International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.703

(03/2010)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Secondary distribution of IPTV services

IPTV client control interface definition

Recommendation ITU-T J.703

ITU-T

Recommendation ITU-T J.703

IPTV client control interface definition

Summary

Recommendation ITU-T J.703 defines the interface that enables the service client in the customer's network to send requests for content and application transport using Internet Protocol (IP) technology to the Internet Protocol Television (IPTV) service functions in the operator's network. Examples of IPTV content include digital video and audio programme content, including the metadata describing the programme content. Examples of IPTV requests include requests for broadcast or video on demand (VoD) content, requests to manipulate VoD content delivery (pause, play, rewind, etc.), and requests to record content for later viewing.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T J.703	2010-03-01	9

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T J.703

IPTV client control interface definition

1 Scope

The scope of this Recommendation is the i-3 interface, identified as the control interface for IP transport for enhanced broadcasting defined in [ITU-T J.700] and in Figure 1 below, that enables the service client in the customer's network to send requests for content and application transport using IP technology to the IPTV service functions in the operator's network. Examples of IPTV content and application to be requested through the i-3 interface include digital video and audio programme content, including the metadata describing the programme content, and applications to be presented or executed at the service client. Examples of IPTV requests include requests for broadcast or video on demand (VoD) content, requests to manipulate VoD content delivery (pause, play, rewind, etc.), and requests to record content for later viewing.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.770]	Recommendation ITU-T H.770 (2009), *Mechanisms for service discovery and selection for IPTV services*.
[ITU-T J.222.0]	Recommendation ITU-T J.222.0 (2007), *Third-generation transmission systems for interactive cable television services – IP cable modems: Overview*.
[ITU-T J.700]	Recommendation ITU-T J.700 (2007), *IPTV service requirements and framework for secondary distribution*.
[IETF RFC 2326]	IETF RFC 2326 (1998), *Real Time Streaming Protocol (RTSP)*.
[IETF RFC 3376]	IETF RFC 3376 (2002), *Internet Group Management Protocol*, Version 3.
[ISO/IEC 13818-6]	ISO/IEC 13818-6:1998, *Information technology – Generic coding of moving pictures and associated audio information – Part 6: Extensions for DSM-CC*.

3 Definitions

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAS/DRM	Conditional Access Solution/Digital Rights Management
CBI	Common Billing Interface
CDRP	Call Data Rating Point
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specifications
DSM-CC	Digital Storage Media Command and Control
DVR	Digital Video Recorder
EAC	Emergency Alert Controller
EAM	Emergency Alert Message
EAS	Emergency Alert System
ECM	Entitlement Control Message
EPG	Electronic Program Guide
FTP	File Transfer Protocol
G-PON	Gigabit-Passive Optical Network
HD	High Definition
HTTP	HyperText Transfer Protocol
IANA	Internet-Assigned Numbers Authority
IGMPv3	Internet Group Management Protocol, version 3
IPT	IP Telephone
IPTV	Internet Protocol TeleVision
ISA	Instruction Set Architecture
iTV	interactive TV
MAC	Media Access Control
MPEG	Moving Picture Expert Group
MST	Minimum Spanning Tree
NAT	Network Address Translation
NGN	Next Generation Network
NMS	Network Management System
PVR	Personal Video Recorder
QoS	Quality of Service
RG	Residential Gateway
RSVP	Resource reSerVation setup Protocol
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SDP	Session Description Protocol
SI	System Information or Service Information
SRM	Service Reference Model
SSM	Source Specific Multicast
STB	Set Top Box

STUN	Simple Traversal of UDP through NATs
UDP	User Datagram Protocol
VoD	Video on Demand
XML	Extensible Markup Language

5 Conventions

None.

6 Overview

6.1 IPTV network reference points

[ITU-T J.700] identifies significant reference points, shown in Figure 1 between the CPE and the various network functions with which it interfaces, between the session/resource/policy management functions and the IPTV application servers, and between the IP content sources and the content processing, distribution and storage functions. The CPE reference points are meant to address IP interfaces for hybrid and IP CPE. The network interface points for the moving picture expert group (MPEG) CPE and the MPEG portion of hybrid CPE are of a legacy nature and therefore not addressed.

