International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.290

(11/2006)

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

Cable modems

Next generation set-top box core architecture

ITU-T Recommendation J.290

ITU-T Recommendation J.290

Next generation set-top box core architecture

Summary

This Recommendation describes a core architecture functionality of next-generation STB that operators and equipment vendors MAY elect to follow in making network and product investment decisions. This architecture defines a cost-efficient platform with capacity and flexibility to support growth of on-demand video, high definition digital TV, managed in-home networks connecting a wide range of consumer-provided devices, and future IP multimedia services including IP voice, video telephony, and multiplayer gaming. The goal of this Recommendation is to provide core functionalities and can serve as foundations for network specific environments. It SHOULD be noted that home networking portion of this architecture is based upon ITU-T Rec. J.190. In actual implementation of NG-STB-A functionalities, this Recommendation MUST be used with either ITU-T Rec. J.292 or ITU-T Rec. J.291 based on access network availability.

Source

ITU-T Recommendation J.290 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.290

Next generation set-top box core architecture

1 Scope

This Recommendation describes a core architecture functionality of next-generation STB that operators and equipment vendors MAY elect to follow in making network and product investment decisions. This architecture defines a cost-efficient platform with capacity and flexibility to support growth of on-demand video, high definition digital TV, managed in-home networks connecting a wide range of consumer-provided devices, and future IP multimedia services including IP voice, video telephony, and multiplayer gaming. The goal of this Recommendation is to provide core functionalities and can serve as foundations for network specific environments. It SHOULD be noted that home networking portion of this architecture is based upon ITU-T Rec. J.190. In actual implementation of NG-STB-A functionalities, this Recommendation MUST be used with either ITU-T Rec. J.292 or ITU-T Rec. J.291 based on access network availability.

2 References

None.

3 Definitions

This Recommendation defines the following terms:

3.1 authorized service domain (ASD): The devices in this domain are able to authenticate themselves and support content usage rights as defined by the network operator.

3.2 application ID: This is a field indicating a numeric ID for an application running on the set-top device.

3.3 authorized output domain (AOD): The devices in this domain are connected to the ASD using operator-approved output interfaces.

3.4 best effort domain (BED): Devices and physical layer segments not conforming to the requirements of ASD, AOD, GSD. The devices in this domain do not require content protection or guaranteed quality of service.

3.5 CA_system_ID: This is a field indicating the type of CA system applicable for either the associated ECM and/or EMM streams. The CA_system_ID may be used as a DSG client ID in DSG advanced mode.

3.6 DSG client: The DSG (DOCSIS set-top gateway) client terminates the DSG tunnel and receives content from the DSG server.

3.7 entitlement control messages (ECMs): An ECM is an encrypted message that contains access criteria to various service tiers and a control word (CW).

3.8 embedded PS: A portal services element that does not use a stand-alone interface to connect to a set-top box device.

3.9 embedded set-top box: An embedded set-top box is an embedded service application functional entity. It includes the DSG client(s), a DSG client controller, an embedded processor for an application environment, and either an embedded or removable module for conditional access.

3.10 entitlement management messages (EMMs): The EMM contains the actual authorization data and shall be sent in a secure method to each CPE device.

3.11 guaranteed service domain (GSD): Devices in the GSD will be able to receive QoS-sensitive content services such as VoIP, multiplayer interactive gaming, and IP video-phone.

3.12 home access (HA) device: A grouping of logical elements used to achieve HFC access for IPCable2Home network(s).

3.13 home bridge (HB) device: A group of logical elements used to bridge IPCable2Home networks together.

3.14 home client (HC) device: A group of logical elements used to provide functionality to client applications.

3.15 LAN IP device: A LAN IP device is representative of a typical IP device expected to reside on home networks, and is assumed to contain a TCP/IP stack as well as a DHCP client.

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

3.17 one-way: This expression infers that the downstream path (from the network to the subscriber) is operational, and that the upstream path (from the subscriber to the network) is not operational. This may occur because the upstream path is not available, the set-top device is not registered, or the set-top device does not support a two-way mode of operation.

3.18 QoS parameter set: The set of service flow encodings that describe the quality of service attributes of a service flow or a service class.

3.19 residential gateway: The device that provides interconnection functionalities between access network and home network as described in ITU-T Rec. J.190.

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

3.20 service class: A set of queuing and scheduling attributes that is named and that is configured at the head-end equipment. A service class is identified by a service class name. A service class has an associated QoS parameter set.

3.21 set-top controller: This is the computer system responsible for managing the set-top devices within a cable system. It manages set-top devices through control and information messages sent via the out-of-band channel.

3.22 set-top device: A receiver that contains an embedded PS function for home network connectivity and an embedded set-top box.

3.23 two-way: This expression infers that the downstream path and the upstream path are operational.

3.24 well-known MAC address: This refers to the MAC address of the client within the set-top device. This MAC address has been assigned by the manufacturer of the conditional access system within the set-top device.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES Advanced Encryption Standard

API Application Programming Interface

ASD Authorized Service Domain

BED Best Effort Domain

BP (IPCable2Home) Boundary Point

CA	Conditional Access
CAS	Conditional Access System
CBC	Cipher Block Chaining
CE	Consumer Electronics
CMTS	Cable Modem Termination System
Codec	Coder/Decoder
CPE	Customer Premises Equipment
CSA	Common Scrambling Algorithm
CSP	Configurable Security Processor
CW	Control Word
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services Architecture for Network Traffic
DLNA	Digital Living Network Alliance
DRM	Digital Rights Management
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line
DTCP	Digital Transmission Content Protection
DTV	Digital TV
DVB	Digital Video Broadcast
DVI	Digital Video Interface
DVR	Digital Video Recording
ECB	Electronic Code Book
ECM	Entitlement Control Message
EMM	Entitlement Management Message
EPG	Electronic Program Guide
FIPS	Federal Information Processing Standards
FTTH	Fibre to the Home
GigE	Gigabit Ethernet
GSD	Guaranteed Service Domain
HDCP	High-bandwidth Digital Content Protection
HDMI	High Definition Multimedia Interface
HDTV	High Definition TV
HFC	Hybrid Fibre Coaxial
ID	Identifier
IP	Internet Protocol
Layer 3	Network layer in OSI stack; Layer in firewall in which routing is based on IP address

MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MPEG	Moving Picture Experts Group
MPTS	Multiple Program Transport Stream
MTA	Multimedia Terminal Adapter
NAT	Network Address Translation
NCS	Network Call Signalling
NE	Network Element
NG-STB-A	Next Generation STB Architecture
NIU	Network Interface Unit
OCAP	OpenCable Applications Platform
OEM	Original Equipment Manufacturer
OSS	Operations Support System
PC	Personal Computer
PHY	Physical layer
PID	Packet Identifier
PS	Portal Services
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAN	Regional Area Network
RMS	Rights Management System
RSA	Public key cryptosystem developed by Rivest, Shamir, Adleman; also company by same name marketing public key technology
RSVP	Resource reSerVation Protocol
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SCTE	Society of Cable Telecommunications Engineers
SD	Secure Digital
SHA-1	Secure Hash Algorithm 1
SNMP	Simple Network Management Protocol
SOC	System-on-Chip
SPTS	Single Program Transport Stream
STB	Set-Top Box
SVD	Subscriber Video Device
TCP	Transmission Control Protocol

TOS	Type of Service (also DiffServ Code Point, DSCP)
TS	Transport Stream
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoD	Video-on-Demand
VoIP	Voice over IP
XML	eXtensible Markup Language

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 Integrated multimedia architecture

The following are key attributes of the NG-STB-A for an *Integrated Multimedia Architecture*:

– *Expanded capacity*: Provides expanded capacity that will be non-limiting to the introduction of new services. Enables cable operator options to use spectrum more efficiently through use of: converting analog channels to digitally-compressed video services; advanced compression algorithms; more advanced modulation schemes; integrated spectrum resource management at the head-end and switched digital video.

– *All-digital transition*: Supports a transition to all-digital services while continuing economically to support legacy analog TVs and VCRs.

– *Flexible, secure conditional access (CA)*: Implements CA through internal hardware (the NG-STB-A configurable security processor, or CSP) that can be remotely configured or renewed by software downloads. Supports multiple CA options including legacy CA and new proprietary or non-proprietary CA, thus enabling integration of CPE from multiple suppliers. Provides flexibility at lower cost than physically removable CA. At the same time, cable networks can continue to support physically separable security via use of security card device.

