DOI : 10.3745/JIPS.2009.5.1.025

Implementation of Advanced IP Network Technology for IPTV Service

Young-Do Joo*

Abstract: It is absolutely essential to implement advanced IP network technologies such as QoS, Multicast, High Availability, and Security in order to provide real-time services like IPTV via IP backbone network. In reality, the existing commercial networks of internet service providers are subject to certain technical difficulties and limitations in embodying those technologies. On-going research efforts involve the experimental engineering works and implementation experience to trigger IPTV service on the premium-level IP backbone which has recently been developed. This paper introduces the core network technologies that will enable the deployment of a high-quality IPTV service, and then proposes a suitable methodology for application and deployment policies on each technology to lead the establishment and globalization of the IPTV service.

Keywords: *IPTV, Premium Backbone, QoS, Multicast, High Availability, Security*

1. Introduction

IPTV (Internet Protocol TV) is a type of TV service delivered over an IP-based network. Technically speaking, IPTV is defined as a range of multimedia services which converges the realms of telecommunication and broadcasting including television, video, audio, text, data through high-speed internet. The appearance of IPTV is due to multi-service network with broad bandwidth to transmit good-quality of multimedia services. Network convergence combines various single service networks to allow TPS (Triple Play Service; to cover voice, data and video service) and FMC (Fixed Mobile Convergence). For the last decade, broadband convergence with all IP has accelerated to develop the IP premium network which is known as NGN (Next Generation Network) or BcN (Broadband Convergence Network).

Usually, the commercial internet has been evolved for internet-connection service itself, so there are many limitations meeting the unique characteristics of real-time delivery of the IPTV service. The major obstacles to the launch of the IPTV service on the existing internet are the restrictions of the features and performance of the network gears already in use. It would be a considerable risk to add new technological features to those outdated products collectively in terms of network reliability and service. Consequently, the large-scale enhancements of network equipments should be preceded seamlessly. In order to provide such a real-time service as IPTV, the internet backbone requires advanced IP network technology to sustain the required level of QoS (Quality of Service), multicast, high availability and security etc. Recently, new IP backbone networks of premium-standard have been deployed by the major network providers to initiate the IPTV service. Based on network engineering experiments involving the implementation of such underlying technologies and the deployment of the IP premium backbone, this paper introduces the network technologies that are essential to IPTV, as well as the desired method of application and the related policies for each technology.

Manuscript received October 13, 2008; revised December 29, 2008; accepted January 7, 2009

Corresponding Author: Young-Do Joo

This work was supported by Kangnam University Research Grant in 2008.

* Dept. of Computer and Media Engineering, Kangnam University, Yongin, Korea (ydjoo@kangnam.ac.kr, ydjoo910@naver.com)

2. Multicast Implementation

IP multicast is a network technology designed to transmit the same data simultaneously to a group of users without duplication of the data in the way of 1 to N. When an application service of streaming data like broadcasting is provided, IP multicast technology is an effective means of reducing the waste of network resources including routers and servers across the IP backbone network. For example, if 100 subscribers watch the same channel with the existing unicast technique, 100 streams are transmitted. On the other hand, a multicast method transmits a single stream for the group of 100 subscribers. Therefore, the multicast method can significantly diminish not only backbone traffic but also the load of streaming servers. The saving of network resources and the decreases of servers'