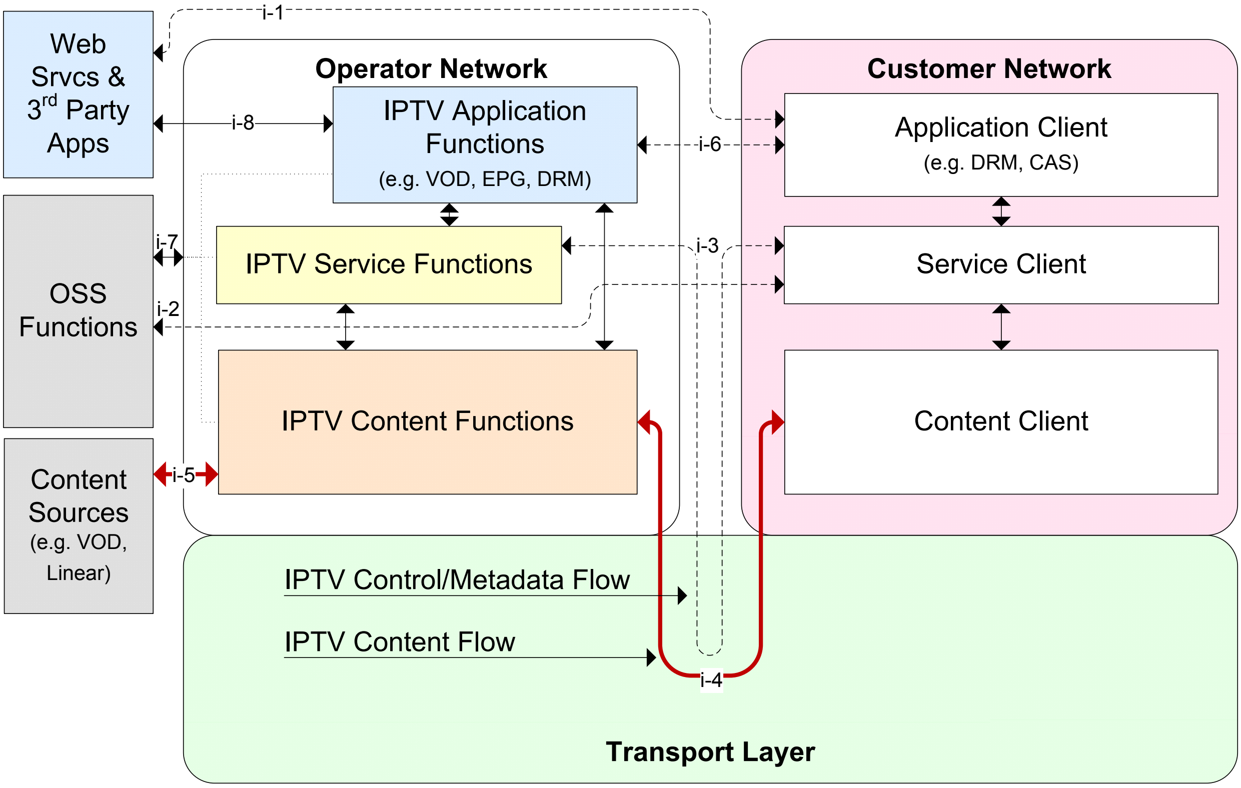


Figure 1 – IPTV network reference points

The focus of this Recommendation is the i-3 interface, IPTV service functions – service client. The i-3 interface enables the service client in the customer's network to send requests for content and application transport, using IP technology to the IPTV service functions in the operator's network.

Examples of content and application to be requested through the i-3 interface include digital video and audio programme content, including the metadata describing the programme content, and applications to be presented or executed at the service client. Examples of IPTV requests include requests for broadcast or VoD content, requests to manipulate VoD content delivery (pause, play, rewind, etc.), and requests to record content for later viewing. Potential supporting protocols include IGMP/MLD [IETF RFC 3376], RTSP [IETF RFC 2326], SDP and DSM-CC [ISO/IEC 13818-6].