– *Support for retail distribution*: Facilitates retail sale of subscriber video devices (SVDs) by providing capability for subscriber activation, supported by remote configuration by the operator for compatibility with any NG-STB-A cable system.

– *Secure in-home networking*: Supports open home networking technologies and standards, digital rights management (DRM) systems, and ubiquitous use of IP (Internet Protocol) for distribution of content in the home. Enables network operators to offer head-end managed multimedia home network services. Supports use of multi-room entertainment systems that employ in-home storage devices to serve content to a variety of low- and higher-end networked devices. Integrates multimedia services between formerly video-centric set-top devices and data-centric PCs.

– *Secure two-way authenticated channels*: All next generation CPE provides secure 2-way authenticated communication channels between the head-end and CPE. This increases security relative to achievable security in one-way systems. Such channels are used for renewable conditional access key management, remote management of CPE, downloadable firmware updates, private interactive application data, and reconfiguration of encryption algorithms.

– *Flexible transport options*: Supports broadcast, multicast and/or IP unicast video transport.

– *CPE equipped for future transmission and compression standards*: Allows for future increases in effective system capacity with minimal incremental investment without stranding prior CPE investments, whether such investments are made by operators or by consumers at retail.

– *Well-defined applications environment in CPE*: Includes capability for the J.200 series ITU-T Recommendations applications platform middleware to support downloadable applications, enabling rapid service creation, innovation, and new business models, with intent to run the J.200 series of ITU-T Recommendations on all SVDs subject to reasonable licensing terms. Provides the cost savings of a standard platform without limiting the ability of cable operators to innovate in the user interface and overall look-and-feel of services.

– *Rapid provisioning of new services*: Supports self-installation and rapid provisioning of new services through auto-discovery, remote management, and remote configuration features of NG-STB-A-compliant CPE.

– *Improved resource management through open head-end interfaces*: Restructuring of head-end network elements with open interfaces allows more efficient use of system resources, effectively increasing usable system capacity and flexibility, reducing cost, and expanding the number of suppliers of head-end components, while ensuring interconnection capability.

6.1 Reference architecture description

The reference architecture is defined in terms of a set of network elements that are used to meet specific needs. These network elements operate within the major network segments comprising the back-office, head-end, outside plant, and customer premises, as diagrammed in Figure 1.

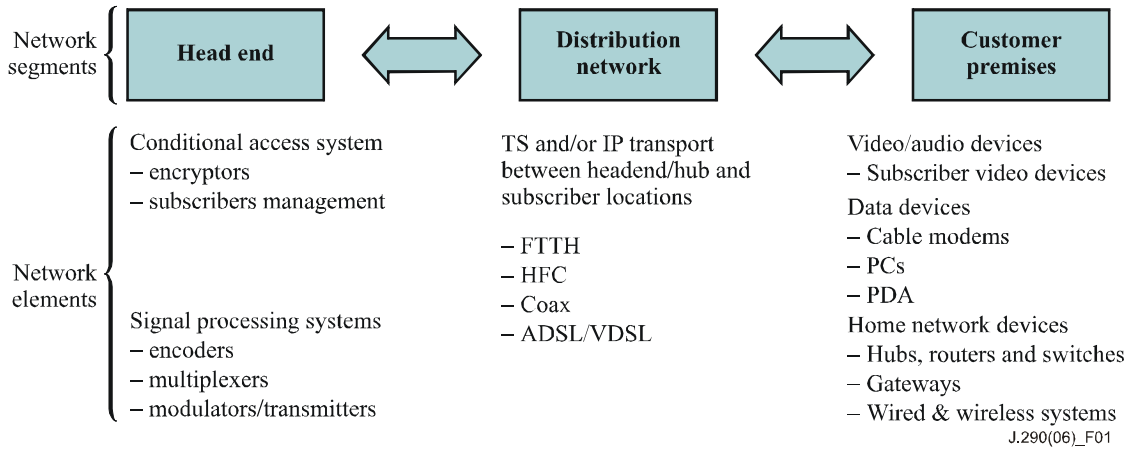


Figure 1 – Major network segments and elements

6.2 Attributes of an integrated multimedia architecture

6.2.1 Video services architecture

At a minimum, NG-STB-A-compliant CPE will have the following attributes:

– *Conditional access*: Employs reconfigurable internal CA based on a hybrid of a hardware engine for decryption (CSP) and software-defined key exchange. Supports multi-stream decryption for DVR, local advertizing insertion capabilities and other applications requiring multiple signals.

– *Video transport*: Supports two modes:

  • Non-IP mode (Baseline MPEG over QAM);

  • IP mode (MPEG encapsulated inside IP).

– *Video device applications support*: All video CPE have the minimum required resources (i.e., memory and processor power) to support [b-ITU-T J.200], [b-ITU-T J.201] and [b-ITU-T J.202].

– *Video codecs*: Support for decoding of H.262 (MPEG-2 Video) plus advanced codecs, H.264 (MPEG-4 AVC), and optionally VC-1. The client device MUST be able to switch nearly instantaneously between the currently active advanced codec and MPEG-2.

– *Audio codecs*: Supports for decoding of MPEG AAC or Dolby Digital.

6.2.2 IP multimedia architecture

– *Internet protocol*: IP selected as the basic bearer layer for all in-home network multimedia services.

– *QoS (quality of service) in IP home network*: {informative text: Plan to conform UPnP (universal plug and play standards) to enable remote management, provisioning, and service observation of UPnP devices on in-home networks.}

– *IPv6*: Support for both IPv4 and IPv6 in all IP-connected devices, with the intent eventually to transition to IPv6.

6.2.3 In-home networking

– *In-home network domains*: Defines in-home network domains as a function of level of service and of content protection.

  • GSD (guaranteed service domain): QoS managed from head-end to end device.

  • ASD (authorized service domain): Content can be transferred to receiving devices that have a certified, network operator-authenticated DRM or conditional access systems.

- OAD (output authorized domain): Content can be transferred through a rights-managed interface from the ASD to devices with non-operator-authenticated DRM.
- BED (best effort domain): Connected devices outside of GSD, ASD or OAD.

  CPE MAY be located within any one of these domains or in multiple domains where there are overlaps.

– *USB-2 and/or Ethernet port*: Provides universal CPE connection to in-home networks. Any physical layer capable of carrying IP transparent traffic (e.g., CAT5 Ethernet) can be supported through use of an adapter between the USB port and the specific physical layer.

– *Applications sharing*: Supports applications sharing between J.200 series devices as well as non-J.200 series devices that resides in one or more of the home networking domains defined in clause 6.5.1, for example, a PC with an NG-STB-A-compatible client. Applications examples include: remote access to DVR content; multiplayer games; personal information manager (e.g., family calendar, address book, alarm clock).

6.2.4 Program insertion

– *Program insertion*: Program insertion techniques such as ITU-T Rec. J.181 (Digital Programme Insertion) supports operator needs for flexible program delivery. The ability to splice two encrypted streams together, for example to replace an encrypted content in a broadcast stream with an encrypted content previously cached on the local hard drive.

6.2.5 Network segment: Customer premises

– *Subscriber video devices (SVDs)*: SVDs are NG-STB-A-compliant video devices that include a tuner, such as set-top or set-back units or stand-alone digital TV sets (DTVs). A baseline (low end) SVD is defined with minimum required NG-STB-A functionality. Higher-end SVDs include various step-up options at the discretion of suppliers, network operators and retailers. Baseline SVD functions and examples of step-up options are listed in Table 1.

Table 1 – Baseline and extended SVD functionality

Baseline SVD functionality	Optional step-up SVD functions (Examples)
• Support for multiple transport modes • Support for decoding MPEG-2 (SD and HD) plus H.264 • In-home networking connectivity as a client • Downloadable CA • Capability for J.200-series middleware • Standard definition output • High definition video output • Digital output interfaces with copy protection • OEM provided universal remote control capable of controlling the SVD and the legacy TV • Supports J.83 QAM downstream modulation as an option • Includes general purpose USB-2 and/or Ethernet port for in-home networking connectivity and possible unspecified peripheral connection	• Copy-protected digital interfaces (e.g., HDMI, DVI) • Built-in gateway (client, server, and IP address management) function between access and in-home networks • DVR baseline functionality • VC-1 codec

– *Rights management*: CPE devices respect and protect rights of content owners over the use of their high-value content.