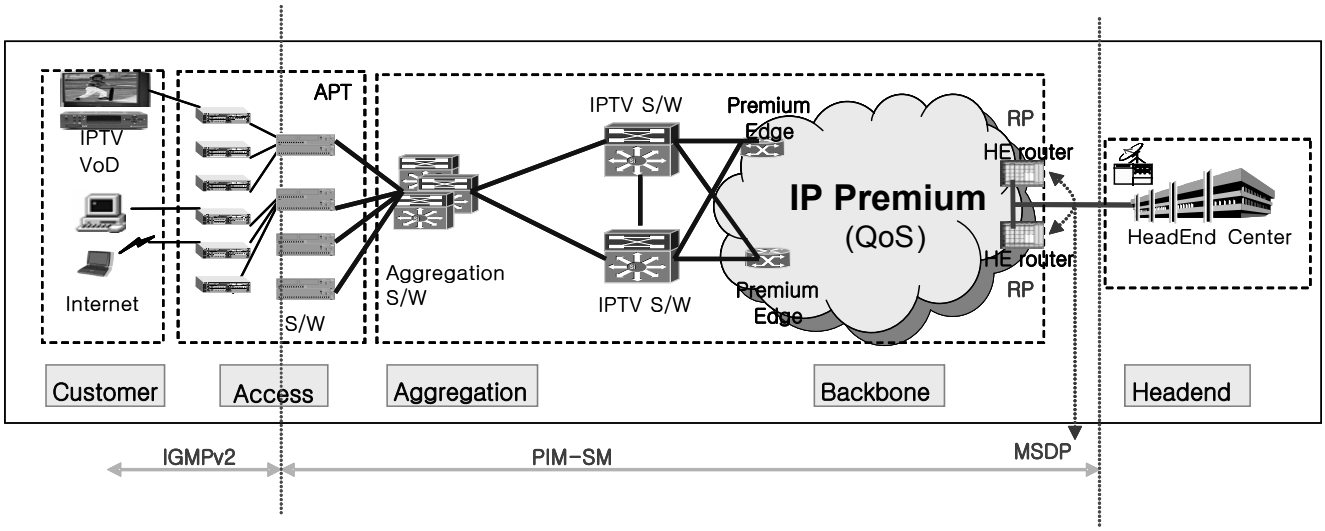

Fig. 1. Deployment of Multicast Protocol

load allow a true multimedia service offer through IP, and will ultimately facilitate the activation of the service.

2.1 Adoption of Stable Multicast Routing Protocol

In order to operate the multicast technology in the IP backbone, the search for stable multicast routing protocols must be considered. As has been proved empirically on field sites for many years, the PIM-SM (Protocol Independent Multicast-Sparse Mode) and the IGMP (Internet Group Membership Protocol) are typically reliable multicast routing protocols available for the IP backbone[1][2]. PIM, as a basic protocol for delivering multicast traffic, generates a distribution tree regarding a multicast traffic path along with multicast routers. PIM is used for a backbone network whereas IGMP is used for an access network to which subscribers are attached. IGMP is used to manage multicast group membership of multicast hosts whether they join or leave any group.

RP (Rendezvous Point) is a linking node between the multicast source and the subscribers. If source is not known for groups, all the routers generate a tree to an RP. If the RP verifies the source from the received multicast traffic, then it sends source join message to the source to yield a source tree[1].

When the number of multicast channels happens to increase, and/or a multicast service is provided to different multicast domains, it leads to an increase in the number of RPs and MSDP (Multicast Source Discovery Protocol) is used to share source active information among RPs. MSDP is a protocol for exchanging multicast source information among RPs, so MSDP peers exchange (S,G) information[3].

However, for well-known source information through the network, receivers may use the SSM (Source Specific Multicast) function instead of PIM-SM RP. SSM sends source information at each multicast router by the static configuration, so receivers can directly send a join message to the source based on the source information acquired by the multicast routers using SSM[4]. SSM requires that all receiver hosts should install IGMP version 3, but some terminals are not yet ready to support it as of today[5].

Fig. 1 depicts the optimal deployment of the previously described multicast protocols in the IP premium network[6]. IGMP is used in the domain of customer side and PIM-SM is deployed in IP the backbone area, and then MSDP is activated between the head-end routers for the exchange of source information. The RPs are marked at the head-end for the deployment since such positioning yields the best performance in various tests as explained in the following section.

2.2 Design of Optimum Multicast Topology

The second technical concern when running multicast in an IP backbone is the design of the multicast topology. As mentioned earlier, an RP is one of the key players in the PIM-SM, so that optimal positioning and the redundancy of an RP should be considered when attempting to provide a reliable multicast environment.

2.2.1 RP Positioning

To minimize service failover time in the event of an RP failure, it is necessary to find the optimal location for the RP. To derive the optimal RP positioning, various test

scenarios were set up founded on the network deployment of the protocol in the previous section. Throughout the test, we derived the correlation between network stability and RP positioning at the point of the link/node failure, and measured the multicast service traffic delay at various RP locations. Based on the information, we obtained the following test results.

