

IGAP : IP Multicast Management Protocol that can collaborate with User Authentication

Akihiro Tanabe[†], Daisuke Andou[†], Kaori Izutsu[†],
Tsunemasa Hayashi[‡] and Hiroshi Tohjo[‡]

[†]NTT Access Network Service Systems Laboratories
Email: {atanabe, dandou, izutsu}@ansl.ntt.co.jp

[‡]NTT Network Innovation Laboratories
Email: {hayashi.tsunemasa, tohjo.hiroshi}@lab.ntt.co.jp



Abstract

It is important to create broadband network services that will popularize new broadband content like video stream distribution on IP rather than traditional Internet applications. The IP multicast architecture can be used to distribute broadband content, however, it has been considered difficult to add to it a user authentication and accounting mechanism.

IGAP (Internet Group membership Authentication Protocol) allows the user authentication and accounting mechanism to be added to multicast group services. IGAP is based on the architecture of IGMP, and transfers information for user authentication and accounting. We implement this protocol in multicast routers and user client equipment, and confirm that it operates correctly.

Keywords

content distribution, IP multicast, IGMP, user authentication, accounting

Introduction

[What do we want to achieve?]

Provide New Content Service for Broadband IP network
(using xDSL, fiber optic network, ...)

[Viewpoints]

- Network should be able to transfer many broadband contents.
--> **CDN with IP Multicast**
- Service providers should strictly manage the data of their users.
- Per content accounting mechanism should refer to the access data of users.
--> **No mechanism available**



IGAP
(Internet Group membership Authentication Protocol)

1. Introduction

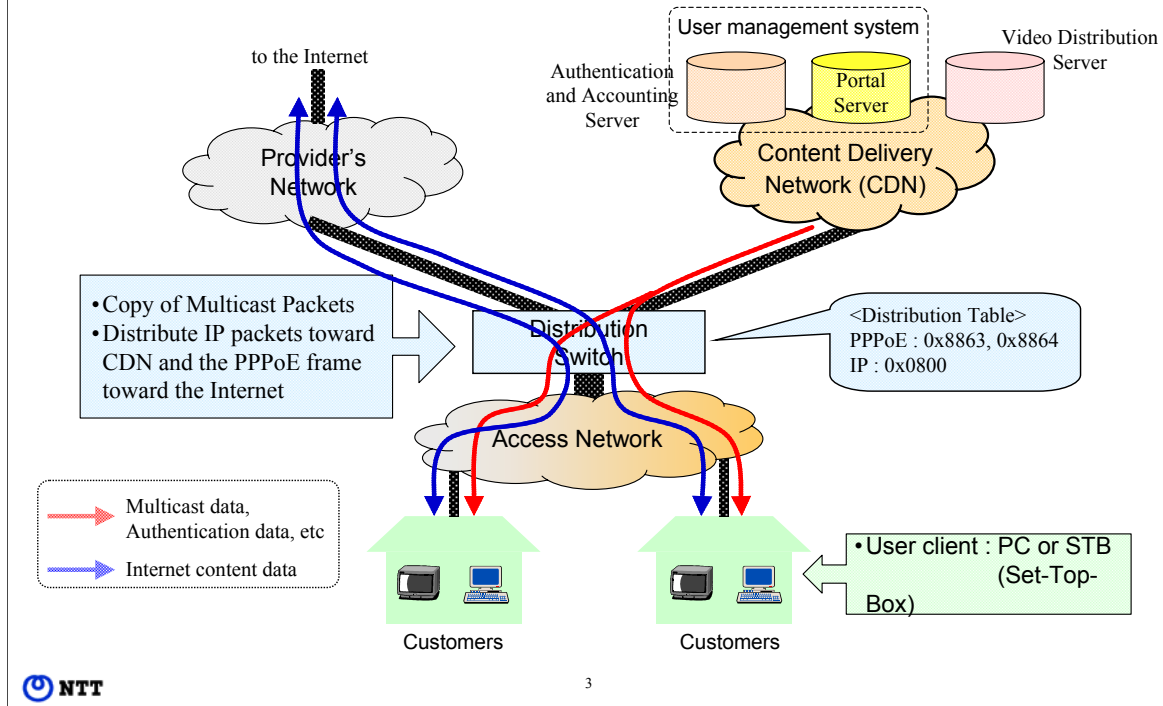
Broadband access architectures for customer network service, e.g., optical fiber line, are becoming very popular. Many content services are provided on the Internet, i.e. IP architecture, using the high-speed access lines. Most are already well-known and used by many customers, so service providers are looking for new content services. As an example, real-time video distribution on the IP network, image quality rivals the of digital broadcast content, is being tried.