6.2.6 Network segment: Head-end

- *QoS & session resource management*: Defines logical structure and process flows associated with QoS (requests, grants and service assurance). Coordinates and conforms head-end QoS processes associated with all resources in head-end, outside plant and in-home network.
- *OSS/BSS interfaces*: Defines model for interfaces with back-office billing system, operations support system (OSS), and business support system (BSS).

6.3 Video services architecture

The common features of video services architecture include:

- **Security**: Configurable security processor manages conditional access (CA), copy protection, support for secure on-demand services, secure downloads, and in-home digital rights management (DRM) functions.
- **Copy protection**: Copy protection mechanisms for delivering content across protected outputs.
- **Firmware downloads**: Provides device configuration.
- **Video transport**: Support for non-IP mode (baseline MPEG over QAM) and IP mode (MPEG encapsulated inside IP).
- **Video codecs**: Support for H.262 (MPEG-2 video) and H.264 (MPEG-4 AVC) codecs, and support for SMPTE 421M (VC-1) optionally.
- **Video client software environment**: Supports J.200 series middleware in all next generation network devices that support downloadable applications, plus provide flexibility to support applications through head-end based systems.
- **Secure software download**: Support for installing and upgrading software applications, drivers, kernels and J.200 series middleware implementations.

6.3.1 Security

An SVD will include an internal next-generation configurable security processor (CSP) for managing security aspects for services. Security aspects can be categorized as follows, with some overlap:

- Device authentication and management;
- CA of services between the head-end and subscriber equipment;
- Secure download of firmware updates and downloadable applications;
- Copy protection;
- Authorized service domain security;
- DRM within devices on one or more home networks within the authorized service domain;
- A security bridge between CA and DRM is defined in ITU-T Rec. J.197.

The next generation security model includes three subsystems:

1) *content and key encryption/decryption*, which is hardware-based but can be remotely reconfigured;
2) *key management*, which is partially software-based and thus re-definable by secure conditional access system download; and
3) *authentication*, which is partially software-based and thus renewable by the secure CAS download.

These subsystems will support operator management of the following aspects of CA:

- Remote reconfiguration of the decryption engine to support several predefined scrambling algorithms including commonly used legacy CA algorithms as well as new CA algorithms.
- Software-defined initial download and renewability of the CA key exchange mechanism.

In the CSP reference model, content MAY be secured with either an open standard, non-proprietary CA/DRM system and/or a proprietary CA/DRM system (legacy or otherwise).

The "flexible decryption engine" in the CSP, as shown in Figure 2, is configurable to support multiple algorithms. It is flexible enough to allow configuration by remote command to be compatible with the encryption algorithms used by the CA system as well as the content protection system(s). Entitlement messages and control messages are encoded and distributed over out-of-band and in-band channels to the video CPE such that keys can be securely recovered by the CSP; this is referred to as the firmware-defined conditional access key management application.

The secure aspects of the CSP are protected by integration on a system-on-chip (SOC) that includes a configurable decryption engine and a micro-controller for key management. The SOC will include the CSP and decoder elements so that in-the-clear and compressed digital video never leaves the SOC. In-the-clear digital video will be protected between the CSP and the decoder elements of the SOC using simple hashing or fast cryptographic techniques.

The CSP will be structured to avoid incurring liability for royalties for inactive or dormant CA/DRM systems. It is expected that the intellectual property rights (IPR) related to a CA/DRM system would not be used unless and until that CA/DRM system is activated by the operator.

Examples of possible algorithm choices are shown in Figure 2. The algorithms that will be supported will ultimately be decided when specifications are developed. To support transition from legacy CA, the client device MUST possess the ability to operate in a simulcrypt or multicrypt environment. In the event that simulcrypt is enabled, the CSP will support key sharing in the CPE.

The CSP will employ technologies to support the decryption of proprietary or non-proprietary standardized secure transport streams based on such as variants of DES, 3-DES, CSA, AES and Multi2 encryption algorithms.

The CSP will be capable of securely generating digital signatures inside tamper resistant hardware without exposing the private keys or the processing needed to generate the hash and encryption keys. The next generation network will be capable of digitally signing messages used for authentication and providing integrity using a secure hash.

Each CSP in a CPE device will be identified with a completely unique ID. For private serialization, each could contain a unique identifier known as a Private Seed ID. This Seed ID is used to generate the unique key to decrypt the entitlements for that specific CPE device. The CPE device will be capable of changing the Seed ID to another unique value upon secure command from the head-end. The encryption key would then be generated using this new Seed ID as a component of the key. An asymmetric key could also be used to decrypt the category key sent in the EMM (entitlement management message).

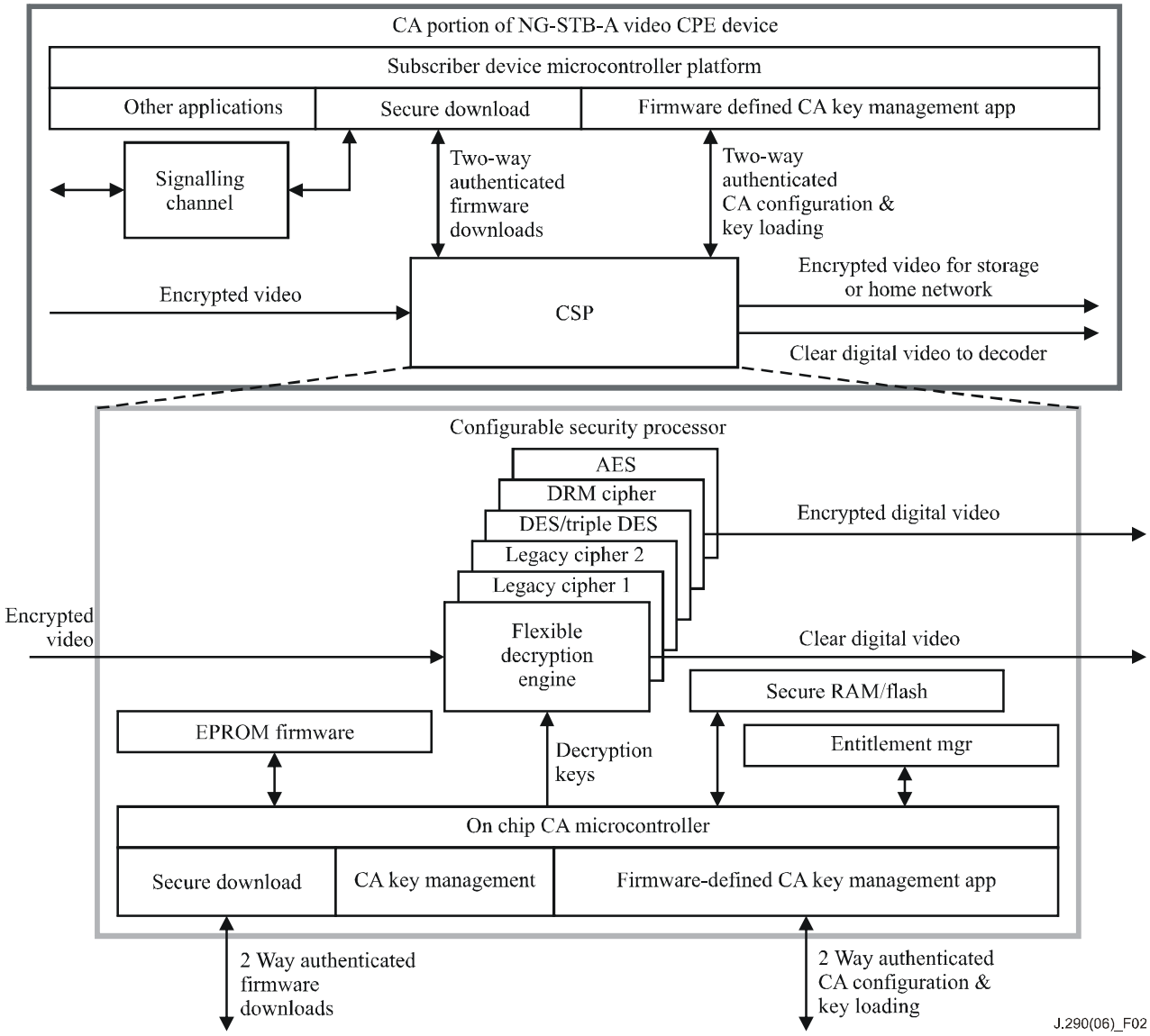


Figure 2 – Example of security block diagram

6.3.1.1 Multiple stream support

CSPs will be capable of decrypting/re-encrypting multiple content streams simultaneously. It is expected that different CSPs will be capable of processing differing numbers of streams depending on the capabilities of the associated CPE, but that all CSPs will be capable of processing some minimum number of streams simultaneously. CSPs SHOULD support the following multi-stream scenarios:

- *Watch and record*: The ability, using two tuners, to watch one encrypted stream 'live', while recording another simultaneously to a hard drive. This likely requires the CSP to remove the network CA encryption and apply a local hard drive encryption simultaneously to both streams.
- *DVR server*: DVR device with multiple tuners and a hard drive that supports other devices in the home that do not have hard drives by delivering recorded material via the home network. A DVR server can support multiple concurrent record-and-play streams, e.g., streaming content concurrently to multiple devices in the home while simultaneously recording several programs. The DVR device's CSP MAY have to support Watch and Record while also serving encrypted streams from the hard drive to remote devices in a multi-room DVR scenario.