- Under the environments to model diverse network topology, no great difference in multicast traffic packet delay by RP positioning was observed.
- As the location of the RP is close to the head-end center, the service failure time by link failure decreased.
- When RP is located close to the head-end, fewer service failures caused by RPF neighbor mismatching during topology looping were observed to occur. Furthermore, it is more efficient from operation and management viewpoint.

Therefore, according to these observations, the head-end router may be determined as the optimal RP position, and hence the multicast network for the IPTV service was deployed and being operated according to this positioning.

2.2.2 Optimal RP Redundancy

When the primary RP fails, all the multicast routers recognize the situation and select a new RP to minimize the service failure time. RP redundancy can be achieved by using dynamic RP selection or static RP selection to involve anycast RP. Dynamic RP is selected by the protocol dynamically whereas static RP is selected by an operator statically. Anycast RP is a means of combining both the dynamic and static cases in which the RP address is set by anycast IP, whereupon RP is selected by the operator.

In particular, the anycast RP method yielded a better test output in terms of operation and management as well as service recovery time, as shown in Table 1.

Table 1. RP Redundancy

Operation/Management	Dynamic RP	Anycast RP
Configuration	Easy	Easy
Troubleshooting	Difficult (Management Overhead)	Easy
Service Recovery Time	Max. 3 min.	Under 1 sec.
Others	Interoperability Issue	Needs MSDP

2.2.3 Multicast Load Balancing

As even the major router vendors do not support completely Equal-Cost-Load-Balancing features that are suitable for multiple PIM join groups, it may be a serious problem with respect to link efficiency across the network.

In the case of multicast load balancing for the same group with multiple sources, identical traffic occurs from multiple sources of the group. This situation may bring about the duplication of multicast traffic at a single PIM router without having an impact on the service. It is possible to provide multicast traffic load balancing by distributing different groups to multiple sources. The multicast load balancing issue needs to be considered along with that of multicast source redundancy.

2.3 Multicast Address Policy

In order to share numerous contents for multicasting among the IPTV service providers, it is required to use a globally unique multicast address or another address translation scheme to enable multicast channels to interoperate with one another. Recommendations have been made by the international organizations and the standard bodies responsible for multicast address issues[7].

- References on the multicast address assignment
  - IANA allocation of the class D address[8]
  - Information on multicast address definition[9]
    RFC 3180 range (GLOP addressing in 233/8)
- Conforming to the references above, the multicast address policy can be defined as follows:
  - 239/8: Used as a site-local address only.
  - 233/8: Defined as a globally routed private address. Every public AS can be translated into one C-class GLOP address[10].
    Ex) KORNET AS 4766 case: 233.18.158.0/24
    Ex) Other AS number 5662 case: 233.22.30.0/24
  - According to the appropriate agreement among networks to allow multicast, RFC3138 (Extended Assignments in 233/8) and RFC2365 (Administratively Scoped Block) can be used.

2.4 Multicast Routing Policy for Network Interoperability

PIM, MBGP (Multi-protocol Extensions for BGP-4), and MSDP are normally used as a multicast routing protocol in the case of network interoperability among multicast network providers. When PIM is applied to network interoperability, the previously introduced policy

and multicast security policy, which will be discussed in a later section, can be referred to. The interoperability policies concerning MBGP and MSDP will be described in the following sections.

2.4.1 MBGP Interoperability Policy

Usually, the use of MBGP is recommended among multicast domains in order to advertise RPF checks and multicast source information[11]. Since MBGP delivers unicast information such as BGP, the principal policy used for BGP peering can also be applicable.

