward to MALC and IGMP joins and leaves will process at the access node. In sparse mode, new joins will be sent to an upstream Router if the IGMP address for that channel is not present. This allows streaming only the broadcast in use. It differs from IGMP snooping (Layer 2) in that MALC using IGMP Proxy and its query table to determine if a join is an active multicast or initiate a new routed stream from upstream in the network.
Conclusions

Bridged or routed modes can both work for IPTV multicast video services, with traffic and volume determining which is best able to assure a quality level of service. There is no way to quantitatively determine how many subscribers, how large the network or how many streams will cause degradation to bridged IGMP snooping. Too many variables, such as user patterns and peak hour demands play a part, thus it becomes a field performance issue that shows up when a combination of factors cause thresholds to be exceeded. In every deployment, large or small, IGMP multicast is optimized for performance and consistency when routing is used at the access edge with IGMP proxy. The carrier must determine how much risk their deployment faces based on size and scalability, compared to the provisioning and operational impacts distributed IPGMP multicast and routing causes.
It is important, however, to offer carriers the choice to decide. By supporting either bridged or routed IGMP multicast in MALC, Zhone lets the customer decide how it wishes to configure its network. Many access systems and vendors only support IGMP in a bridged mode with snooping since they are merely Layer 2 devices.

Zhone promotes the concept of operator flexibility with a minimum of future investment. MALC allows a carrier to implement IPTV services with multicast in a simple bridged mode and, when subscriber growth or performance requires it, re-provision multicast to routed in either dense or sparse mode. Adding new equipment such as edge routers to offload the centralized core Router is not necessary. Nor making future upgrades to set tops and middleware to support IGMP V3 for distributed multicast in the core network necessary. Re-provisioning MALC merely enables the imbedded IGMP proxy features to operate and create a fully distributed multicast network using the existing network, unlike access systems supporting only bridged multicast as Layer 2 devices that cannot migrate, and therefore force the network to change.

Figure 4: IPTV edge routing functionality