CSPs MAY support multiple streams by employing multiple CSP cores, or by increasing the throughput of a single core, or both.

6.3.1.2 Conditional access

The NG-STB-A Plan envisions providing support for multiple conditional access (CA) options for the cable operator, allowing a network operator to support proprietary CA as well as any new standardized CA systems. The CSP within each CPE can be configured to run the particular CA chosen by the cable operator.

Because the CA choice can be made anytime under control of a head-end command, a system equipped with a CSP can be migrated gracefully from one CA option to another. CSP will be compatible with security cards. Subscriber devices that have security card interfaces SHOULD default to the CSP if no security card is installed.

6.3.1.2.1 CA software renewability

Certain aspects of algorithms, key exchanges, key management, and cryptographic protocols are implemented in software or renewable firmware on the CSP. Renewability in software is an important aspect of a strong security system and is desired in the next generation system. For cost reasons, it is desirable to use software renewability as a substitute for hardware renewability in as many situations as possible.

NG-STB-A does not support a "software-only" CA in which cryptographic functions are performed on a general purpose processor. Hardware security elements are a required part of an effective security system for high-value content. Software and specialized hardware elements are complementary and MAY provide additional security over software or hardware-only solutions.

6.3.1.2.2 CA hardware renewability

Although software renewability is more cost effective and easier to implement operationally, some level of hardware renewability is desired in the technology for key management and transport decryption within the CSP.

Hardware renewability of both key management and transport decryption can be achieved in several ways using removable hardware capable of supporting the bandwidth requirements of transport streams. For example, for NG-STB-A devices that support a multi-stream security card interface, the insertion of a security card would allow full renewability. Alternatively, a communication port such as USB 2.0 could be used to host a new device that could be deployed for full hardware renewability if device security were compromised.

6.3.2 Copy protection

If an NG-STB-A device employs a security card, the interface shall implement renewability and configurability. Additional next generation copy protection methods will also be considered.

6.3.3 Firmware and/or software downloads

SVDs are assumed to support three types of secure firmware downloads:

- General control firmware that controls the user interface, device operation, and support for applications (e.g., VoD, EPG, J.200 series of ITU-T Recommendations);
- Internal firmware that manages and communicates with the CSP;
- Highly secure messages intended to be passed to the CSP, which reconfigure the hardware engine and/or install CA key management firmware in the CSP.

The secure downloads are encoded for transmission to the SVD over a secure channel. All of the secure download signal paths require two-way authenticated exchanges and it is further assumed that physically accessible signals paths between blocks in Figure 2 are encrypted.

6.3.4 Video transport

Digital video and audio streams are typically carried over MPEG-2 transport streams. Both single program transport stream (SPTS) and multiple program transport streams (MPTS) MAY be delivered at various segments of the system. MPEG-2 program specific information and service information (J.94 SI) are used at the MPEG transport layer.

6.3.4.1 Backbone

The backbone audio/video transport (broadcast and on demand) is typically MPEG-2 transport over user datagram protocol (UDP)/IP carried over Gigabit Ethernet. Both SPTS and MPTS MAY be used. An example of SPTS is a video-on-demand stream at the streaming server's Gigabit Ethernet output. An example of MPTS is the multiplexed broadcast streams from a multiplexer. The IP encapsulation in the backbone is usually terminated at the edge of the network (at the QAM or CMTS).

Future backbone networks MAY make use of RTP or other protocols to recover timing affected by jitter and latency in the network. The use of an additional header such as RTP MAY enable additional video specific information to be carried in the packet, such as VoD session ID or program ID.

6.3.4.2 Edge to subscriber premises

The NG-STB-A reference architecture envisions two alternative means to carry audio/video data between the head-end edge and the subscriber premises. The video data will be compressed via MPEG-2 or an advanced encoding scheme described below. Audio data will be in MPEG-1 Layer 3, or an advanced audio encoding scheme. The two possible transport methods are:

- **Baseline: MPEG-2 transport over QAM**

  MPEG-2 multiple program transport stream (MPTS) over QAM is the conventional approach used in today's digital cable system. In order to maintain backward compatibility, the digital subscriber video device (SVD), or next generation video CPE, shall be able to process MPEG-2 transport over QAM for both broadcast and on-demand applications. The transport stream payload MAY be MPEG-2 audio/video or an advanced codec compressed stream.

- **Enhanced: Video over IP**

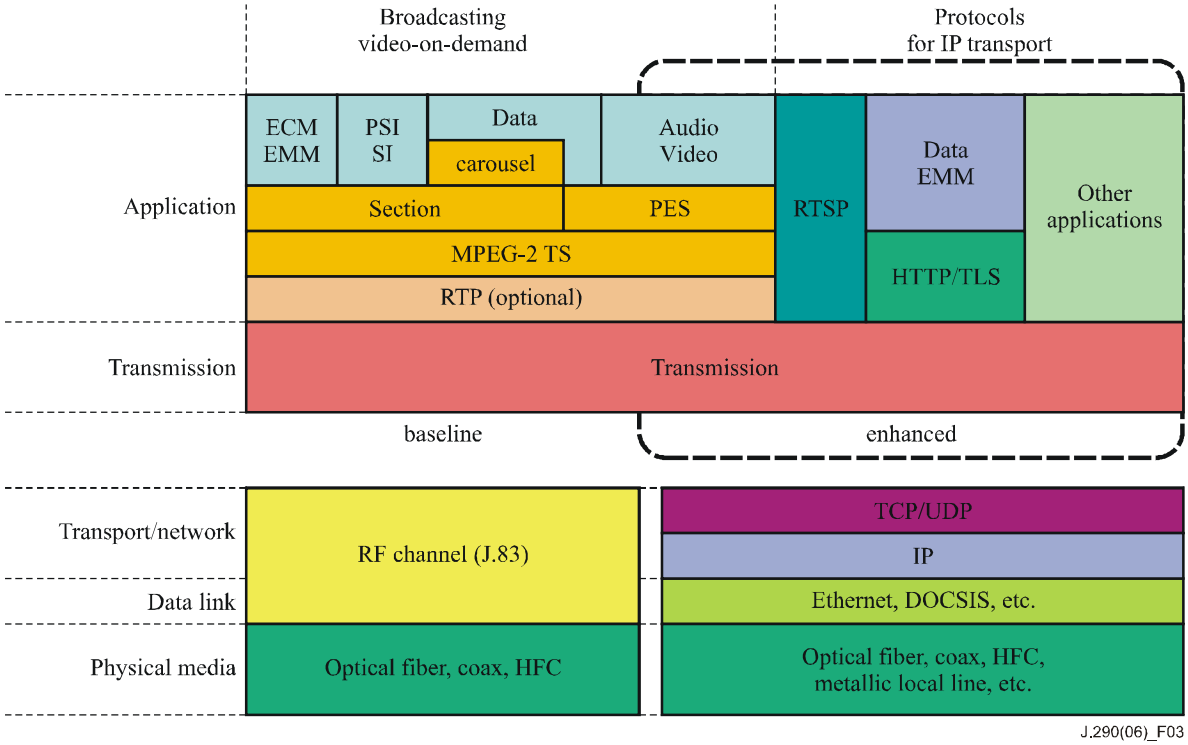
  In this approach, video is carried over IP and delivered over various media such as FTTH, DSL, HFC, Coax channels. This allows future services such as IP-based streaming media to the digital SVDs. The audio and video MAY be carried in any of these formats:

  – MPEG-2 transport packets over IP;
  – MPEG-2 transport packets in RTP payloads over IP;
  – RTP (or other realtime IP timing protocol) payloads over IP.