- Advertisement of summary information among service providers
  Summarized information should always be advertized among ISPs using a method like CIDR. Systematic and hierarchical address assignment must be a prerequisite to this end.
- Route filtering policy
  ISPs which receive the summarized information should apply filtering policies to the following routes so as to prevent certain routes from leaking out information inside their own network.
  - Default information (0/0)
  - Private addresses (RFC 1918 range)
  - All Multicast groups (224/4)
  - IP address range of an ISP that receives the information.
- AS path filtering
  Normally, the MBGP peer only permits its direct ISP's AS number, and does not accept a third party's AS numbers connected to the direct peer. However, it is possible to negotiate the transit boundary between peers.
- Maximum prefix limitation
  In reality, routers have some limit on the number of prefixes to process due to performance, and a service failure can occur when they exceed that limit. In order to avoid such an undesirable situation, there should be a certain restriction associated with the number of prefixes which MBGP peers are able to accept, and such a limitation needs to be determined by mutual agreement at the time of interoperability.
- MD5 (Message-Digest algorithm5) authentication
  MBGP peers should prepare against DoS (Denial of Service) attacks by adopting MD5 authentication.

2.4.2 MSDP Interoperability Policy

MSDP enforces the RP to exchange SA (Source Active) messages within one multicast domain or between different domains. An MSDP SA message is composed of a pair of multicast sources and a group address. The origin RP initially creates an SA message and then advertises it to the MSDP peers. SA messages can include bogus or false information. Consequently, it may cause unnecessary resource usage and multicast service failure. In order to prevent such a problem, the following reserved address blocks of multicast are recommended to apply filtering to both the sender and the receiver. In other words, these address blocks are not interoperable among the different network providers.

- Domain-local multicast applications: limited in an identical multicast domain without any interoperability between different domains.
- Auto-RP groups: reserved for Cisco auto RP
- Administratively scoped groups (239/8): limited for local use.
- Default SSM range (232/8): assigned by IANA for source specific multicast for IPv4.
- Loopback addresses (127/8): reserved for loopback.
- Private addresses (RFC1918 range): defined as private IP addresses.

3. High Availability

IPTV services consist of applications which are sensitive to packet loss, delay and delay jitter. IP QoS technologies are indispensable to achieving a high-quality IPTV service, and the successful accomplishment of quality guaranteed depends on the reliability of a network. That is, to provide an IPTV service, the IP backbone network has to guarantee high availability with perfect operability and thus to offer a seamless IPTV service in the event that a single system or link goes down.

3.1 Importance of High Availability

It has been defined that IP QoS such as Diffserv is the narrow-sense technology and HA (High Availability) is the wide-sense technology in the context of the guarantee of quality.

Certainly, IP QoS technologies may be a part of the technical implement to secure HA. Fig. 2 shows the causes and percentages of failure of worldwide major ISP networks. 86% of the total failures are due to link failure, router failure and router operation. What is surprising is that the level of failure caused by traffic congestion is just 5%. In attaining the goal of delivering a high-quality IPTV

service, HA technology is far more crucial than IP QoS technology closely where the issues of traffic control are concerned.

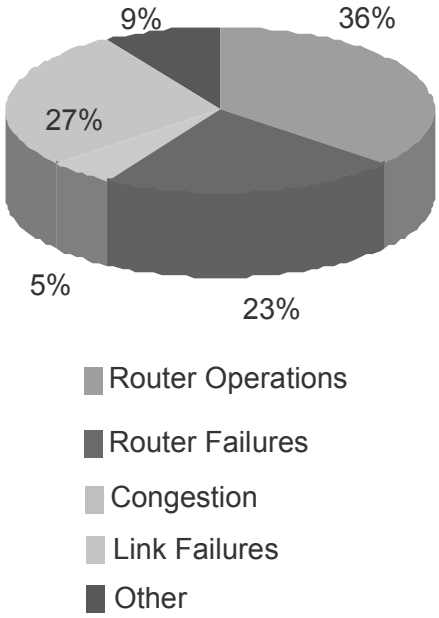

Fig. 2. Causes of Network Downtime
(Source: University of Michigan)

3.2 High Availability Policy

With respect to the causes of failure described in the previous section, we may classify the six major causes of network failure and then devise a corresponding solution for each one of the causes.

The first classified cause of failure concerns human error with regard to network operation and management. To prevent this type of error, ISPs have to set up the standard configuration and operation process and educate operators to be familiar with these standards. In particular, ISPs should offer their operators an intensive training program on IP Multicast and MPLS (Multi Protocol Label Switching) technologies, which are the core technologies of the IP backbone network for IPTV services.

