International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.292

(11/2006)

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

Cable modems

Next generation set-top box media-independent architecture

ITU-T Recommendation J.292

ITU-T Recommendation J.292

Next generation set-top box media-independent architecture

Summary

This Recommendation describes a core architecture that is not dependent on transport media for a next generation set-top box that will allow service providers to offer existing and new advanced services regardless of the transport media in the future. It is assumed in this Recommendation that all contents are transported on IP packets with an adequate QoS controlled mechanism. This Recommendation reflects key functional aspects of the next generation set-top box, such as network resource adaptability, secure two-way authenticated communication and session resource management and a QoS-control mechanism.

Source

ITU-T Recommendation J.292 was approved on 29 November 2006 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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

ITU-T Recommendation J.292

Next generation set-top box media-independent architecture

1 Scope

This Recommendation describes the core architecture of a next generation STB that is not dependent on the transport media. Operators and equipment vendors MAY elect to follow in making network and product investment decisions. This architecture specifically defines network resource adaptability, secure two-way authenticated communication and session resource management and QoS-control mechanism over full-IP environments. This architecture is applicable to support the growth of on-demand video, high-definition digital TV, managed in-home networks connecting a wide range of consumer-provided devices, and IP multimedia services including IP voice, video telephony, and multiplayer gaming. The goal of this Recommendation is to provide core functionalities for next generation STB regardless of the transport media. In actual implementation of NG-STB-A functionalities, the Recommendation MUST be used with [ITU-T J.290]. This Recommendation contains some technical solutions as examples to help the reader's understanding, not for the specification for the media-independent STB. It should be noted that the future Recommendations will define technical solutions relevant to the media-independent STB.

2 References

None.

3 Definitions

This Recommendation defines the following terms:

3.1 content distribution network (CDN): CDN contains a Core network and Access network where content delivery is controlled by identified packet routing and a QoS oriented mechanism.

3.2 customer premises equipment (CPE): CPE covers subscriber video devices (SVD), residential gateway (RGW), and optional in-home networking devices.

3.3 IP multicast: It is used for IP broadcasting in terms of bandwidth use efficiency of headend, CDN (Content Distribution Network), and CPE segment.

3.4 2-way authenticated communication channels: These channels are used for renewable conditional access key management, remote management of SVD, downloadable firmware updates, private interactive application data, and reconfiguration of encryption algorithms between the headend and an SVD.

3.5 transport stream (TS): The transport stream described in this Recommendation is delivered using a certain multicast flow, which is identified by multicast group address, UDP port number, etc.

3.6 portal services (PS): A functional element that provides management and translation functions between the HFC and Home network.

3.7 zapping control: The control mechanism for multicast group join and leave considering the IGMP/MLD protocol sequence is required in NG-STB compliant CPE devices.

3.8 residential gateway: The device that provides interconnection functionalities between access network and home network as described in [b-ITU-T J.190].

NOTE – How to apply J.190 residential gateway functionality to various networks SHOULD be considered in the near future.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ARQ	Automatic Repeat ReQuest
BE	Best Effort
BGP	Border Gateway Protocol
CA	Conditional Access
CAS	Conditional Access System
CDN	Content Distribution Network (in terms of the definition in [b-ITU-T J.282])
CoS	Class of Service
CPE	Customer Premises Equipment
DB	Database
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services Architecture for Network Traffic
DOCSIS	Data over Cable Service Interface Specification
DSCP	DiffServ Code Point
DSLAM	Digital Subscriber Line Access Multiplexer
DTV	Digital Television
EMM	Entitlement Management Message
FEC	Forward Error Correction
GigE	Gigabit Ethernet
HDTV	High-definition Television
HE	Headend
HGW	Home Gateway
IGMP	Internet Group Management Protocol
IP	Internet Protocol
Layer 3	Network layer 3 in OSI stack
LDPC	Low-Density Parity Check
MAC	Media Access Control
MLD	Multicast Listener Discovery
MPEG	Motion Picture Experts Group
NAT	Network Address Translation
NG-STB	Next Generation Set-Top Box
NG-STB-MI-A	Next Generation Set-Top Box Media-Independent Architecture
NIT	Network Information Table
OLT	Optical Line Terminal
OSPF	Open Shortest Path First
PCR	Program Clock Reference

PID	Packet Identifier
PIMSM	Protocol Independent Multicast Sparse Mode
QoS	Quality of Service
RGW	Residential Gateway
RTP	Real Time Protocol
RTSP	Real-Time Streaming Protocol
SI	Service Information
STB	Set-Top Box
SVD	Subscriber Video Device
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToS	Type of Service
TS	Transport Stream
UPnP	Universal Plug and Play
VCO	Voltage-Controlled Oscillator
VoD	Video on Demand
VoIP	Voice over Internet Protocol

5 Conventions

Throughout this Recommendation words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST" This word or the adjective "REQUIRED" means that the item is an absolute requirement of this Recommendation.

"MUST NOT" This phrase means that the item is an absolute prohibition of this Recommendation.

"SHOULD" This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT" This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

"MAY" This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

6 Next generation STB architecture on media-independent environment

In addition to clause 6 of [ITU-T J.290], the following items are mandatory key attributes of the next generation STB (NGSTB) architecture for a media-independent IP network environment:

– *Network resource adaptability*. Enables the network operator to utilize network bandwidth more efficiently through the use of: packet loss recovery schemes; residual traffic suppression caused by channel zapping; unified end-to-end QoS management from the headend to a subscriber video device (SVD) compliant with NGSTB media-independent architecture (NG-STB-MI-A); together with the advanced audio/video codec described in [ITU-T J.290].