7 IPTV client control interface

The IPTV client control interface makes use of multiple protocols to access or implement several of the IPTV service functions – or portions thereof – identified in [ITU-T J.700]:

1) System information (SI) acquisition and management;

2) CAS/DRM control processing and client handling;

3) EPG acquisition and management;

4) Emergency Alert System (EAS);

5) Accessing broadcast services, including accessibility functions;

6) Accessing on-demand services, including accessibility functions;

7) Networked DVR control functions;

8) Session/resource control;

9) Policy management.

7.1 Procedures for client sign-on

The following procedures are necessary for a client CPE to sign-on to the operator's network. The operator provides information about itself and its network topology to CPEs using a set of IP multicast flows. The first multicast flow, known as the system-wide flow, contains IP names or address of the various IPTV application functions and servers in the system and a code download list that tells the set-tops in the system when to upgrade boot and client code. After obtaining an IP address from a dynamic host configuration protocol (DHCP) server, all CPEs join the system-wide flow during the boot process (once the boot loader has control and again when it launches the CPE client application). The system-wide flow resides at a well-known IP multicast address, registered with the IANA. The IP names or addresses are provided on the system-wide flow using the DSM-CC UNConfigIndication messages. The remaining flows in the system should be arranged in a hierarchy as shown in Figure 2. The system is divided into hubs and clusters as shown in the diagram below. The lowest level in the hierarchy, a cluster, is a collection of IP subnets. The operator assigns each CPE in a system to a cluster and each cluster to a hub. Since there is only one system-wide flow, a well-known multicast address is used. The remaining flows use dynamic addresses. The set-tops acquire the address of the hub and cluster flows during the registration process (in the UNConfigConfirm message).

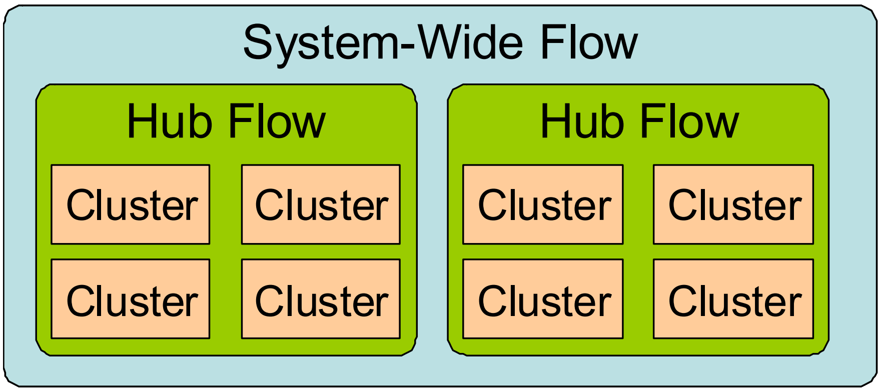


Figure 2 – Multicast control flows

The hub flow provides the system information or service information (SI) table, which contains service parameters for each service in the system.

The cluster flow provides a way for the IPTV service functions to send messages to one or more set-tops. The cluster flow is special in that it is the only permanently joined multicast flow in the system. All other flows in the system are joined on demand. The cluster flow allows the IPTV service functions to provide change notification for all other flows. When there is new information in one of the other system multicast flows, a change notification is sent on the cluster flow. The CPE will then join the dynamic flow that contains new information and wait for the update. Once the updated information is obtained, the CPE will leave the dynamic flow. The change notifications are provided on the cluster flow using DSM-CC [ISO/IEC 13818-6] UNPassThru messages. When the emergency alert services are used, the EAM messages are carried on the cluster flow.