The receiving CPE SHOULD be able to process streams delivered in any of the above three formats.

In addition, data and EMM MAY be carried over HTTP with TLS. For VoD applications, RTSP MAY be used for session control. The receiving CPE SHOULD also support these protocols. For VoD applications, RTSP is used for session control such as SETUP, PLAY, PAUSE, TEARDOWN.

It is required that the subscriber terminal shall support two transport methods: baseline and enhanced. Figure 3 shows alternative video transport approaches based on the two transport methods.



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

Figure 3 – Alternative video transport approaches

6.3.5 Video codec

NG-STB-A cable systems will deliver video content in either of two compressed formats: MPEG-2 (both high definition and standard definition) as delivered on today's systems, and an advanced compression format. The choice of MPEG-2 or an advanced codec will be on a program-by-program, or service-by-service basis (including switching between program and advertizing content). Therefore the SVD MUST be able to switch rapidly between decoding MPEG-2 compressed content and advanced codec compressed content. The transition from MPEG-2 content decoding to advanced codec decoding MUST be as seamless to the viewer as current transitions between MPEG-2 programs.

The advanced compression format will be H.264 (MPEG-4 Part 10, Advanced Video Coding) and optionally VC-1.

The operator will choose which advanced compression format to use. It is not expected that an operator will use both advanced compression formats simultaneously on the plant. Therefore the SVD is expected to be capable of decoding both MPEG-2 and only one of the advanced codecs at a time. It is expected that the SVD would discover which advanced codec is needed for the system it is attached to and configure the decoder appropriately at boot time. This could imply download of appropriate firmware or activation of the appropriate resident firmware.

It is expected any dormant aspects of the unused advanced codec (i.e., hardware structures or firmware code) shall not infringe the intellectual property rights (IPR) related to that codec. The IPR would not be used unless and until the advanced codec is activated by the operator. This requirement is necessary so that OEM suppliers of NG-STB-A-compliant SVDs as well as cable operators deploying such devices will not be obligated to pay IPR royalty licensing fees unless they actually use the alternate advanced codec algorithms.

In addition to advanced video coding techniques, advanced audio coding schemes with significant improvement over the currently deployed audio coding scheme will also be considered.

6.3.6 Video client software environment

All NG-STB-A-compliant SVDs will be provided with sufficient memory and processor resources to be capable of running the J.200 series of ITU-T Recommendations middleware. The middleware MAY be resident or downloaded to the device. It is intended that the middleware will be run on the SVDs subject to negotiation of reasonable licensing terms. J.200 series of ITU-T Recommendations provides a consistent environment for unbound and bound applications; the former (unbound applications) are independent of any particular programming channels, such as a game, and the latter (bound applications) are tied to specific programming channels such as a clickable link to a review of a movie currently being watched.

J.200 series of ITU-T Recommendations comprises a set of APIs for the middleware component of a software solution. J.200 series of ITU-T Recommendations specifies a set of permission request files, a digitally-signed code image and a monitor application for various security and resource contention issues.

Figure 4 describes the software architecture in video CPE hosting J.200 series of ITU-T Recommendations.

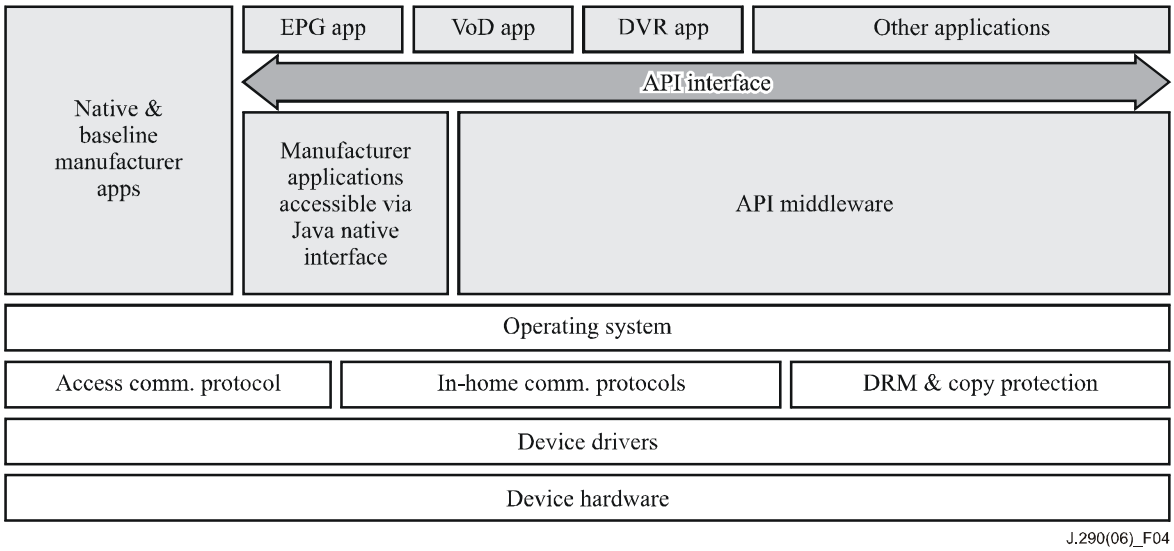


Figure 4 – Video CPE software architecture

The reference model identifies two categories of native applications that the device manufacturer would likely include in its products. Manufacturer applications described as "native and baseline" would have direct access to the operating system and bypass the J.200 series of ITU-T Recommendations middleware layer to interface directly to host and user interface; for example, these might include giving the user the ability to select between cable-ready versus off-the-air broadcast mode of operation. The other category of manufacturer applications is designated as "accessible via Java Native Interface" (JNI). These applications would also be supplied by the manufacturer and would map through the J.200 series of ITU-T Recommendations middleware layer.

The default for J.200 series of ITU-T Recommendations would be to pass these applications through to the host and user interface; however, J.200 series of ITU-T Recommendations would have the ability to modify the default or even to supplant the OEM application with a new application, for example, by one downloaded by an end-user on top of J.200 series of ITU-T Recommendations. An example of such default native applications might be up/down control of the sound volume on a DTV. Normally J.200 series of ITU-T Recommendations would allow the manufacturer's application to have control, but in the event of an emergency alert (EA), the network

operator EA application running on top of J.200 series of ITU-T Recommendations middleware could take over control of the sound volume.

Downloadable applications run in the J.200 series of ITU-T Recommendations middleware environment. Examples of applications that a network operator MAY choose to download would most likely include a core set of essential applications: electronic program guide (EPG), video-on-demand (VoD), and other cable applications such as support for head-end rendered applications. With this last option, the visual display of the user output interface is created as a still video frame picture at the head-end for freeze frame display by the CPE, or alternatively this MAY be implemented as a unicast video stream if bandwidth allows and the user interface involves moving components. Support for the user input interface would consist of relaying user interaction with the remote control back to the head end to communicate a menu selection, or cursor selection, from the display.

{informative text: Besides J.200 series API, Internet-based API such as html, java and flash SHOULD be applicable for rather simple applications. These API SHOULD be subject to negotiation of reasonable licensing terms. Current work to define relationship of content format for example HTML, FLASH to J.200 architecture may be added in the future.}

There are expected to be differences between CPE devices in terms of applications and capabilities that are supported. For example, high-end devices will support some applications, such as DVR, that are not present on lower-end CPE.

6.3.6.1 Security enhancements

Next generation client software will be a critical component in the overall system security architecture. Since system security for boot-time authentication, device driver authentication and system kernel security is not covered in the J.200 series of ITU-T Recommendations specification, and since this creates risk of security compromise, it will be important to specify the other security requirements for the complete next generation client software solution. The suggested solution includes a trusted and non-modifiable boot loader that is the foundation of all software downloads and upgrades. It also includes the authentication of all software elements including J.200 series of ITU-T Recommendations implementation, system kernel, device drivers, J.200 series of ITU-T Recommendations applications and all other software at both boot time and during download. In addition, it includes trusted kernel technology that creates a trusted environment for task context switching. All cable-provided client software security in the CPE SHOULD be tied to the trust of the CA system instead of creating a separate stand-alone trust model.

6.3.6.2 Advanced user interface

J.200 series of ITU-T Recommendations and head-end based applications can be employed together with other NG-STB-A elements to provide advanced user interfaces to new services. Since the next generation network architecture will support a much richer variety of services as well as rapid service introduction, it will be important to have intuitive user interfaces that are convenient and easy to learn to use.