– *MPEG-2 TS transfer over IP*. Enables the network operator to distribute transport streams in a media-independent environment through the use of a standard Internet Protocol suite with stream description information specified for IP multicast.

– *Resilient TS-clock synchronization with headend*. Enables all NG-STB-MI-A compliant SVDs to avoid play-out buffer overrun and underrun over the IP network environment.

– *Common presentation engine*. Enables an NG-STB-MI-A compliant SVD to support presentation engines defined in [b-ITU-T J.200] and [b-ITU-T J.201].

– *Location awareness*. Enables the network operator to control the distribution area of the transport stream based on the location of SVDs. SVD location awareness is optionally required.

– *Secure two-way authenticated channels via IP network*. Transport Layer Security (TLS) 1.0 in an NG-STB-MI-A compliant SVD provides secure 2-way authenticated communication channels between the headend and an SVD. Such channels are used for renewable conditional access key management, remote management of SVD, downloadable firmware updates, private interactive application data, and reconfiguration of encryption algorithms.

6.1 Reference architecture

The reference architecture of an IP content distribution service infrastructure is diagrammed in Figure 1. The relationship among major network segments is also summarized, e.g., CPE (customer premises equipment) including subscriber video device (SVD) and in-home network devices such as residential gateway (RGW), content delivery network (CDN) that MAY be separately defined as core and metro networks, Internet, and headend (HE). In a media-independent environment, all content distribution services are provided by an IP unicast or multicast transmission bearer. IP multicast SHOULD be used for IP broadcasting in terms of bandwidth efficiency of headend, CDN, and CPE segment.

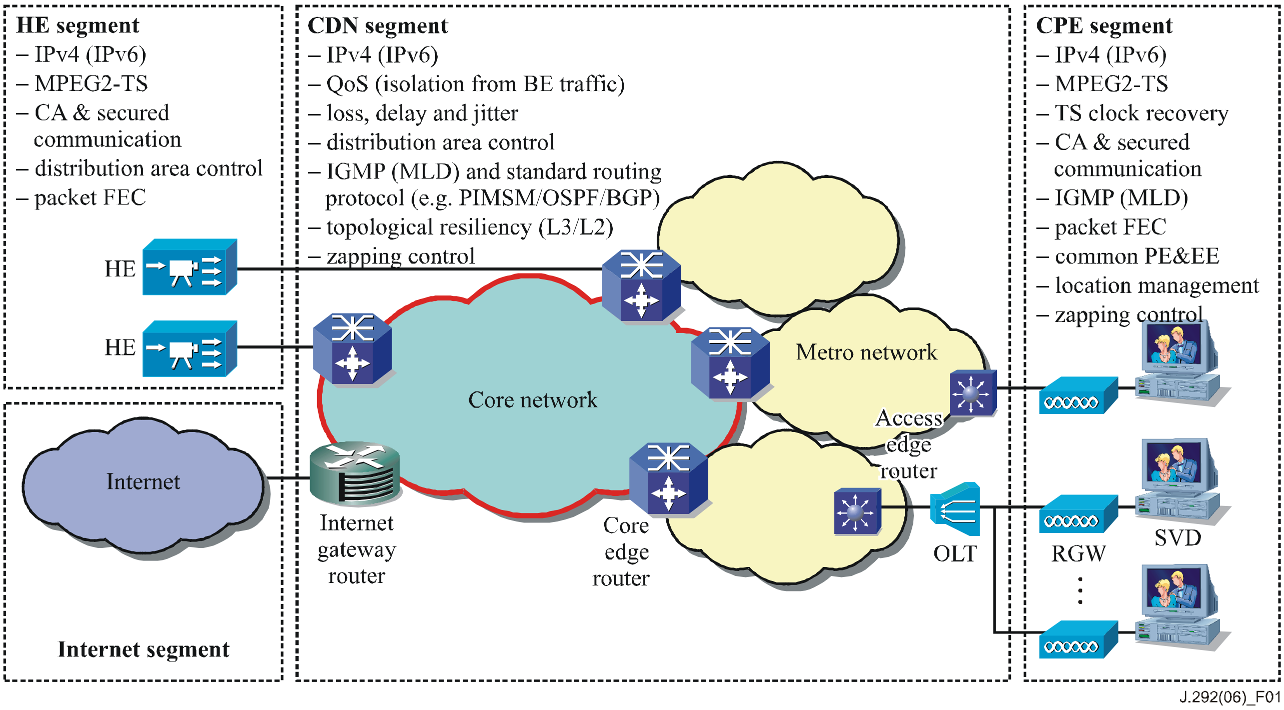


Figure 1 – Reference architecture of IP content distribution service infrastructure

6.2 Attributes of next generation STB for media-independent environment

6.2.1 Content distribution services architecture

At a minimum, NG-STB-MI-A SHOULD have the following attributes in addition to clause 6.2.1 of [ITU-T J.290].

– *IP-based content distribution*. IP is selected as the basic bearer layer for all content distribution services. All NG-STB-MI-A-compliant devices are required to support IPv4 with future IPv6 upgradeability. IPv4/v6 dual stack is also possible to use. Auto configuration mechanisms such as DHCP are also required for providing IP connectivity without manual configuration effort.

– *Linkage between multicast flow and TS*. The transport stream is delivered using a certain multicast flow, which is identified by multicast group address, UDP port number, etc. It is recommended to assign a different group address to each transport stream. All NG-STB-MI-A-compliant SVDs are required to obtain multicast flow information corresponding to the transport stream that the SVD wants to play out.

– *Zapping control*. The control mechanism is required in NG-STB-MI-A-compliant CPE devices for content zapping scenarios, where SVD consecutively changes multicast groups (i.e., transport streams) at high speed. As a result, residual traffic from groups having already left MAY cause congestion in the CPE segment.