After each CPE boots, it registers with the IPTV service functions in the operator's network. The registration process consists of a request from the CPE to the service functions, called the UNConfigRequest or UNCR, and a reply from the service functions to the CPE, called the UNConfigConfirm or UNCC. The UNCR message, sent from the CPE to the service functions, contains the MAC address of the CPE, among other parameters. The service functions store the information from the UNCR for each CPE in a database. The UNCC message, sent from the service functions back to the CPE, contains the multicast addresses of the site, hub and cluster flows, the SRM hostname, and the location of the broadcast file system directory carousel.

An IPTV client that contains an embedded data over cable service interface specification (DOCSIS) modem MUST follow all mandatory DOCSIS procedures specified in [ITU-T J.222.0], including the DOCSIS provisioning flow as the first step in the provisioning process.

7.1.1 CPE booting process

There are two parts in the CPE booting process. First, the boot loader must obtain an IP address and check for a new code. If a new code is available, the boot loader must obtain the new code from the service functions, then boot the new code. Second, the boot loader must start the video applications (client code). The booting process is outlined in this clause and is summarized in Table 1.

[ITU-T H.770] describes some portions of the booting process.

Table 1 – Set-top box booting process

Step	Description
1	Boot loader obtains IP address from DHCP server.
2	Boot loader joins system-wide flow (IANA registered address) and obtains code download list.
3	Boot loader compares the CPE identity and current code version to the code download list. If there is a new available code, the boot loader downloads new code before continuing. If there is no new available code, continue with next step.
4	Boot loader boots CPE client code.
5	The CPE continues to listen on the system-wide flow for UNCI messages containing: – IP host name of the primary service function server; – IP host name of any IPTV service function servers (including STUN and NMS).
6	The CPE leaves system-wide flow.
7	The CPE uses DNS to resolve IP addresses of any IPTV service function servers (including STUN and NMS).
8	The CPE contacts a STUN server and obtains NAT mappings for any IPTV services that may require NAT mappings (including UNPassThru messages).
9	The CPE registers with the primary IPTV service function server by sending a UNConfigRequest message (UNCR).
10	The primary IPTV service function server replies to the UNCR with UNConfigConfirm (UNCC) message containing: – ClusterID and multicast address of cluster flow; – HubID and multicast address of hub flow; – VoD session resource manager host name; – Multicast address of broadcast file system directory carousel; – IP host name of the VoD catalog server.
11	The CPE joins cluster flow (from UNCC message) and listens for UNPassThru messages that may contain: – EAS messages; – Directory update messages which contain version change information for system-wide flow, site flow, hub flow, UNCC and broadcast file system flows; – System time table. The CPE is permanently joined to the cluster flow.
12	The CPE joins the hub flow, obtains SI table, then leaves the hub flow.
13	The CPE joins the broadcast file system directory carousel, obtains the full broadcast file system directory listing, and then leaves the broadcast file system directory carousel.
14	The CPE listens on cluster flow for UNPassThru messages indicating a change in one of the other multicast flows. If a change is indicated, the CPE will join the changed flow long enough to obtain the change. Unless a change notice is received, the CPE is joined only to the cluster flow.
15	As files are requested by applications, the CPE may join the broadcast file system flows to obtain specific files.

7.2 System information or service information management

The system information or service information (SI) acquisition, as detailed in clause 7.1 above, can be done on a hub-by-hub basis over the hub multicast flow. CPEs can be placed in individual hubs and different services can be provided and provisioned to different CPEs (and subscribers) based on hub. Table 2 details the minimum amount of information needed to allow a CPE client to obtain video-related multicast services.

Table 2 – System information field descriptions

Field	Description
Service ID	The ID to reference the video service; this can be directly linked to the virtual channel number (for display in the EPG).
Source IP	In most IPTV systems, a SSM (source specific multicast) will be necessary. If this is the case, a source IP is required for each service.
Multicast IP	The IP address of the video service to be joined by the CPE to acquire video content.
Encapsulation Type	Whether the video service is delivered as RTP encapsulated content or simply UDP/IP.
UDP Port	This field represents the multicast port of the stream to be joined by the CPE to acquire video content.
Client Application	The application to launch when this service is requested (e.g., through the EPG). Example client applications include DVR, VoD and LiveTV.