The NG-STB-A reference model is intended to support expanded hardware and software user interface concepts beyond baseline remote control keypads and/or keyboards such as:

- Advanced remote controls with new input devices such as touch pads, pointing devices, and software defined keypads;
- Remote controls, or other ancillary devices with screens additional to the main display screen that allow messages, web pages, navigation, help, or control information to be displayed to one person or multiple persons in the same room;
- Non-typical input/output devices such as force feedback on game controls, vibration devices keyed to program content, and special effects generators that present three-dimensional sound effects.

In order to support such additions, a standard expansion port is defined (see clause 7) that can be employed to interface to an external advanced user interface device.

6.4 IP multimedia services architecture

Core IP multimedia services include high-speed data service and VoIP-based telephony. It is anticipated that cable-provided interactive IP-based multimedia offerings will grow to include, as representative examples: the sharing and display of high-quality still photographs, full-motion video telephony and conferencing, presence-enhancement for emerging communications media, applications-sharing and collaboration tools, and online-enabled multiplayer gaming. The next generation IP multimedia services architecture will serve as an enabling platform for a rich suite of applications addressing a wider range of CPE devices and a richer set of services.

Many IP multimedia services are sensitive to network delay, jitter and throughput; the NG-STB-A enables end-to-end QoS treatment for data traffic associated with IP multimedia services delivered to devices within in-home network domains. In addition to supporting QoS, it provides for service provisioning and monitoring, digital rights management, and NAT-traversal.

IP multimedia services are delivered over IP transparent channels, both:

i) between the head-end and subscriber premises; and

ii) within in-home network domains involving protected content (authorized service domain or ASD) and managed QoS (guaranteed service domain or GSD).

Physical network layers are not defined by NG-STB-A but could include IP traffic on coax or non-coax in-home networks, e.g., CAT5, HomePlug, or wireless. While NG-STB-A for different types of services could support essentially any physical layers, in general there is a preference for PHY layers that support QoS and offer capacity for multiple HD channels.

Potential IP multimedia service endpoints might include J.200 series of ITU-T Recommendations subscriber devices connected to the coax network, PCs sharing a DOCSIS high-speed data connection over the in-home data network, and personal wireless devices providing mobility and convenience functions within the home. A sampling of prospective IP multimedia applications hosted on these CPEs follows:

- PC(s) on the in-home IP data network configured as media servers and accessed by subscriber video CPE on the in-home IP network for high-fidelity presentation of music, video or still pictures.
- Gaming consoles interfacing with both video CPE and the home and access data networks facilitating participating in online multiplayer gaming sessions.
- Video telephony terminals and mobile, wireless communications devices receiving enhanced QoS-based network support while sharing infrastructure with other services within the home.
- Internet appliances that provide for telephone caller ID display, call logging, and message retrieval on subscriber video devices and PCs.

NG-STB-A will support extensions to the cable network that will enable cable operators to partner and/or compete with wireless voice and data service providers, offering services such as:

- Unified messaging services that integrate wired line with wireless universal numbering, voicemail, fax, follow-me voice, email, rich media messaging, and virtual private networks.
- IP mobility and roaming between cable modem services and public network WiFi hotspots.
- Deploying access points on outside plant to provide WiFi or other wireless technology coverage in public locations.

6.4.1 Transport

The delivery of multimedia services will be over IPv4 using both unicast and multicast. Support for IPv6 will be necessary to ensure future capabilities of the NG-STB-A as more network devices are connected to the network.

The regional area network will be IP-based and is anticipated to be carried over Gigabit Ethernet technologies, e.g., 1GigE and 10GigE. It is likely that a common regional area network infrastructure will be shared between the video and IP multimedia services architectures.

The NG-STB-A plan does not prescribe specific in-home data network physical layers (PHY). However, any suitable PHY MUST satisfy two requirements:

- The PHY MUST provide IP transparency for services in all in-home network domains.
- For services within the in-home network domain involving QoS, the PHY MUST also be capable of being QoS-managed.

Subscribers MAY select any of a number of choices that are IP-transparent. However, PHY/MAC combinations that can be QoS-managed by NG-STB-A protocols will provide a better user experience. Also, not all PHY choices will have the capability to support high bandwidth applications such as multiple HD streams. Examples of IP-transparent PHY that might be used with NG-STB-A systems include WiFi 802.11a/b/g wireless phone line, power line, coaxial and twisted pair (CAT5) wiring.

6.4.2 End-to-end quality of service

The overall experience that a user will enjoy is dependent upon the end-to-end treatment that a network service's traffic receives. Consequently, it is important to address the boundary between network segments to ensure that appropriate coordination is provided in managing overall session quality.

One approach to consider in the next generation multimedia network is to distinguish three broad segments of the network: the regional area network (RAN), defined as the core network consisting of the bridge between the source of the content or service and the access network; the access network, defined as the HFC segment connecting the CMTS and cable modem (CM) elements; and finally the home network, broadly defined as the entire (physical-layer-agnostic) network topology behind the CM within the home.

NG-STB-A incorporates by reference the mechanisms developed under the IPCablecom and IPCable2Home projects; IPCablecom multimedia (IPCMM) focuses on the access segment, while IPCable2Home targets the home network segment. In addition, the NG-STB-A defines a bridge or gateway between the in-home coax network (typically an extension from the coax drop that connects to TVs and other video devices inside the home), and in-home data networks (typically subscriber-owned, often other than coax, that support PC-centric applications).

6.4.2.1 Regional area network QoS

Many regional area networks (RANs) are maturing to distinguish and route packets over divergent paths (with associated quality metrics) based upon packet marking. IPCablecom multimedia supports DiffServ strategies on the RAN by allowing the network operator to associate a particular DiffServ Code Point (DSCP) with each upstream service flow. All packets exiting this flow will be tagged with this DSCP before entering the RAN. Similarly, IPCablecom multimedia includes the capability to distinguish incoming downstream traffic received from the RAN and to place this traffic on an appropriate service flow based on DSCP markings (as well as conventional IP and MAC-layer originating and terminating address mechanisms). The respective architecture has been outlined in ITU-T Rec. J.174.

Although network architectures outside of RANs are outside the scope of the NG-STB-A project, there are recognized potential benefits of standards for traffic peering for content and services beyond the current peering arrangements for high speed data traffic. For example, the ability to keep VoIP calls "on-net" end-to-end could provide significant cost savings. This is especially true in geographic areas where cable operators have adjacent RANs. Such peering arrangements would include hardware and protocol interfaces and suitable "settlement" systems.

6.4.2.2 Access network QoS

The fundamental prerequisite of access network QoS is the capability of providing bandwidth management for the prioritized traffic.

One approach to the management is to guarantee the bandwidth required for the specific services over access segments; a portion of the available bandwidth is constantly assigned for the prioritized traffic. The traffic is distinguished by the QoS packet marking and passed through the individually assigned path. Priority queuing method is also an effective solution to ensure the access network QoS.

The prioritized traffic is given priority for utilizing the bandwidth resource, which leads to prevent network delay, jitter and throughput degradation.

While several key network elements and interfaces have been identified and profiled within the IPCablecom Multimedia specification, ITU-T Rec. J.179, no session establishment protocol is defined. The NG-STB-A recognizes the prevalence of SIP in many of today's multimedia applications. One of the goals of the architecture is to support a wide variety of applications and their associated session establishment mechanisms. The NG-STB-A will implicitly support SIP in addition to other application-specific session establishment mechanisms.

6.4.2.3 In-home network QoS

IPCable2Home specifications are intended to provide Internet Protocol (IP)-based architecture for managed home-networked services.

NG-STB-A in-home network architecture is partly defined by existing aspects of IPCable2Home [b-ITU-T J.192]. However, the current version of [b-ITU-T J.192] only includes prioritized QoS across the home network to devices that include IPCable2Home QoS boundary point software. {informative text: In order to fully support NG-STB-A QoS objectives, [b-ITU-T J.192] will need to be extended to provide for parameterized QoS control by bridging UPnP and IPCablecom Multimedia.}

QoS capabilities MAY or MAY not be provided to the end client, depending upon the layer-two technologies employed and the location of the client in the network. From a QoS perspective, the client can reside in one of two in-home network domains, in the guaranteed service domain (GSD) or outside the GSD. When a client resides in the GSD, it has QoS capabilities at its disposal for establishing not only in-home network QoS, but also bridging the in-home QoS to the access network for end-to-end QoS treatment. For clients outside the GSD, in-home QoS is not available; however, the client MAY still receive access and RAN QoS treatment through application level signalling. This type of client is most likely a legacy QoS unaware device that can still benefit from access level QoS treatment.