– *Packet loss recovery*. In order to enforce transmission quality of the transport stream (TS), all NG-STB-MI-A-compliant SVDs are required to support packet loss recovery mechanism.

– *TS-clock synchronization*. In order to synchronize audio/video play-out timing with the encoder in the headend segment, a robust TS-clock regeneration mechanism is required even if there is some packet arrival jitter and/or losses of packet with Program Clock Reference (PCR) information in the IP transmission bearer.

– *High-definition video output*. High-definition video output is mandatory even for baseline SVD in media-independent environment.

6.2.2 Network segment: CPE

The CPE segment is composed of subscriber video devices (SVD), a residential gateway (RGW), and optional in-home network devices to which SVDs and RGW are attached. SVD is an NG-STB-MI-A-compliant video device that includes a tuner, such as set-top or set-back units or standalone digital TV sets (DTVs). RGW is located at the edge of the CPE segment and accommodated in an access edge device of the CDN segment. RGW also provides other CPE devices with Internet access. RGW differentiates and protects the incoming transport stream from best-effort Internet traffic. RGW is also required to have responsibility for service differentiation of the outgoing traffic from the in-home network to the CDN segment. RGW MAY also manage the in-home network QoS. As for the CDN access edge device to which an RGW is connected, the following equipment MAY be used but is not limited to: OLT (Optical Line Terminal), DSLAM (digital subscriber line access multiplexer), and layer 2/3 switch.

6.2.3 Network segment: CDN

Transport streams are distributed through the CDN segment. Best-effort Internet traffic MAY be multiplexed via Internet gateway routers. The CDN segment SHOULD arrange sufficient bandwidth to accommodate all transport streams, and usage of this bandwidth SHOULD be guaranteed even if best-effort Internet traffic grows. See [b-ITU-T J.282] for the bandwidth guarantee mechanism. In addition, the CDN segment SHOULD be resilient and avoid single point of failure inside it. See [b-ITU-T J.283] to increase IP network resiliency.

In addition to the specification described in [ITU-T J.290], NG-STB-MI-A compliant network devices in the CDN segment SHOULD support a QoS mechanism if the devices handle both best-effort Internet traffic and high-priority transport stream traffic from the headend segment. As for an example of QoS mechanisms, IEEE 802.1p specifies the priority identifier embedded in Ethernet frames.

6.2.4 Network segment: Headend

The headend segment SHOULD be constructed on an IP basis. GigE or larger bandwidth is required as network interfaces for multi-channel HDTV contents distribution. Packet FEC SHOULD be implemented in accordance with packet FEC implementation in an SVD. See [ITU-T J.290] for other features on the headend segment.

6.2.5 Network segment: Internet

Traffic from the Internet segment can be incoming to the CDN segment via Internet gateway routers and vice versa. Internet gateway routers are required to have sufficient capability of blocking anomaly traffic from the Internet destined to the devices in the headend and the CDN segments.

7 Customer premises

7.1 Functionality of CPE devices

– *Subscriber video devices (SVDs)*. Table 1 lists the baseline SVD functions and examples of step-up options. A baseline (low-end) SVD is defined with the minimum required NG-STB-MI-A functionality. Higher-end SVDs include various step-up options at the discretion of suppliers, network operators, and retailers.

Table 1 – Baseline and extended SVD functionality

Baseline SVD functionality	Optional step-up SVD functions (Examples)

– IPv4;
– Future upgradeability from IPv4 to IPv6;
– IGMPv2;
– Future upgradeability from IGMPv2 to MLDv2;
– DHCP client;
– High definition output;
– Multicast flow/TS linkage;
– Zapping control;
– TLS 1.0;
– Packet FEC;
– TS-clock synchronization;
– Location awareness.
	– IPv4/IPv6 dual stack, IPv6;
	– MLDv2;
	– IGMPv3;
	– Advanced packet FEC and/or local packet ARQ/FEC.

– *Residential gateway (RGW)*. Either layer 3 routing or layer 2 bridging approaches MAY be used for RGW implementation. In order to provide the Internet access for other CPE devices, a layer 3 approach with network address translator (NAT) is more general because other CPE devices need to be protected from the malicious access of hosts outside the CPE segment. However, the following functions in Table 2 are required as layer 3 RGW.

Table 2 – Baseline and extended RGW functionality (Layer 3)

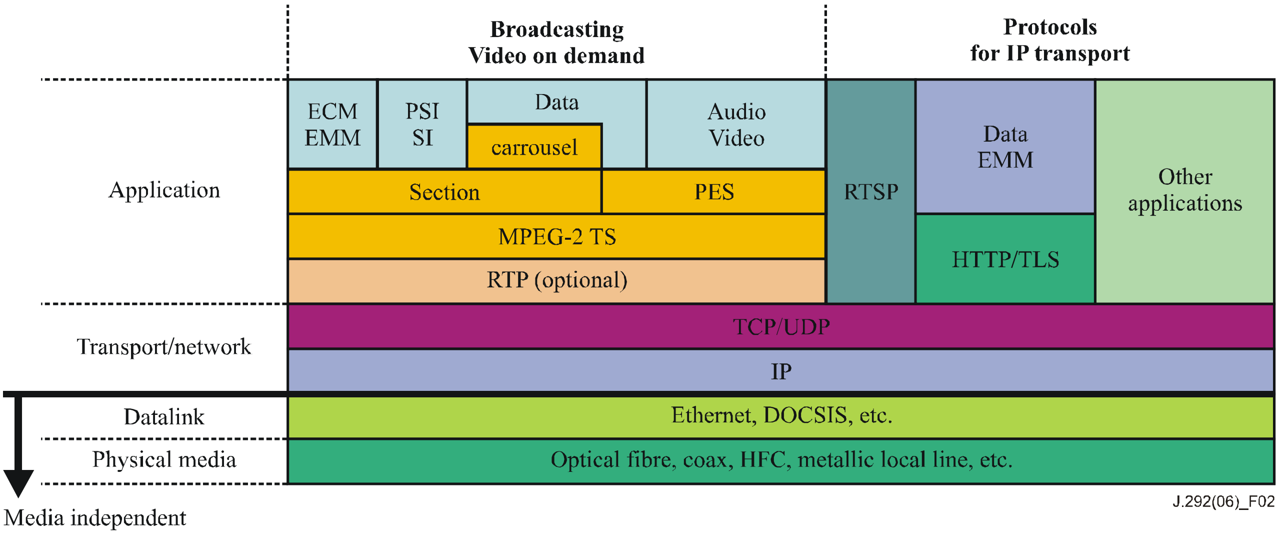
Baseline RGW functionality	Optional step-up RGW functions (Examples)