To deliver such new content, it is important to keep provide constant network bandwidth for stable distribution. The IP multicast architecture can be used to transfer content to many customers. The content delivery network (CDN), built separately from the Internet, prevents the bandwidth instability caused by other burst traffic in the Internet. So this research assumes that CDN is used to support the IP multicast architecture. User-client employs IGMP[1] to receive IP multicast packets.

In pay content services, user authentication and accurate accounting per content are essential to prevent access by customers who are subscribers, and to charge correctly. There are some user authentication mechanisms in actual service. RADIUS[2][3] or HTTP are the dominant mechanisms. In most pay content services, these mechanisms are independent of network management, and it is difficult to manage the transfer of multicast data by collaborating with the authentication and accounting mechanism. If user management data like authentication and accounting could be accessed from the network layer, more adaptable services would be become possible.

We solve this problem by proposing a protocol for the management of IP multicast. It is based on IGMP architecture, and tightly integrates the user authentication and accounting mechanism. It is named IGAP (Internet Group membership Authentication Protocol). In this paper, we present the IGAP architecture and an implementation of multicast routers and user-client machines, and report upon their performance.

Assumed Network Environment



2. Network Environment

We assume that the CDN services provide real-time video contents encoded in MPEG2 at about 6Mbps. The distribution of high quality video content is expected by Internet Service Providers (ISP) to be a killer broadband network service.

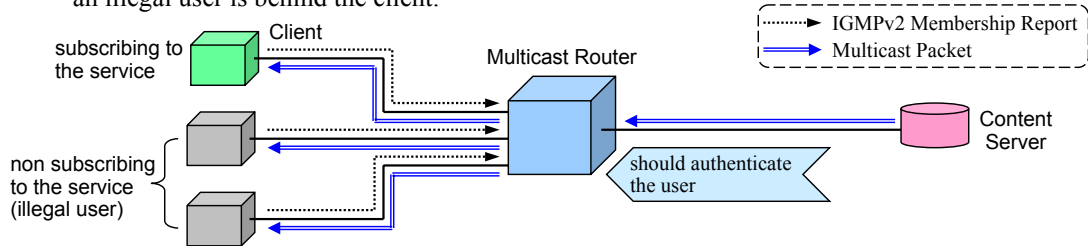
This figure shows the network environment of this service model. The multicast packets containing video content are copied by the Distribution Switch, and are transferred to user clients[4]. Customers use PC or STB (Set-Top-Box) as the user-client. The STB receives IP packets and displays the video on TV. User-clients keep sending the requests of IP multicast, e.g. IGMP membership reports.

The video content must have high quality, so it is generally believed that End-to-end QoS management will be used. But this may be difficult to establish given service providers will try to differentiate themselves by offering different QoS levels. Accordingly, we assume that the core network is separated into the CDN and the provider's network. The provider's network connects to the access network and the Internet. The Distribution Switch differentiates the frames for CDN services and those for Internet Access. The value of the Ether Type field in Ethernet frames can be used for this. PPPoE[5] is normally used to connect to the Internet. When the Distribution Switch receives a frame via the access network, it checks the Ether Type value in the frame, if the value is the defined number of PPPoE, i.e. 0x8863 or 0x8864, it transfers the frame to the provider's network. Other frames are transferred to the CDN.