7.3 EPG acquisition and management

One of the IPTV service function servers retrieves the raw EPG data from an EPG service (usually reachable through the Internet), via FTP or HTTP. Once the raw data is retrieved, the application server parses the guide data and inserts data into the service functions database and file system. Once the files are placed on the service functions file system, the service functions server distributes the EPG files via the broadcast file system to the CPEs.

The acquired EPG data are then formatted and delivered to the CPE. The CPE then parses the EPG data and presents them to the end-user in a visible and navigational format. Upon the user selecting a service from the navigational EPG, the system information (SI) is referenced and the service is acquired as directed.

[ITU-T H.770] provides the method for service discovery, using EPG data acquisition and management.

7.4 Emergency alert service

The emergency alert system (EAS) is used in the United States to allow the National Weather Service (NWS) and local authorities to broadcast important weather and warning messages to service subscribers. Therefore, this clause is only relevant to deployments in the United States.

The Federal Communications Commission (FCC) requires that service providers receive and be able to send emergency alert messages (EAMs). The FCC also requires that service providers conduct regular tests of the EAS.

The EAM is received with a special RF radio receiver and sent to an emergency alert controller (EAC), one of the IPTV service functions of the operator's network. The EAC then sends the message to the primary IPTV service function server. A special process receives EAMs. Each EAM has a corresponding audio message that is placed on a broadcast file system. The EAM is then sent to the appropriate group of set-top boxes using a DSM-CC UNPassthru message on the cluster multicast flow. The set-tops then take the appropriate action by displaying the message in a banner and playing an audible tone.

7.5 Procedures for broadcast/multicast content signalling

The IPTV client accesses broadcast/multicast content using IGMP procedures [IETF RFC 3376] as detailed below.

The broadcast video services and some of the foundational set-top services rely on IP multicast. IP multicast provides a very efficient means to send the same data to many endpoints. IP multicast makes use of the concept of groups to let endpoints communicate their interest in a particular flow. A multicast group can be referenced by destination address only (*, G) or by the source and group address (S, G). Originally, multicast was designed to send data from a small number of senders to a large number of receivers. Therefore, join messages specified the stream to join by destination group address only (*, G). The * signifies that the source is not relevant. This approach has drawbacks. First, any sender can legally transmit to the multicast group. This is not ideal in an IPTV environment. Second, the total number of addressable streams is limited by the 248M possible group addresses. This may sound like a lot. However, IP addresses are usually assigned in blocks by the second or third octet. It is possible to run out of group addresses. Third, since multicast routing tables are built using trees back to the source, building a (*, G) tree is complicated. Most deployments use a device called a rendezvous point (RP) to merge all the sources into a virtual source so a minimum spanning tree (MST) with a single root can be built from the RP (called a shared tree). Then, a MST is built back to each source. Last, since the assumption is that a group can have multiple senders, a sender registration protocol is needed. This provides inefficiencies, and complicated setup and troubleshooting.

In an IPTV environment, there is only a single sender and the client knows the source address of the sender, so the client can specify the sender when a join is sent and a more efficient source tree can be built back to the single sender. This approach is called source specific multicast (SSM). With SSM, clients specify a source and a group (S, G) when sending a join message to request a stream. This means that the source and the group address are significant. Now, not only is the unicast source IP address the only legal transmitter, but the total number of group addresses are multiplied by the total number of usable source IP addresses in the provider's network. Also, MST trees are built back to the source, providing an optimal forwarding path from the sender to all clients (no RP involved). Only one MST is needed since there is only a single source, using far less memory and CPU in the intervening routers. Therefore, SSM provides simplicity, security and scalability.

SSM requires a client that can specify sources in a join message. This means that a client must support IGMPv3. SSM mapping, however, allows a map to be built (either in the local configuration or on a DNS server) that maps group addresses to specific sources. This provides a mapping from IGMPv2 (*, G) joins to IGMPv3 (S, G) joins, allowing the provider to control what sources are legal for which groups even in an IGMPv2 environment.