The second cause is router failure, namely the breakdown of network gear. There are no routers without faults. Common modules for the router such as the routing processor, power module and fans must have a redundancy module. Furthermore, these modules should operate an active-active mode or an active-standby mode. The failure on a single module should not cause the whole system to fail. Also, it is necessary to provide a graceful restart function for the routing protocol such as IGP, BGP, and PIM. With a graceful restart function, the service outage time could be minimized in cases of routing processor failure.

The third cause is link failure, which is common to most of ISP networks. Even under an environment equipped with fully redundant topology to prevent a single point of failure, some packets are still lost during the network convergence time. As a solution, Fast-IGP convergence or MPLS fast-reroute mechanism is required to minimize the packet loss.

The fourth cause is service degradation or system failure brought about by traffic congestion. To resolve traffic congestion, the implementation of QoS function such as Diffserv is compulsory. ISPs should provision their network with the basis of CoS (Class of Service) and prepare sufficient bandwidths to satisfy the requirements of each class. A traffic engineering technique for traffic management could also be used if necessary.

The fifth cause is failure resulting from DDoS (Distributed DoS) attack**.** ISP routers are the main target of a DDoS attack. As such, these routers should be able to endure a variety of abnormal DDoS attacks and have the appropriate methods to protect their resources from such attacks. These methods include uRPF (Unicast Reverse Path Forwarding), which applies MD5 to routing protocol and filters unnecessary packets towards routers. Concerning for the security recommendations and continual update should be accompanied.

Finally, the sixth cause concerns failures in the customer device**.** Customer devices are located in the blind spot of the ISP. A managed-type service for customer devices and well-designed customer terminals (i.e., modem or set-top box) are required for the purpose of simple control.

For reference, Static IGMP Join could be used to secure the HA of an IPTV service. Static Join is a technique that always pulls the IPTV traffic closer point to the customer. Static Join can minimize the channel zapping time and the service outage time caused by router failure. But as mentioned above, IPTV traffic is streaming to the static join point even if no user joins that channel. Therefore, the usage of a broader bandwidth and the consequential increase in the cost should be taken into account when designing the network.

4. IPTV QoS Implementation

Recently, network service providers have sought to provide voice, data and video services over a single IP Backbone. As mentioned earlier, the implementation of High Availability should precede the application of IP QoS technology as a priority in order to provide an acceptable and uninterrupted IPTV service.

IP QoS revolves the techniques of protecting IP traffic even under a situation of severe traffic congestion. Diffserv (Differentiated Service) technology is the most feasible