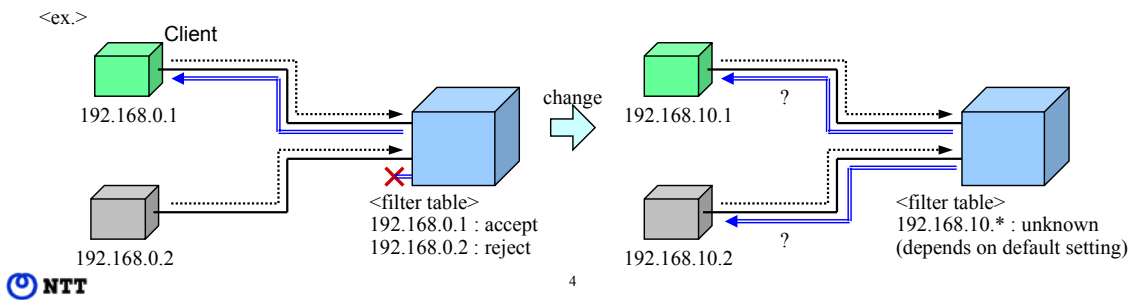
The CDN will host many servers that will provide Video content, program guides, user authentication, accounting, and other functions. A core set such as user authentication server, accounting server, program guide server will be integrated into some form of management system. The management system is implemented as software, and minimizes the administrator's workload in actual service.

Current Situation in IGAP development

Any client sending IGMPv2 Membership Report can join a multicast group, even if an illegal user is behind the client.



Filtering by IP address is not sufficient, because IP address of clients may be changed for every connecting to network.



3. IGAP (Internet Group membership Authentication Protocol)

3.1. Background to the development of IGAP

IGMP is the protocol used to join and manage multicast groups. But its mechanism is lacking in important process for secure access. IGMP makes any user join to multicast group if only they send IGMP Membership Report. For example, in a video distribution service with IP multicast using IGMP, some users may be able to watch the video content, even if they are not subscribers. So, user authentication mechanism should be used with the IGMP. In actual service, it's obvious that content data will be encrypted and only subscribers will be able to decrypt the data. But using only encryption is not enough. We note that even though the non-subscribers can't watch the video, they are still receiving the data packets, and this may trigger unwarranted charges. It is better to prevent the data from being sent to the non-subscribers.

If the multicast router used some filtering mechanism based on IP address, the multicast packets could be blocked from being received by the non-subscribers. Unfortunately, user IP address allocation may not be stable, and IP address change with every connection if DHCP or a similar mechanism is used. Moreover, accounting should not depend on IP address.

Our approach is to develop a new management protocol for IP multicast. The new protocol has the following functions.

- recognition of the user requesting to join a multicast group by not IP address but by user specific parameters (user-ID, password, etc)
- accessing the user authentication and accounting mechanism using those parameters
- effectivity for integrated service management system in actual service (described in Section 2.)

Summary of IGAP

- IGAP is based on IGMPv2, and works with user authentication and accounting mechanism. So users accepted by the multicast group can only receive the content data by IP multicast.
- Router implementing IGAP sends user authentication (accounting) data to authentication (accounting) server, and sends message about result of authentication and accounting status (start or stop) to user-client joining multicast group.
- IGAP can check whether the user is accepted for accessing the multicast group while receiving the multicast packets (re-authentication).
- Leave process of IGAP differs from that of IGMP. IGAP leave process is designed to lower the delay upon changing multicast content (such as changing TV channel).

3.2. Summary of IGAP

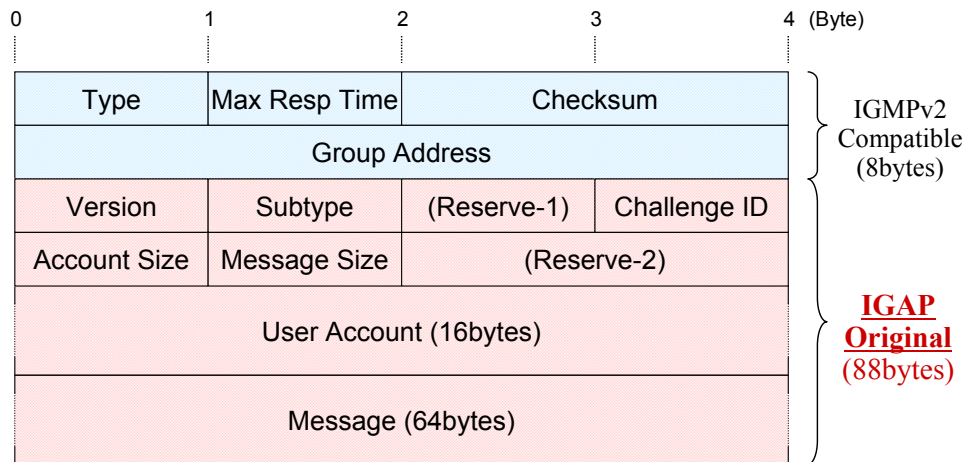
The new protocol is based on IGMPv2, and works tightly with the user authentication and accounting mechanism. The key to this is the its parameters support user authentication and accounting. The protocol is called IGAP (Internet Group membership Authentication Protocol). IGAP is at an advanced stage of standardization in IETF.