– IPv4;
– Future upgradeability from IPv4 to IPv6;
– IGMPv2 proxy;
– Future upgradeability from IGMPv2 proxy to MLDv2 proxy;
– DHCP client/server;
– Internet connectivity;
– NAT traversal for IPv4;
– Location awareness.
	– IPv4/IPv6 dual stack, IPv6;
	– MLDv2 proxy;
	– IGMPv3 proxy;
	– Local packet ARQ/FEC toward SVD.

– *Optional in-home network device*. An in-home network MAY be constructed inside the CPE segment using other devices that contain switching functions, such as Ethernet switches. For further information regarding the in-home network such as QoS control, refer to [ITU-T J.290].

7.2 Protocol architecture of video transport and data applications

Figure 2 shows the protocol architecture of video transport and data applications. All the NG-STB-MI-A compliant devices utilize IP as a basic transmission bearer to realize media independency in all the network segments. Video transport applications, such as broadcasting and VoD, are MPEG-2 TS-based and one or several TS packets are transferred as RTP/UDP messages. Note that TCP can be used instead of UDP for IP unicast-based services such as VoD. However, in IP broadcasting services, RTP/UDP over IP multicast is recommended because of the bandwidth efficiency on headend, CDN, and CPE network segments, where only one packet copy is required on transmission links between adjacent network devices.



NOTE – TCP is required for transmission of RTSP and HTTP/TLS.

Figure 2 – Protocol architecture of video transport and data applications

There are two IP versions, IPv4 and IPv6, whose differences are mainly their address length. Procedures for multicast distribution, signalling and address management have been defined for each protocol. All NG-STB-MI-A compliant CPE devices are required to support IPv4 and future IPv6 upgradeability at the minimum. IPv4/v6 dual stack is also possible to use. The IP version reconfiguration is recommended to be provided on an online basis, e.g., firmware download via the CDN segment.

If more secure content protection than the existing CAS system is required, a group of MPEG-2 TS packets in a RTP/UDP payload is encrypted. Figure 3 shows an example of RTP/UDP message with encrypted MPEG-2 TS packets. This example contains encrypted MPEG-2 TS packets, ID of encryption key and key update information.

RTP header	Key ID	Encrypted group of MPEG-2 TS packets	Key update information

Figure 3 – Example of RTP/UDP message with encrypted MPEG-2 TS packets

7.3 Signalling protocol between CPE and CDN segments

IGMP and/or MLD are used as program selection mechanisms of SVDs. As for the IGMP/MLD peer, an RGW or an access edge router of the CDN segment is possible to use. In case of layer 3 RGW, it SHOULD work as an IGMP/MLD proxy, which acts as the IGMP/MLD router (querier) for SVDs and as an IGMP/MLD host for the access edge router.

IGMPv2 or optionally IGMPv3 is recommended for an IPv4 environment, and MLDv2 for an IPv6 environment. When using IGMPv3, interoperability of IGMPv2 MUST be guaranteed as shown in RFC 3376.

7.4 Linkage between multicast flow and TS

The linkage information required for acquiring a certain transport stream are listed below.

1) Service ID;

2) Transport Stream ID;

3) Network ID;

4) IP version (v4 or v6);

5) Transport protocol (TCP or UDP);

6) Multicast group or Destination address;

7) Destination port number;

8) Usage of RTP header;

9) FEC type;

10) Frame format.

The items listed below are not mandatory, but are desirable in terms of security, generality, and ease of operation of SVDs.

11) Source IP address;

12) Source port number;

13) IP packet size;

14) TS packet size;

15) TS rate;

16) FEC flow information, including source/destination IP addresses and port numbers if different flow information from the transport stream is used for FEC packets.

There are several schemes to distribute the linkage information described above, which are categorized into push and pull types. In the push type, it is possible that the information is always distributed as NIT (network information table) using in-band multicast flow of transport streams, or a certain well-known and out-band multicast flow, to which all the SVDs need to listen. On the other hand, in the pull type, a linkage information server MAY be used, where all the SVDs need to access this server.

7.5 Packet loss recovery

An error correction method is useful for packet loss recovery. Considering burst packet loss scenarios, some interleave techniques are effective, where FEC calculation is performed among packets whose transmission orders are separated from each other. Figure 4 shows an FEC example, where up to 25 consecutive packet losses can be recovered.