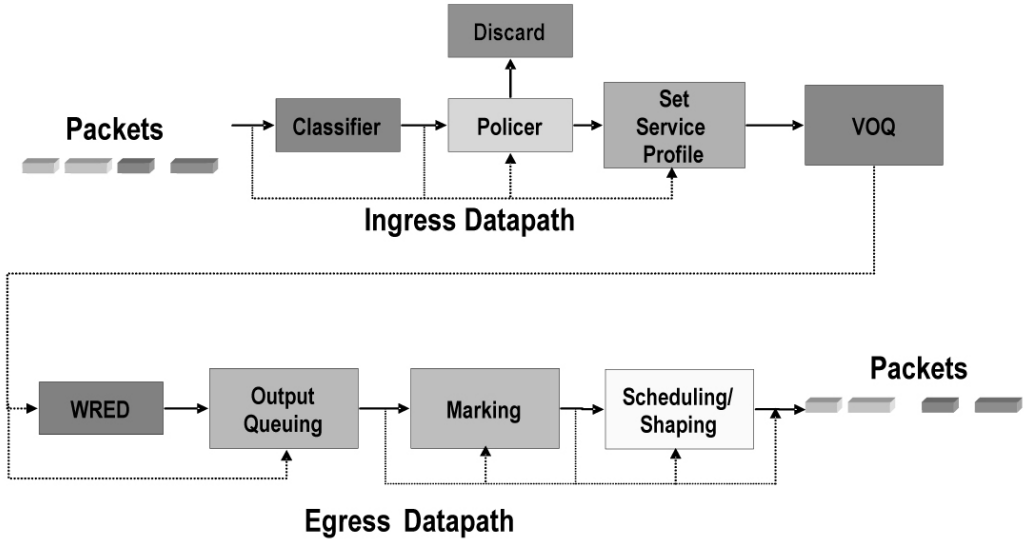

Fig. 3. IPTV QoS Process Procedure

way to provide IP QoS[12][13]. The realization of Diffserv features across the IP backbone depends on the precise implementation of PHB (Per Hop Behavior) according to each class of service. It is necessary to control the bandwidth of each service class, which is the mechanism for handling the congestion.

4.1 Implementation of Diffserv

Diffserv implementation for IPTV QoS starts from packet classification for injected traffic at the ingress interface. In an access network, each router classifies every packet with the information of the IP header or the TCP/UDP header based on the QoS policy, and then assigns the IP precedence bit to each packet. In the backbone network, each router classifies every packet with an IP precedence/MPLS experimental bit based on the QoS policy for the fast packet forwarding.

As the next step, the differentiated PHB rule is assigned to each service class. There are two types of PHB actions: congestion management and congestion avoidance. Queuing and scheduling techniques can be used as congestion management features, while shaping or policing techniques can be used as congestion avoidance features.

To properly implement Diffserv, it is necessary to decide on detailed parameters for each of the Diffserv technologies; for example, minimum and maximum values of bandwidth per class, queue size per class, and the threshold value for RED (Random Early Drop) are the fundamental parameters of Diffserv technology. Those parameters should be determined by considering the injected traffic volume, the type of router and each router's queuing mechanism.

In particular, traffic volume is the decisive factor in setting up Diffserv parameters; hence a measure for monitoring the volume of each service class's traffic should be embodied. Fig. 3 illustrates IPTV QoS processing procedure. When packets come in, they are classified by the classifier process. Then, the policer determines whether to discard each packet, while the service profile assigns the policy on the packets and hand-over to the out-bound side. The algorithm such as WRED determines the packets to be dropped at congestion time and transfer them to the output queue and then, finally the packets go out through the process of marking and scheduling.

4.2 Example of Diffserv Implementation Policy

Table 2 summarizes the Diffserv technology implemented in the MPLS-based IP Backbone. At the ingress interface, the classification of each service class based on the IP precedence/MPLS experimental bit is needed and if necessary, queuing can be used for the ingress interface. At the egress interface, queuing and shaping technology should be provided based on the Backbone QoS policy, and the remarking of the IP precedence/MPLS experimental bit should be also followed.

Table 2. Diffserv Implementation Policy

IP Backbone Router	QoS Policy
Ingress Interface	- Prec/Exp based QoS Classification, - Queuing, if necessary (ex. VOQ)
Egress Interface	- Queuing(ex. MDRR/WRED) - Stern Shaping - EXP & ToS Remarking based on Backbone Policy

5. Network Security

5.1 Network Security Policies

For a real-time service such as the IPTV, service providers should ensure stronger protection against unauthorized access to their backbone network and network-accessible resources. Additionally, network-accessible resources have to meet integrity, confidentiality and availability so that a stable service is offered. Various security features should be considered to provide reliable IPTV services. The scope of such network security includes user and router access control, server security, and security device management etc.

First of all, an AAA (Authentication, Authorization and Accounting) function is used to allow user access control. A secure connection such as SSH (Secure Shell) and a banner message is used to prevent illegal connections. MD5 authentication is used between neighbors to improve the reliability of the routing protocol. uRPF (Unicast Reverse Path Forwarding) is used at the edge routers to prevent source spoofing attacks. Moreover, service providers should install other security functions to protect network resources against well-known DoS attacks.

5.2 Multicast Security Technologies and Policies

TPS services over the IP backbone call for distinct security policies for each service. In particular, attacks aimed at utilizing multicast with malicious intent may bring about critical effects in the whole network suddenly. Accordingly, multicast security policies applicable to the features of multicast and the network architecture are required[14][15].