IGAP is used between user-client and router. The Multicast Router that implements IGAP (IGAP Router) not only copies the multicast packet but also authenticates the clients. When the IGAP Router receives an IGAP request packet for joining a multicast group, it sends user authentication data to the authentication server, e.g. RADIUS server, and then transfers the requested multicast packets if the user is accepted. In addition, the IGAP Router sends the data for accounting purposes, such as start time of receipt, to the accounting server. Note that the RADIUS server can also provide the accounting service. If access is rejected, multicast packets are not transferred to the client. While IGAP allows the functions of multicast copy and client authentication to be implemented on different routers, the two routers must be deeply associated and delay would be come a serious problem. Thus it is better for one router to implement both functions.

IGAP checks whether user access is still accepted during the multicast service. This re-authentication coincides with a query process like IGMP. Re-authentication is used when delivered content is changed with the same multicast address like TV programs, and authentication for receiving changed content is needed.

The leave process of IGAP differs from that of IGMP. IGAP leave process is designed to minimize the delay experienced when changing the multicast content being received (such as changing the TV channel). This mechanism is called the Fast Leave against IGMP leave process. Fast Leave is effective for zapping, i.e. changing of receiving content hurriedly. Fast Leave can send accounting stop message faster than leave of IGMP, so the duration of connect is more correct and it's effective for billing.

IGAP Header Format



- Challenge ID : the parameter for encryption of password by Challenge-Response mechanism
- User Account : the parameter to indicate the user name
- Message : the parameter for authentication, e.g. password

<http://www.ietf.org/internet-drafts/draft-hayashi-igap-02.txt>



4. IGAP specifications

4.1. IGAP header

This figure shows the IGAP header. This header and parameters are described in the latest draft.

In this header, the format of the upper 8 bytes equals the IGMPv2 header format. Type field stores one of the following values.

- 0x40 ; IGAP Membership Report (also called IGAP Join)
- 0x41 ; IGAP Membership Query (also called IGAP Query)
- 0x42 ; IGAP Leave Group (also called IGAP Leave)

The details and usage of these types are described later.

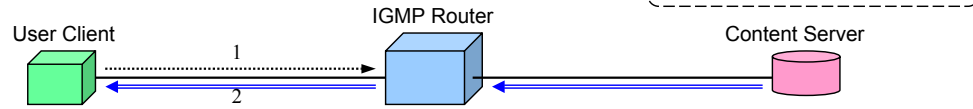
The format of the lower 88 bytes is specific to IGAP. The fields are described as follows.

- “Version” is set to 0x10 to indicate IGAP version 1.
- “Subtype” indicates the identification of the message transferred in the IGAP packet.
- “Challenge ID” is meaningful only when Challenge-Response authentication is used, and the value depend on the Challenge-Response protocol like CHAP[6]. If this field is not used, the value is 0x00.
- “Account Size” indicates the valid length of the “User Account” field (in units of bytes).
- “Message Size” indicates the valid length of the “Message” field (in units of bytes).
- “User Account” contains the user’s identification word, e.g. name.
- “Message” contains certain information for authentication, e.g. password.
- “Reserve-1” and “Reserve-2” is not used now.