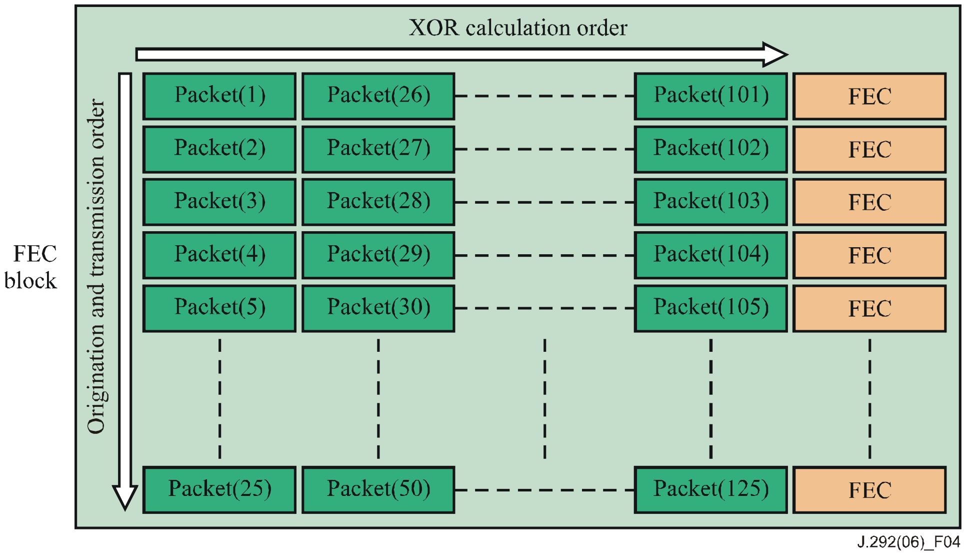


Figure 4 – FEC example

Some advanced FEC such as low-density parity check (LDPC) MAY provide better performance of packet recovery. Local packet retransmission between RGW and SVD is also considerable.

7.6 TS-clock synchronization

The reference clock of the decoder is controlled in order to synchronize with the clock of the encoder in the headend segment by a phase-locked loop (PLL) mechanism between transmitted PCR packets and an adjustable voltage-controlled oscillator (VCO) inside the decoder. The decoder in a SVD, however, SHOULD not directly use the PCR packets transmitted through the CDN segment because the amount of jitter of typical IP networks is much larger than the tolerated PCR jitter of 500 ns that is defined in the MPEG-2 system. Therefore, a de-jitter mechanism to satisfy the jitter tolerance of MPEG-2 system is necessary. The method for de-jittering is implementation dependent and outside the scope of this Recommendation.

7.7 Zapping control

Zapping, i.e., frequent multicast group changes, induces transient traffic increase and results in a waste of bandwidth in the meantime. In order to promote the most efficient use of bandwidth, a zapping control mechanism SHOULD be implemented in appropriate NG-STB-MI-A compliant devices that handle a host-router multicast control protocol, i.e., IGMP and/or MLD.

There are two approaches to attaining the zapping control. One approach is to restrict the number of channel requests from an SVD during a specific time period, which means that the SVD does not request the unnecessary channels. This approach is categorized into the multicast traffic receiver-side control.

The other approach is to restrict the registerable number of the multicast group addresses on a multicast transfer table at intermediate network devices handling IGMP and/or MLD control messages originating from the SVD. The following network devices are possible candidates: an RGW and CDN access edge devices such as a layer 2/3 switch with IGMP/MLD (snooping) capability. In such devices, multicast transfer is managed with the multicast transfer table, which associates between a multicast group address and a set of destination ports. By limiting the registerable number of the multicast group address per destination port or SVD's MAC address, the zapping can be controlled. This method substantially bounds the allowable maximum bandwidth of multicast traffic per destination port or SVD's MAC address; therefore, this is categorized into the multicast traffic transmitter-side control.

7.8 Location awareness

Since the IP CDN MAY cover a relatively wide area, e.g., national or even worldwide, there is concern that an SVD in any region potentially has an access to transport streams purposed for other regions. Therefore, a location-aware mechanism MAY be required to control the distribution area of transport streams based on the regional location of SVDs.

The regional location of client access edge devices in the CDN segment can be managed by the CDN operator; the location of RGW and SVDs is required to be linked to them. Some port-based authentication mechanism such as IEEE 802.1X MAY be required to be applied between each pair of adjacent devices, e.g., RGW and the corresponding client access edge device, RGW and SVDs, etc.

8 IP multicasting

8.1 IP multicasting

IP multicasting is defined as the transmission of an IP datagram to a "host group", a set of zero or more hosts identified by a single IP destination address. A multicast datagram is delivered to all members of its destination host group as regular unicast IP datagrams. The membership of a host group is dynamic; that is, hosts MAY join and leave groups at any time. There is no restriction on the location or number of members in a host group, but membership in a group MAY be restricted to only those hosts. A host group MAY be permanent or transient. A permanent group has a well-known, administratively assigned IP address. A transient group, on the other hand, is assigned an address dynamically when the group is created, at the request of a host.

Full support for IP multicasting allows a host to create, join, and leave host groups, as well as send IP datagrams to host groups. It requires implementation of the Internet Group Management Protocol (IGMP) and extension of the IP and local network service interfaces within the host.

8.2 IGMP

The IGMP (Internet group management protocol) is a protocol used between hosts and multicast routers on a single physical network to establish hosts' membership in particular multicast groups. Multicast routers use this information, in conjunction with a multicast routing protocol, to support IP multicast forwarding across the Internet. A router SHOULD implement the multicast router part of the IGMP.

Joining and leaving a multicast group is done through the IGMP. When initiating an application and joining a multicast group, the IGMP sends an IGMP membership report message to routers in the subnet to notify them of those joining the multicast group. This report is called the IGMP join message. A router sends an IGMP query message once per minute to confirm the presence of SVDs in the multicast group. Each SVD returns the IGMP membership report to this query message. By doing this, the router detects which SVD is present on the interface and sends the multicast packet to the required interface only.