To bridge between the access and in-home networks, the IPCable2Home device can take advantage of the robust packet classification mechanisms introduced in DOCSIS 1.1 and carried on into IPCablecom Multimedia. It is possible to identify and forward packets exiting the home network segment based on a number of distinguishing characteristics, including IP and MAC-layer originating and terminating addresses and ports, DiffServ/ToS marking and 802.1q VLAN tags.

Currently IPCable2Home 1.1 [b-ITU-T J.192] has adopted a packet-marking and priority queuing scheme based on 802.1q. {informative text: Moving forward, alignment between IPCable2Home QoS capabilities and those defined by UPnP is anticipated.}

For devices to reside in the GSD, the home network links between the gateway and GSD device will need to support parametric QoS. {informative text: Additionally, the client device will need to comply with IPCable2Home quality boundary point requirements (which are a superset of UPnP Device requirements).}

NG-STB-A will provide application level interfaces allowing client services to request bandwidth and content resources. The specific network segment within which these resources reside will determine what interface will be accessed. It is desirable to maintain a common language in order to simplify application requirements. {informative text: Examples of these interfaces MAY include IPCablecom multimedia with SOAP/XML extensions, IPCable2Home with UPnP QoS support, and J.200 series of ITU-T Recommendations home networking application extensions.} These enhancements will provide a standard mechanism for application interface.

6.4.3 IPv6

In order to support the envisioned large-scale deployments, support for IPv6 will be necessary for network clients. This requirement is necessary to ensure capital investment is not stranded and to ensure a large enough address space to support utility-based telemetry services in addition to other smaller market services. While coexistence and transition strategies for IPv6 have not yet been defined, support for IPv6 can be interpreted as software upgradeable. No hardware upgrades SHOULD be necessary to support IPv6 for NG-STB-A devices (this MAY or MAY not be true for existing legacy devices).

6.4.4 Security and privacy

In order to provide a telemetry service, consideration of the user's privacy and thus the securing of the user's data is imperative. NG-STB-A will provide mechanisms to allow an endpoint to authenticate the request as well as secure the endpoint's response to such requests. The following features are required for secure telemetry and control applications:

- All endpoints shall have factory defined identities;
- Secure cryptography mechanisms (i.e., AES, 3DES) shall be maintained through all tuning, gateway, network and client elements; and
- All management communications (XML, SNMP) shall be able to be secured.

6.5 In-home network architecture

This clause is about "in-home networking" within and between the several networks that will exist within the home.

While many homes have one or more home networks today, they are generally not well integrated with the cable system and provide limited support for multimedia (e.g., best-effort delivery of low-quality video vs guaranteed delivery of HD video). Extension of cable operator-provided services and content onto home networks will enable a greater variety of devices to participate and provide new opportunities for novel services and business models.

The next generation network architecture will include a comprehensive in-home network architecture that will support the seamless transfer of traffic between devices on the cable outside plant (e.g., DOCSIS, MPEG-TS) and various home network segments/technologies. NG-STB-A will support a variety of application models within the in-home network. One such model has J.200 series of ITU-T Recommendations on both client and server devices (e.g., a low-end SVD communicating with a high-end SVD). {informative text: In addition, NG-STB-A MAY also define

application interfaces, such as UPnP Remote UI, that would be independent of the OS and middleware on certain devices.}

Examples of services and applications that such an in-home networking architecture would support include:

- A low-end subscriber video device (SVD) could access a high-end SVD functioning as a digital video recorder (DVR) on the coax network for the purpose of viewing content stored on the hard drive of the high-end SVD. Thus, the low-end SVD would access the DVR application function of the high-end device without the cost of an additional hard drive and also provide a unified view of stored content at multiple locations in the home.
- A low-end SVD with limited memory and processing power could access J.200 series of ITU-T Recommendations supported applications running on a high-end SVD and obtain the application functionality as though the application were resident on the low-end SVD.
- An SVD on the coax in-home network could access video or multimedia media content resident on a personal computer located on the non-coax in-home network, or vice versa.
- Message traffic could be passed between the in-home coax and non-coax network to support applications such as display of caller ID on TV connected to an SVD or perhaps display of the e-mail inbox summary on a TV connected to an SVD.

The most demanding traffic on the in-home network in terms of bandwidth is likely to be high definition TV (HDTV) content. There is a preference for PHY layers that provide capacity for simultaneous real-time streaming of multiple HDTV channels within and between various in-home network segments and technologies.

The IPCable2Home project has defined a home networking gateway element to bridge between the cable operator's DOCSIS network and the subscriber's in-home network(s). This gateway is designed to be provisioned and managed in a secure fashion, and additionally can prioritize packets passing between the DOCSIS and home network segments. The next generation in-home network architecture will complement the foundation elements defined by the IPCable2Home project with the considerations necessary to transport high quality content (e.g., content requiring rights management and stringent QoS enforcement) within and between each network, to manage various LAN segments, and to admit client devices to the network.

6.5.1 General architecture elements and domains

A gateway element extends the functionality of IPCable2Home portal services (PS). This gateway element adapts the in-home network segment(s) to the MAC Layer, and possibly MPEG-TS, network; its functionality includes transferring traffic among and between various in-home network segments(s) and technologies. The gateway MAY have many physical implementations, from embedded xDSL modems or cable modems, to modem/NAT combinations, to implementations within a high-end SVD.

As shown in Figure 5, the gateway provides the ability to support multiple transport technologies allowing traffic to move seamlessly around the premises in a transport-agnostic IP environment. The traffic on the in-home network MAY comprise various combinations of content, content control, navigation, and applications sharing to allow for interaction between data, video, and IP multimedia services.

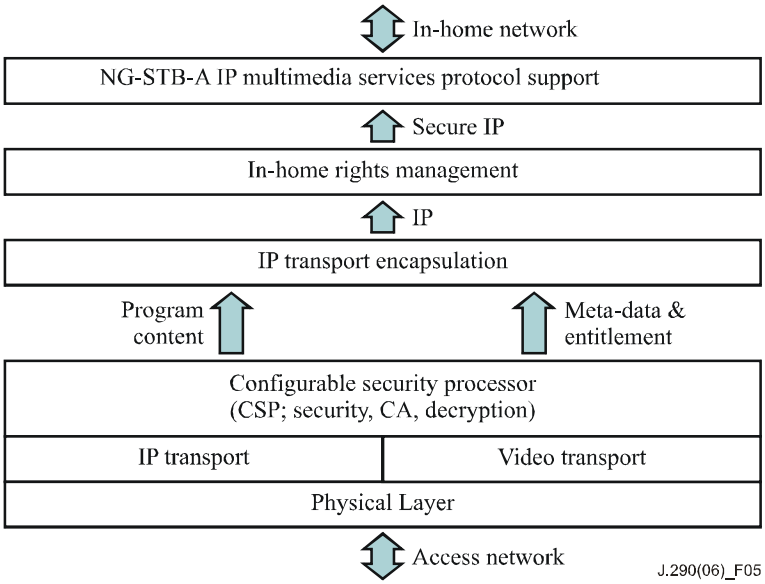


Figure 5 – Gateway communications architecture

The various in-home network technologies are unspecified at the media access control (MAC) and physical layer. Candidates for these layers include any known, or future, layers capable of high-speed Internet Protocol (IP) support. {informative text: Examples of such layers include Ethernet over CAT5, HomePlug power line carrier, Home PNA, MoCA, and 802.11a/b/g/n.} It is likely that many homes will utilize multiple home networking technologies to meet different needs.

The various in-home network segments are assumed to be IP-based; in addition to providing continued support for high-speed data applications, IP provides a standards-based and ubiquitous interoperability layer across multiple network technologies and devices.

As shown in Figure 6, within the communications architecture of the in-home network, there are functional domains that vary both by management of QoS and in terms of rights management (content protection).