IGAP Join process

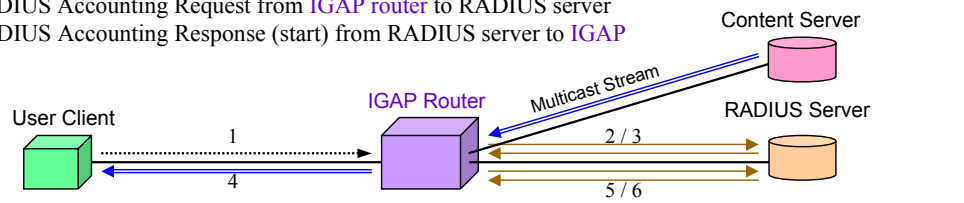
[Join multicast group using IGMPv2]

1. Send IGMPv2 Membership Report from user client to IGMP router
2. Start to send multicast packets from IGMP router to user client



[Join multicast group using IGAP]

1. Send IGAP Join from user client to IGAP router
2. Send RADIUS Access Request from IGAP router to RADIUS server
3. Send RADIUS Access Accept from RADIUS server to IGAP router
4. Start to send multicast packets from IGAP router to user client
5. Send RADIUS Accounting Request from IGAP router to RADIUS server
6. Send RADIUS Accounting Response (start) from RADIUS server to IGAP router



7

4.2. IGAP sequence

4.2.1. Join process

This figure shows an example of the process used to join a multicast group using IGMPv2 or IGAP. As stated earlier, IGMPv2 does not have any function to identify users, so any user client sending an IGMPv2 Membership Report can receive multicast service requested.

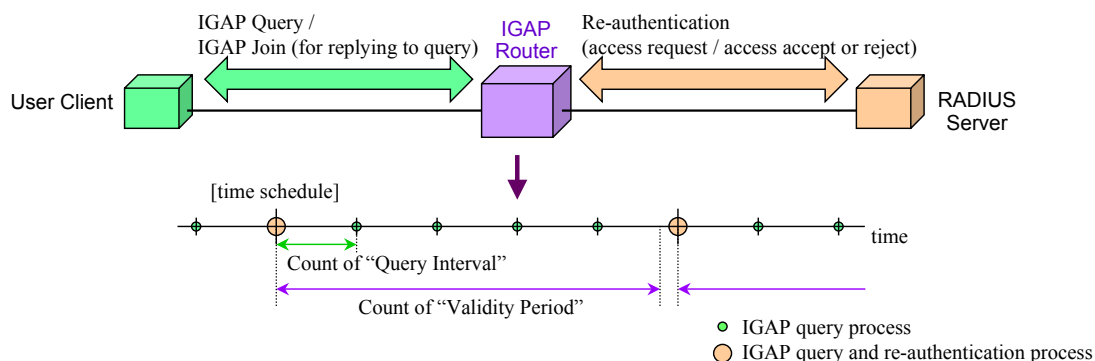
In contrast, the joining mechanism of IGAP implements user authentication as follows. In the example shown in this figure, the RADIUS server performs authentication and accounting.

- User client sends IGAP Join packet to IGAP Router. If Challenge-Response authentication is used, the process for requesting Challenge ID and replying is added.
- The process for user authentication, executed between IGAP Router and RADIUS server, uses the identification user account and password, or some unique parameters.
- When IGAP Router receives the Access Accept for the user from RADIUS server, multicast packets are transferred to the user-client. If IGAP Router isn't currently receiving the multicast packets via CDN, it sends a request packet for the multicast data using IGMP, PIM, or similar protocol.
- IGAP Router sends the Accounting Request to RADIUS server. The message indicates start for client billing. (This is not always sent, IGAP Router selects either sending or not.)

In IGAP Join (Type value 0x40), there are three Subtypes as follows. Every IGAP Join packet is sent from user client to IGAP Router.

- Password Mechanism Join (0x02); The data of message field is encrypted by a password mechanism like PAP[7].
- Challenge-Response Mechanism Join Challenge Request (0x03); This is a request packet for Challenge-Response authentication.
- Challenge-Response Mechanism Join Response (0x04); The data of message field is encrypted by Challenge-Response authentication mechanism.

IGAP Query process and Re-authentication



[Query Interval (same as IGMPv2)]

This is interval for resending IGAP Query packet. When the timer of Query Interval expires, IGAP Router sends a Query and restarts the timer.

[Validity-Period]

This is interval to re-authenticate user, RADIUS server tells the value to IGAP Router. When the timer of Validity Period expires, IGAP Router sends the packets for re-authentication after IGAP Join received in reply to next IGAP Query.



4.2.2. Query and re-authentication process

IGAP has a query process which is similar to that in IGMPv2. The interval between IGAP query packet sending is given by Query Interval. The usage of this parameter basically equals that in IGMPv2.