In case of IGMPv2, the SVD sends a leave message explicitly when leaving the multicast group. However, it cannot avoid delivering multicast packets from specific sources to networks where there are no interested SVDs.

IGMPv3 adds support for "source filtering", that is, the system's ability to report interest in receiving packets only from specific source addresses sent to a particular multicast address. That information MAY be used by multicast routing protocols to avoid delivering multicast packets from specific sources to networks where there are no interested SVDs.

8.3 IGMP snooping

IGMP snooping is a useful protocol to control multicast flooding. When a SVD sends an IGMP join message, a switch transmits this to routers. At this moment a switch analyses the message and registers the MAC address of the multicast group where the SVD joins the group. The switch can relay multicast frame to the interface only where the SVD exists, thus avoiding flooding of multicast packet.

8.4 Multicast routing protocol

Routers or switches are not always in the same subnet where the SVD exists. In order to locate the SVD, a multicast routing protocol is used. A first-hop router is placed at the interface point between the multicast source and the packet transmission network, while the last-hop router is located at the interface point between the multicast group and the CDN segment in Figure 1. The multicast routing protocol is usually applied at the section between the first-hop router and the last-hop router.

There are two modes in the multicast routing protocol: Dense mode and Sparse mode. The Dense mode creates a tree configuration of distribution for one source and delivers packets based on the configuration in flooding mode. Packet delivery is ceased when not required. The Dense mode does not send the packet delivery request from SVD to routers upstream. The Sparse mode transmits packets with a combination of tree configurations for one multicast source and for multiple sources. In Sparse mode, a network core router and routers called Rendez-vous Point (RP) are defined. One RP is mandatorily required per multicast group. A tree configuration distributed by source is applied for the section between multicast source and RP; another configuration from the multicast group is applied for the section between RP and SVD. In contrast to Dense mode, Sparse mode has the function of multicast packet delivery request to upstream routers explicitly. This is called the Explicit Join message. In this mode, if a new SVD joins the group, the router can send a packet delivery request to upstream routers, extend delivery trees, and the delivery of multicast packet to the new member becomes available. The Dense mode MAY seriously affect the network with packet flooding. In case of a wide multicast distribution network, the Sparse mode is recommended.

9 QoS priority and policy mapping

9.1 QoS priority

Any SVD belonging to the [ITU-T J.292] architecture SHOULD be capable of providing QoS under the control of the residential gateway (RGW).

Informative NOTE 1 – In this Recommendation, it is assumed that the terminal device or CPE MUST conform to appropriate home network specifications such as UPnP.

The description in this clause gives an example of QoS bridging. The actual protocol will be described in a future Recommendation. The QoS control method, including admission control, from RGW to SVD SHOULD refer to the home network specifications.

Informative NOTE 2 – In case of the UPnP architecture, control messages are initiated from UPnP control point elements and responded to by UPnP Service elements.

The architecture is also characterized as a distributed architecture in that there MAY be multiple instantiations of a particular service in the home network (HN) that MAY be used interchangeably.

Informative NOTE 3 – This Recommendation describes certain UPnP QoS Services that SHOULD be contained within the PS of RGW.

This Recommendation defines three categories of QoS priority for packet transmission between RGW and SVD.

– Traffic importance number;

– Queuing priority;

– Media access priority.

9.1.1 Traffic importance number

Informative NOTE – In this Recommendation, UPnP traffic is a bilateral packet between the RGW and the SVD. UPnP traffic importance number (TIN) is shown in Table 3. It is noted that UPnP specifies TIN as 0 to 7; TINs 1 and 2 are in lower priority than TIN 0 that is assigned to the best-effort service traffic. UPnP QoS manager gives the TIN to traffic control function, one of portal service (PS) function in RGW based on QoS requirement from each terminal device.

The list of TINs SHOULD be registered in the PS database of the RGW.

Table 3 – Traffic importance number

Traffic importance numbers
7 (Highest)
6
5
4
3
0 (Best effort/Legacy)
2
1 (Lowest)

9.1.2 Queuing priority

It is assumed that packets from multiple interfaces would reach to PS functions of the RGW that belong to [ITU-T J.292] network. However, packets MUST be sent to only one interface toward the SVD. In order to guarantee total QoS service, packet queuing MUST be required on this interface. This Recommendation describes several prioritized queuing processes for QoS packets. The following queuing methods are widely used, and the choice is left to the operator.

Informative NOTE – Service or application (i.e., UPnP Traffic Importance Number) SHOULD decide which queuing method is to be applied.

This combination of queuing methods MUST be registered in the PS database of the RGW.

– *WFQ (Weighted Fair Queuing)*

The WFQ method dynamically prioritizes the queue per application flow. It schedules the assignment of bandwidth equally, based on the IP precedence of each packet. This method helps prevent large-size packets from obstructing the delivery of the small-sized ones.

– *CBWFQ (Class-based Weighted Fair Queuing)*

CBFWQ assigns packets into operator-defined classes with queuing priorities. This method schedules the assignment of an appropriate bandwidth to each explicitly assigned class. WFQ automatically assigns queuing per flow, whereas CBWFQ can assign bandwidth in accordance with the class that the operator has set explicitly: this allows for flexible queuing control.

– *PQ (Priority Queuing)*

The PQ method creates four-level queues, i.e., High, Medium, Normal, and Low, in accordance with the required priority. In this method, packets in the "High" priority queue are accorded first priority. Packets in other queues are not delivered until the "High" prioritized packets are transmitted completely. The PQ method makes it possible to assign "High" priority queuing to time-critical packets such as those from the VoIP or main frame.