7.6 Procedures for on-demand content signalling

The IPTV client accesses on-demand content using either RTSP [IETF RFC 2326] or DSM-CC [ISO/IEC 13818-6] for content session setup and control. On-demand, content catalogs can be browsed from the CPE using HTTP or HTTPS protocols, with the on-demand catalog returning XML formatted metadata query results. Furthermore, content ingest should be accomplished using a combination of ISA/CORBA [b-CORBA ARCH] protocols (for sign-up and fulfilment of new iTV services) and [b-CableLabs-ADI] specifications (for directory structure and file format). FTP mechanisms may also be used for transfer of content as well as control words and ECMs to provide with the digital content. A common billing interface (CBI) or XML can be used to notify the billing system of content availability and acquisition.

7.7 Admission control and policy management

Without admission control, mis-provisioned or misbehaving network elements can direct more traffic into a higher-priority queue than bandwidth reserved for that queue. In times of congestion, routers will queue up packets until sufficient bandwidth is available to transmit the waiting packets. When queue depth starts to build, traffic in the queue experiences delay. When queue depth varies widely, so does delay, introducing delay variation (jitter). When a queue fills to maximum depth, the router throws away new packets, resulting in drops.

Most traffic classes placed in higher priority queues are sensitive to delay and drop. Video traffic is especially sensitive to drop. Therefore, a mechanism for admitting no more than a maximum amount of traffic into a queue is needed to protect egress and downstream links from delay and drop. These mechanisms are referred to as "admission control".

Ideally, all applications that needed reserved bandwidth would speak a universal admission control protocol. Ideally, this protocol would be used to admit both unicast and multicast traffic and would reserve bandwidth directly on the path through the network the admitted traffic will take. Unfortunately, this ubiquitous, universal admission control protocol does not yet exist.

There are three options currently available for admission control. First, the RSVP can be used as on path admission control for applications that support it. Second, application-based rate limiting (as known as application admission control) can be used to manage bandwidth within a manually provisioned partition. Third, a feature called "multicast rate limiting" can be used to limit the multicast bandwidth used on certain links.

Access lists can be created in the Layer 3 edge router to associate multicast addresses with bandwidth. The provisioning of this information could be accomplished through a variety of means. One example is as follows: if all the HD channels were addressed with 230 in the first octet and SD with 231, an access list could be created that mapped all 230.x.x.x addresses to 8 Mbit/s and all 231.x.x.x addresses to 2 Mbit/s. Once the access lists are created, bandwidth pools are created for each downstream (toward the access node) interface. As IGMP [IETF RFC 3376] joins are processed, the router subtracts bandwidth from the pool on the appropriate interface (based on the destination multicast address of the join). When a pool runs out of bandwidth, no new multicast replication can happen on that interface (until bandwidth is removed by a leave). In this way, multicast rate limiting can keep multicast traffic from overwhelming access node links. This is not true admission control as there is no way to give a negative acknowledgement to the device that sent the IGMP [IETF RFC 3376] join. However, it is an effective means to keep from overfilling the video queue on the access node uplinks. Multicast rate limiting can be used in conjunction with any of the access link QoS models below.

7.7.1 Access link QoS models

Approaches to access link QoS can take multiple forms as outlined below. Note that the term *oversubscription* means that more video streams are potentially available from the service provider than will fit on the access line.

In each of these models, the service provider uses a diffserv marking for its video traffic so that this traffic can receive appropriate QoS treatment.

Fully provisioned: The access line is sized such that all available service provider video streams can be carried simultaneously. This is most appropriate when high-capacity access technologies are available and a limited selection of multicast-delivered video is offered by the service provider. This model is also appropriate for multicast and unicast-delivered video in environments where the number of devices in the home is restricted so that the total video traffic demand on the access link does not exceed its capacity.