In addition, IGAP has the function of re-authentication. The Validity Period sets the interval between the packets sent by IGAP router to the authentication server for re-authentication. The value is usually defined by authentication server and sent with the accept packet of user access to IGAP Router. IGAP Router can check whether the user joining to the multicast group is fair by this mechanism.

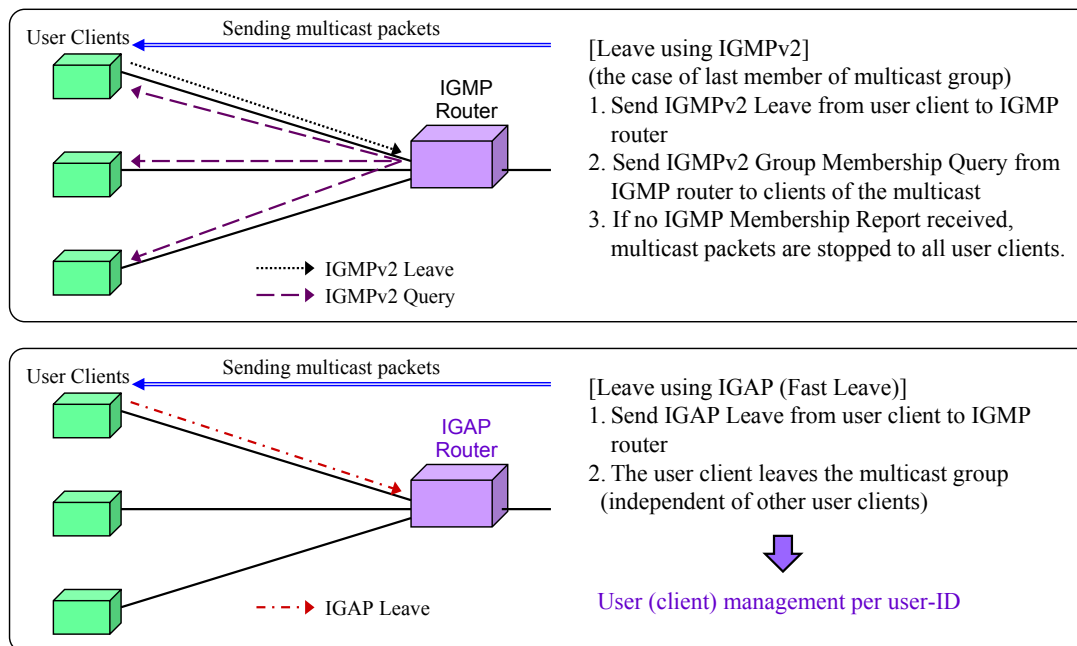
This figure shows the time line of the query process and re-authentication of IGAP Router. When the timer of Query Interval expires, IGAP Router sends IGAP Query packets to all user clients. In a certain multicast group, if no user client sends an IGAP Join packet in reply to the query, IGAP Router drops all users from the multicast group.

When the Validity Period timer expires, IGAP Router sends authentication data packet to RADIUS server after the query process. Re-authentication process is equal to the first authentication process. IGAP Router can also send the accounting data of the user to accounting server after re-authentication. In this case, the authentication server updates the user's accounting data following the accounting data sent from IGAP Router.

In IGAP Query (Type value 0x41), there are four Subtypes as follows. Every IGAP Query packet is sent from IGAP Router to user clients.

- Basic Query (0x21); This is a query packet like IGMPv2.
- Challenge-Response Mechanism Challenge (0x23); This sends Challenge-ID of Challenge-Response authentication.
- Authentication Message (0x24); This indicates accept or reject of user access.
- Accounting Message (0x25); This indicates start or stop of user account.

IGAP Leave process



4.2.3. Leave process

This figure shows examples of the processes used in IGMPv2 and IGAP to leave a multicast group. When the user-client sends an IGMPv2 Leave packet to explicitly leave a multicast group, the multicast router sends query packets to other clients in the same multicast group. If the multicast router does not receive an IGMP Membership Report from any client, multicast packet transmission is stopped to all user-clients.