– *LLQ (Low Latency Queuing)*

The LLQ method assigns packets into operator-defined classes of queue, as does the CBWFQ, and can set to deliver the packet with first priority in the queue. Bandwidth is assigned for the first priority queue and other queues. LLQ makes it possible to deliver prioritized VoIP packets and other packets of application together with the assured bandwidth.

– *WRR (Weighted Round Robin)*

The WRR method has four queues in its output interface and arranges queuing in accordance with the provisioned packet priority. The packet priority and queue are pre-tied, and each queue has weighting. WRR orders queuing according to the weighting, and controls the packet delivery. One queue can be assigned as the first priority queue among the four queues. Queuing starts from the first priority, and other prioritized packet can be delivered after completion of delivery of the first priority packet. A VoIP packet is usually assigned to the first-priority queue.

9.1.3 Media access priority

This Recommendation describes the prioritized QoS mechanism by prioritized packet flows in shared media. Figure 5 shows the broadcast by multicast with pre-provisioned bandwidth and prioritized QoS as an example.

Informative NOTE – The section from RGW to SVD is the QoS section of UPnP; each packet is prioritized, and queuing is controlled in this section.

On the other hand, bandwidth is pre-assigned in the access section, and packet is controlled in DiffServ-based QoS using ToS field with IP Precedence, DSCP or CoS.

As long as the bandwidth of CDN segment is well provisioned and the assigned bandwidth is larger than the total bandwidth of all prioritized packets, the quality of the prioritized packets is guaranteed by delivering them first with prioritized QoS. For example, if the total bandwidth of all prioritized packets is 100 Mbit/s and a bandwidth of more than 100 Mbit/s is assigned for the CDN segment, the prioritized packets must be able to be delivered with no congestion by adopting the prioritized QoS. In terms of the quality, the prioritized QoS with pre-provisioned bandwidth is considered equivalent to parametric QoS.

The QoS mapping MUST be provided at the RGW to exchange QoS signalling in each section.

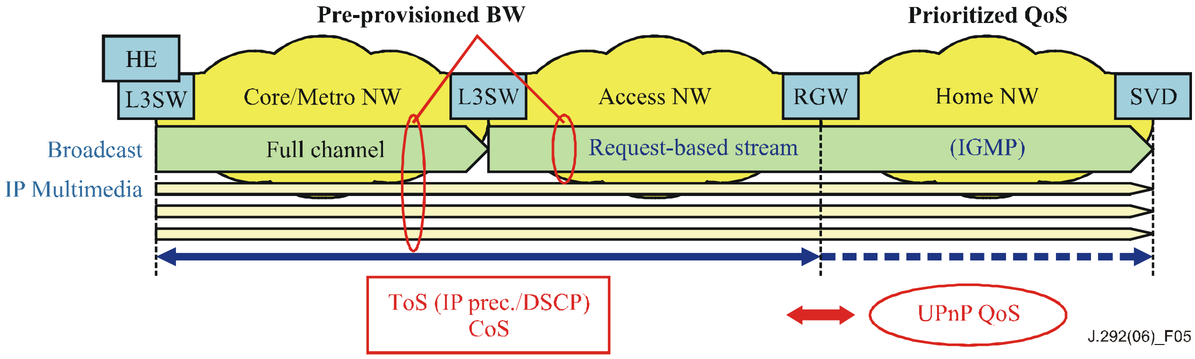


Figure 5 – Broadcast by multicast

A detailed description of QoS mapping is out of scope of this Recommendation, but a guideline is contained in 9.2.

9.2 QoS policy mapping

The packet flow SHOULD be controlled with prioritized QoS packet and prioritized queuing between the RGW and the SVD.

Informative NOTE – The QoS Policy Holder and the QoS Manager have core roles in the UPnP QoS control scheme.

The QoS Policy Holder SHOULD register QoS Policy and SHOULD provide the interface for accessing Policy; however, it SHOULD not control the QoS resources. The QoS Manager co-works with QoS Policy Holder and controls QoS resources in the LAN segment. The SVD MUST provide QoS capability with resource information and provide the interface for resource control. Figure 6 shows a relationship among QoS policy mappings.