First, in the access network, all kinds of multicast traffic with the exception of IGMP join packets should be denied to subscribers. In other words, multicast source spoofing is blocked out from the customer's device of L3 starting point. Second, at the PIM routers, MD5 authentication should be enabled between PIM neighbors. Useless BSR messages from entering and exiting in the multicast domain are filtered out and the TCP/ICMP message that belongs to 224.0.0.0/24 should be denied. From the perspective of multicast router stability, the number of multicast routes to be added in a router should be limited.

Finally, the RP should provide specific filtering functions to improve the security of the network as follows.

- The filtering for the MSDP SA message focuses on each peer, source and instance.
- To prevent unauthorized multicast source registering, the RP should enable PIM register message filtering so that only approved sources can register with the RP.
- The RP should employ group range filtering so that only an approved group range can register with the RP.

6. Conclusion

This study proposes essential network technologies and optimal implementation policies aimed at the provision of a high-quality, stable IPTV service based on various network engineering tests and deployment experiences with the IP premium backbone. Through an extensive application of the network technologies described in this paper, a more sustainable IP backbone to provide the IPTV service could be developed and consequently, the incorporation of all IPTV systems would be accelerated with other constituent technologies including IPTV platforms and customer devices.

First of all, IP network infrastructure supported by robust multicast and QoS mechanism would be a forefront jump-starter to drive IPTV service successfully and to resolve other hot issues; i.e. the differentiation of service contents, marketable service bundling/packaging and competitive pricing. Eventually, network and service providers might not only reduce the costs of network deployment and operation but also settle imminent IPTV technicalities under the evolution phase to open a wireless and mobile IPTV era in the near future.

References

[1] B. Fenner, M. Handley, H. Holbrook and I. Kouvelas, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC4601, August 2006.

[2] W. Fenner, "Internet Group Management Protocol (IGMP), Version 2", RFC2236, November 1997.

[3] B. Fenner and D. Meyer, "Multicast Source Discovery Protocol (MSDP)", RFC3618, October 2003.

[4] S. Bhattacharyya, Ed., "An Overview of Source-Specific Multicast (SSM)", RFC3569, July 2003.

[5] B. Cain, S. Deering, I. Kouvelas, B. Fenner and A. Thyagarajan, "Internet Group Management Protocol (IGMP), Version 3", RFC3376, October 2002.

[6] IPTV Network Topology, KT Corp., August 2007.

[7] Z. Albanna, K. Almeroth, D. Meyer and M. Schipper, "IANA Guidelines for IPv4 Multicast Address Assignments", RFC3171, August 2001.

[8] IANA Allocation of Class D Address, "http://www.iana.org/assignments/multicast-addresses".

[9] Information on Multicast Address Definition, "http://www.ietf.org/internet-drafts/draft-ietf-mboned-addrarch-01.txt".

[10] D. Meyer and P. Lothberg, "GLOP Addressing in 233/8", RFC2770, February 2000.

[11] T. Bates, Y. Rekhter, R. Chandra, and D. Katz, "Multiprotocol Extensions for BGP-4", RFC2858, June 2000.

[12] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss, "An Architecture for Differentiated Services (Diffserv)", RFC 2475, December 1998.

[13] D. Grossman, “New Terminology and Clarifications for Diffserv”, RFC3260, April 2002.
[14] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
[15] T. Hardjono and B. Weis, "The Multicast Group Security Architecture", RFC3740, March 2004.

Young-Do Joo
He gained his M.S. degree in Computer Engineering from University of South Florida in 1988 and his Ph.D. in Computer Science from Florida State University in 1995. He is currently an associate professor in Department of Computer and Media Engineering at Kangnam University. During 1995~2000, he worked as a senior researcher for KT Telecommunication Network and Multimedia Research Lab. He led the research and technology business in ISP at Cisco Systems during 2000~2005. He joined Huawei Technology as a senior executive director in 2005. His research interests include Broadband Convergence Network, Future Internet, VoIP, IPTV, Wireless & Sensor Network, Network Management, Intelligent Systems and Knowledge-Based System.