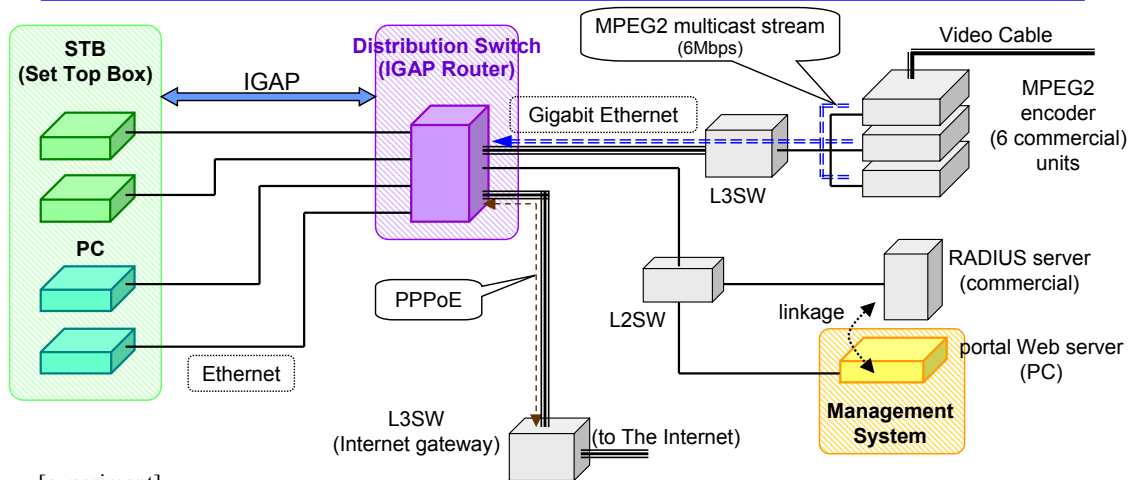
The leave process in IGAP differs from the process in IGMPv2. When IGAP Router receives an IGAP Leave packet from a user-client, it stops sending multicast packets to the user-client without sending query packets. This means that management of the leave process is on a user basis. This is called the Fast Leave process. IGAP Router can send the request packet to stop user billing as soon as it stops multicast packet transmission, so the accounting log is more accurate. If no user asks for the multicast packets, IGAP Router can request the upper router to terminate the transfer of multicast packets.

IGAP Router can authenticate an IGAP leave packet if needed. If leaving is rejected, the process is aborted.

In IGAP Leave (Type value 0x42), there are four Subtypes as follows. Every IGAP Leave packet is sent from user-client to IGAP Router.

- Basic Leave (0x41); This is used when authentication is not required.
- Password Mechanism Leave (0x42); The data of the message field is encrypted by password mechanism.
- Challenge-Response Mechanism Leave Challenge Request (0x43); This packet requests Challenge-Response authentication for leaving.
- Challenge-Response Mechanism Leave Response (0x44); The data of the message field is encrypted by Challenge-Response authentication to confirm leaving.

Experimental Network Environment



[experiment]

Video streams encoded in MPEG2 are transferred by IP Multicast from encoders to IGAP Router.

- Join : Validation by authentication mechanism after STB or PC sends IGAP Join
- Query and Re-authentication : Validation by authentication mechanism after STB or PC sends IGAP Join in reply to IGAP Query, while the STB or PC is receiving multicast streams
- Leave : Validation by "Fast Leave" mechanism after STB or PC sends IGAP Leave
- Management system : Verification of accounting and watching log of users using this system



5. Implementation and Experiment of IGAP

5.1. Transferring video stream with IP multicast

We confirmed the transfer of some real-time video stream contents using IGAP implemented on several user-clients and routers. This figure shows the experimental network environment. Two PCs and two Set-Top-Boxes (STB) were connected to the Distribution Switch by Ethernet across 100BaseTX cables. As described in Section 2., the Distribution Switch is operated as an IGAP Router, and transfers multicast packets or related packets to CDN and the PPPoE frames for Internet service to the provider's network. A commercial layer3 switch, the upper IGAP Router, was used as the gateway to the Internet. A user client can both watch a video distributed via IGAP while browsing Web pages by http over PPPoE.