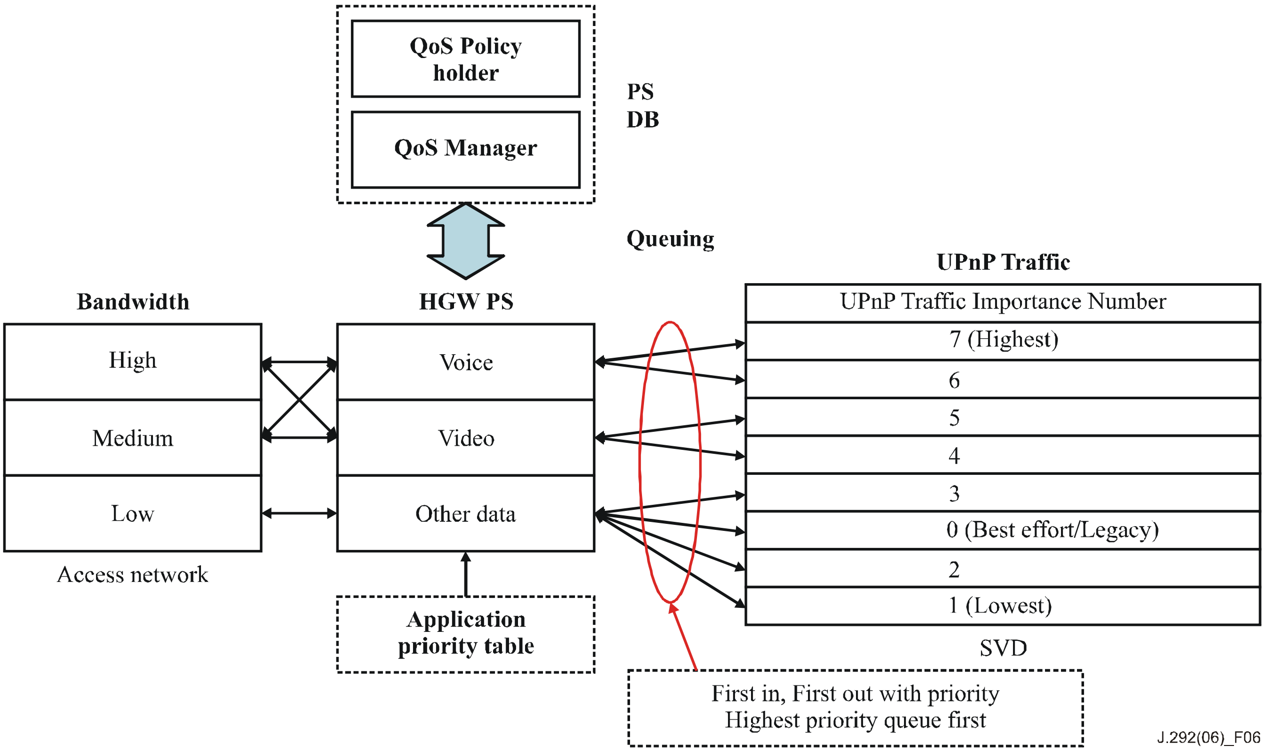


Figure 6 – A relationship among QoS policy mappings

Multiple mapping tables MAY be required for different services. These mapping tables SHOULD be verified with QoS policy and placed under the control of the QoS Manager. Figure 6 shows QoS mapping prioritized by services; other priority methods can be applicable using the port number. Mapping tables SHOULD be provided in the PS database.

10 IP broadcast and channel switching point

Broadcast requires that all programs be delivered to a terminal device; however, technological trends allow that broadcast use telecommunication lines for all programs to arrive at the nearest station. That means multicast delivery to the last-hop router is a kind of broadcast, i.e., IP broadcast. VoD is an application of IP broadcast and occupies bandwidth required by the customer to transmit one program. Figure 7 shows a relationship between IP broadcast and the Channel Switching Point. All IP broadcast content, i.e., IP Stream (IPS), are delivered to the channel switching point from the headend. Selected content is delivered to CPE from channel switching.

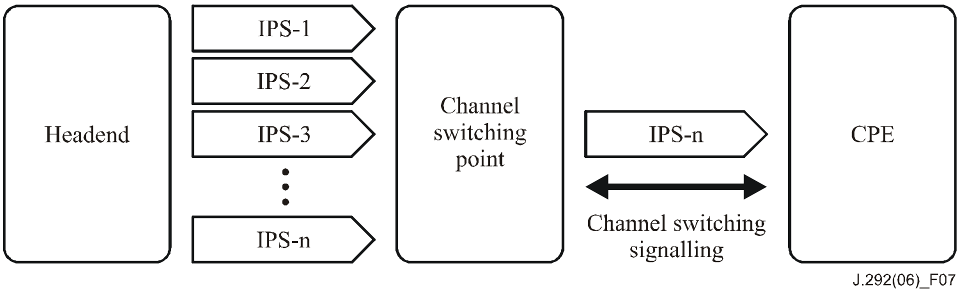


Figure 7 – A relationship between IP broadcast and channel switching point

The IPS is an IP packet stream recognized by address and port number. The channel switching point, not specified in physical implementation, is assumed to include a station switch with OLT/DSLAM, a network terminal with RGW, and software implemented in the CPE. The channel selection signal is a signalling information to control the channel switching point from the CPE, and currently uses IP multicast control protocols such as IGMP/MLD. This is required for expanded functionality to reflect the requirement for anonymous requests.

Multicast Listener Discovery (MLD) is the protocol used in the IPv6 protocol suite by a router to find listeners for a specific multicast group, much as IGMP is used in IPv4. The protocol is embedded in IETF Internet Control Message Protocol (ICMP) v6 instead of using a separate protocol. The protocol is described in IETF RFC 2710.

MLD and MLDv2 are equivalents of IGMPv2 and IGMPv3 respectively.

BIBLIOGRAPHY

[b-ITU-T J.200] ITU-T Recommendation J.200 (2001), *Worldwide common core – Application environment for digital interactive television services*.

[b-ITU-T J.201] ITU-T Recommendation J.201 (2004), *Harmonization of declarative content format for interactive TV applications*.

[b-ITU-T J.202] ITU-T Recommendation J.202 (2005), *Harmonization of procedural content formats for interactive TV applications*.

[b-ITU-T J.282] ITU-T Recommendation J.282 (2006), *Architecture of multi-channel video signal distribution over IP-based networks*.

[b-ITU-T J.283] ITU-T Recommendation J.283 (2006), *IP network architecture with network layer route diversity providing resilient IP multicast video distribution.*

[b-IETF RFC 768] IETF RFC 768 (1980), *User Datagram Protocol*.

[b-IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[b-IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol*.

[b-IETF RFC 1889] IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

[b-IETF RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2733] IETF RFC 2733 (1999), *An RTP Payload Format for Generic Forward Error Correction*.

[b-IETF RFC 3022] IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT).*

[b-IETF RFC 3376] IETF RFC 3376 (2002), *Internet Group Management Protocol, Version 3*.

[b-IETF RFC 3810] IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*.

[b-IEEE 802.1] IEEE 802.1: 802.1X – *Port Based Network Access Control*.

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	Telephone transmission quality, telephone installations, local line networks
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, 2007