Under provisioned with application admission control in home: The next level is to support limited oversubscription of service provider video of the access *line*, with admission control done in the home. In this model, the total amount of video potentially available to the home exceeds the provisioned access line video traffic capacity. The service provider video terminating devices (e.g., STBs, PVRs) in the home cooperate to perform admission control of the service provider video streams to the home, so that at any given time the access link video traffic capacity is not exceeded. A bandwidth manager (e.g., the residential gateway (RG)) owns the access line bandwidth and admits flow requests from the other devices (e.g., STBs). If the flow causes capacity to be exceeded, then the bandwidth manager informs the device and the device will deny the user request. If the RG cannot perform this function, then other devices within the home network (e.g., STBs) cooperate between themselves to manage the access line bandwidth. This model is only applicable if the access link bandwidth can be expressed as a fixed number and the scope of the admission decision is a single home (e.g., in point-to-point access links such as DSL). It has less applicability in shared access links such as cable and G-PON. A very significant point in relation to this solution is that all traffic in the service provider video class on the access link MUST be admission controlled. All devices terminating the service provider video traffic must either support the same (i.e., standardized) admission protocol, or there must be some interoperability gateway techniques employed between different admission protocols used by different devices.

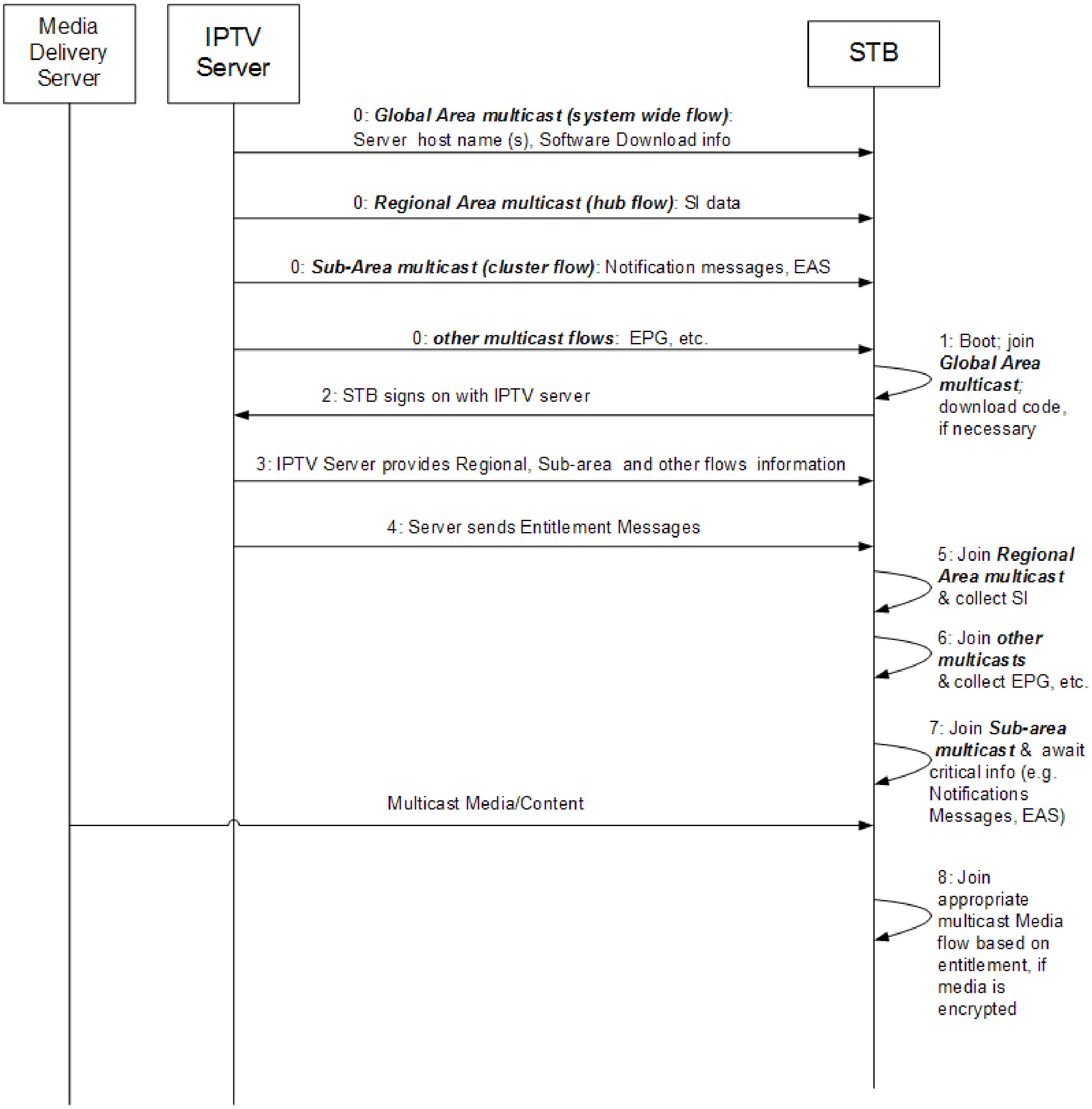
Under provisioned with home-to-network admission control: The next level is to support oversubscription of service provider video on the access *network*, with access line admission control done between the home and the service provider's network. Here, an admission request protocol runs between the home and the Layer 3 edge device, to admit each request for a service provider video flow. This allows oversubscription of the network upstream of the access line. This protocol would either be originated from the RG, or from another device in the home (e.g., STB) which is nominated by other such devices. If originated from the RG, then the protocols used on the home network for admission do not need to be the same protocol used between the RG and the Layer 3 edge device. In either case, though, all devices terminating this service provider video traffic must either speak the same (i.e., standardized) admission protocol, or there must be some interoperability gateway technique employed between different admission protocols used by different devices. This is the preferred model that allows devices in the home (other than the RG) to be agnostic as to the access link technology.