The six commercial MPEG2 encoders in CDN sent multicast packets to the IGAP Router via the commercial layer3 switch. These encoders could send up to six video contents, i.e. there were six multicast groups. The RADIUS server was connected to the layer3 switch for user authentication and accounting. A PC was used as the portal Web server to provide a program guide to user-clients and personal user data, e.g. accounting charge. The PC ran the Management System software[8] to associate the portal Web server with the RADIUS server. IGAP Router was connected to the two layer3 switches by Gigabit Ethernet across optical fiber lines.

We transferred IP Multicasting 6Mbps video streams encoded in MPEG2 from the encoders to IGAP Router, and observed the video on the user-clients. The delay from sending IGAP Join to receiving Multicast Stream packet at user client was less than 600ms. It was admissible for most of user to watch video programs. The IGAP Join operation caused no degradation in video quality.

At the query and re-authentication process, the delay from sending IGAP Join to receiving RADIUS Accounting Response at user client was about equal to the case of first join. At the leave process, video program was off immediately, user didn't feel patient.

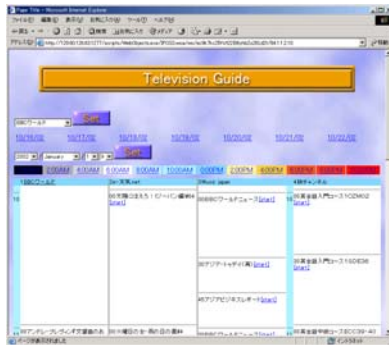
IP Multicast Management System



<Menu Image>



<Program Information (reception time, etc)>



<Program Guide>



<User's Account Information>



5.2. Displaying user information by Management System software

User's access and accounting log were recorded by the RADIUS server. Users can look at their own information, e.g. the programs list, accounting charge to date, and so on. Administrators (service operators) can look at all user's information and modify them as needed. Management System software treat the data as SQL-compliant database. The Management System software calculates user's charge per month using information of the database. There are several account types, e.g. Pay per Day, Pay per Month, Specific Accounting, Free, and so on. Each content has a accounting type. Users can look at fee every watched content and total per month.

Users and administrators can look at the information using Web browser by accessing portal Web server. These figures show the images displayed on Web browser; Menu Image, Video Programs Guide, Reception Information of Programs, and User's Accounting Information. Clicking on a button in the menu image displays the information desired. THE Administrator could add, modify, and delete the data. The program guide shows the video programs distributed within a preset time frame. User's Accounting Information shows total charge for this month, and details of each accounting type can be listed. Program Information shows multicast address of each program, UDP port number, total audiences count. This information is logged in the RADIUS server. Users can accurately count all user accesses to each multicast content, and can see details of access to each multicast content.

Conclusions

[Reports]

- The development of new IP Multicast management protocol IGAP for user authentication and accounting in content delivery services.
- The IGAP implementation for user-client and router
- Validation of IGAP operation

The Improvements

- Revision of IGAP header (concordance with IGMPv3, IPv6, etc)
- QoS mechanism and flow management for keeping content (video) quality (e.g. expedited forwarding)
- Brush up implementation details
- Inspection for actual (commercial) service
- etc

6. Conclusion

The new protocol for managing IP multicast proposed in this paper, IGAP, allows service providers to prevent unauthorized users from joining a multicast group, and to keep an accurate and detailed accounting log of actual service provided. We further study control of the layer2 network, e.g. LAN, for distributing multicast packets to the layer2 network by line concentrator, revision of header to satisfy recent protocols i.e. IGMPv3, extend IGAP to work with IPv6, expedited forwarding for content delivery, and so on.

References

- [1] W. Fenner, "Internet Group Management Protocol, Version 2", RFC 2236, November, 1997.
- [2] C. Rigney, A. Rubens, W. Simpson and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
- [3] C. Rigney, "RADIUS Accounting", RFC 2866, June 2000.
- [4] A.Tanabe, et al., "A Study of the Functions on the Traffic Distribution Switch in the Contents Delivery Network", APNOMS2001 Technical Proceedings, pp.160-171, September, 2001.
- [5] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC2516, February 1999.
- [6] W.Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC1994, August 1996.
- [7] B.Lloyd and W.Simpson, "PPP Authentication Protocols", RFC1334, October 1992.
- [8] H.Tojho, et al., "A Video Distribution Management System Architecture Based on IP Multicast", APNOMS2002 Technical Proceedings, pp. 515-516, September 2002.