Appendix I

IPTV client bootup sequence

(This appendix does not form an integral part of this Recommendation)

Following is a high level example flow diagram illustrating fundamental steps in the IPTV client bootup sequence adapted from [b-ATIS-0800017].



Media Delivery Server
IPTV Server
STB
0: *Global Area multicast (system wide flow)*: Server host name (s), Software Download info
0: *Regional Area multicast (hub flow)*: SI data
0: *Sub-Area multicast (cluster flow)*: Notification messages, EAS
0: *other multicast flows*: EPG, etc.
1: Boot; join *Global Area multicast*; download code, if necessary
2: STB signs on with IPTV server
3: IPTV Server provides Regional, Sub-area and other flows information
4: Server sends Entitlement Messages
5: Join *Regional Area multicast* & collect SI
6: Join *other multicasts* & collect EPG, etc.
7: Join *Sub-area multicast* & await critical info (e.g. Notifications Messages, EAS)
Multicast Media/Content
8: Join appropriate multicast Media flow based on entitlement, if media is encrypted

Figure I.1 – IPTV client bootup sequence

The system should use a channel paradigm for all services. All services are presented to the end customer in a unified program guide. The service functions generate a SI table which contains the mapping of all video applications in the system. Each video application is usually mapped to one or more virtual channel numbers that show up in the program guide. The CPE will obtain this SI table from the service functions on the hub flow. As the end user selects the various services in the program guide, the CPE uses this mapping to call the various video applications residing on the CPE.

Bibliography

[b-ATIS-0800017] ATIS-0800017 (2009), *Network Attachment and Initialization of Devices and Client Discovery of IPTV Services*.

[b-CableLabs-ADI] Metadata 2.0 Specifications (2007), *ADI 2.0 Specification Asset Structure MD-SP-ADI2.0-AS-I03-070105*, http://www.cablelabs.com/specifications/MD-SP-ADI2.0-AS-I03-070105.pdf.

[b-CORBA ARCH] *Common Object Request Broker Architecture: Core Specification (March 2004), Version 3.0.3, Object Management Group (OMG)*, http://www.omg.org/cgi-bin/doc?formal/04-03-12.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2010