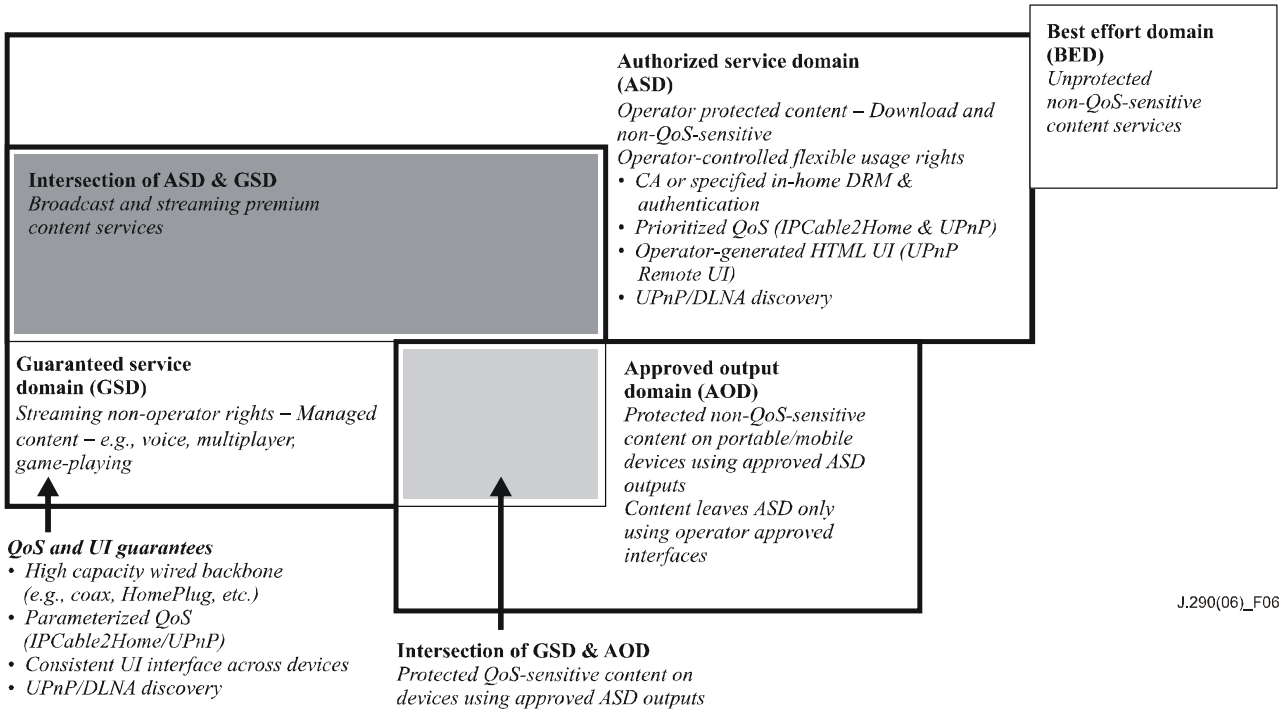


Figure 6 – In-home network domains – Overview

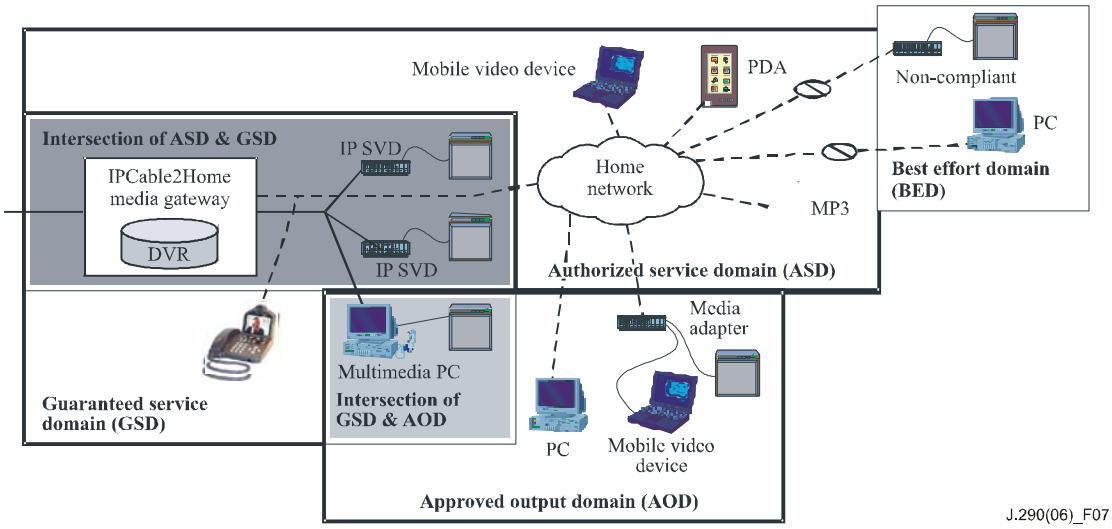


Figure 7 – In-home network domains – Examples

Guaranteed service domain (GSD)

If guarantees of QoS can be maintained from the head-end to a client, the client is considered to be part of the guaranteed service domain.

In order to ensure guaranteed QoS, the client MUST support the appropriate QoS signalling: the home networking technology that the client is connected to MUST be able to provide the guarantees for the necessary QoS parameters such as bandwidth, jitter & delay, and it MUST have enough capacity to carry multiple high-definition streams. {informative text: Example technologies that in the future intend to meet these requirements are wireline technologies based on coax (MoCA), powerline (HomePlug) and phoneline (HPNA 2.0).}

{informative text: The home gateway MUST support the appropriate QoS signalling and necessary hooks to bridge in-home QoS with the access network QoS, and it MUST implement IPCable2Home QoS functionality while the client device MUST implement UPnP QoS. The IPCable2Home QoS functionality is a superset of UPnP QoS.} Hence, a given client MAY be in the GSD when connected to one network segment in the home and not in the GSD when connected to another. Similarly, a given segment is likely to have some clients that are in the GSD and some that are not, based on the level of QoS support in each client device and application.

{informative text: All the devices and the stored content in this domain can be discovered using a mechanism defined by UPnP/DLNA (digital living network alliance, formerly called digital home working group or DHWG). The home gateway acts as a centralized discovery server for the in-home LAN. The cable operator can access this information through an IPCable2Home-defined MIB interface.}

Devices in the GSD will be able to receive QoS-sensitive content services such as VoIP, multiplayer interactive gaming, and IP Video-Phone. This content MAY or MAY not contain third-party DRM-based content protection.

Authorized service domain (ASD)

The devices in this domain are able to authenticate themselves and support content usage rights as defined by the network operator. This segment includes devices that comply with the in-home digital rights management as described below.

It is not necessary to provide QoS to the devices in the ASD. {informative text: However, the client devices MAY be able to support prioritized QoS and therefore SHOULD implement UPnP QoS signalling.} The home networking technology SHOULD be able to support prioritized QoS, particularly in segments where latency- and bandwidth-sensitive content is streamed.

{informative text: All the devices and the stored content in this domain can be discovered using UPnP/DLNA-defined discovery mechanism.}

Devices in the ASD will be able to receive protected non-QoS sensitive content services such as music and non-real-time or low bit-rate video.

Approved output domain (AOD)

The devices in this domain are connected to the ASD using operator-approved output interfaces. When the content flows from the ASD to the AOD, the network operator-specified usage rules are asserted across the interface. Currently, 5C over 1394 and HDCP over DVI (or HDMI, high definition multimedia interface) are approved digital output interfaces for North American cable deployments. For example, a possible interface that MAY be established is a DRM interface that allows the communication of content and usage rules to a third-party DRM system, separate from the DRM of the network operator.

A cable operator relinquishes direct control over the content once it is transferred over the AOD. This is a key difference between authorized service domain and approved output domain.

A device MAY receive content from the ASD over an approved interface. There is no mandate that the device meet any other requirements related to QoS and device discovery. However, some AOD devices will be able to participate in the guaranteed service domain as it relates to device discovery and QoS. All devices in the AOD will be able to receive protected non-QoS sensitive content that has network operator-enforced usage restrictions that depend upon the approved output interface.

Removable media such as recordable DVDs, flash cards and CD-Rs will typically be found in the AOD.

Best effort domain (BED)

Devices and physical layer segments not conforming to the requirements of the above three defined domains MAY still be discovered and participate in services that do not require content protection or guaranteed quality of service.

Intersection of GSD and ASD

The GSD and ASD are independent; a device can belong to neither, one or the other, or both. The devices that belong to both GSD & ASD can provide QoS guarantees and can authenticate themselves and support the in-home DRM. Such devices represent a higher level of compliance and MAY be able to receive high-value content with network operator-enforced usage restrictions.

Intersection of GSD and AOD

The GSD and AOD are independent; a device can belong to neither, one or the other, or both. The devices that belong to both GSD & AOD can provide QoS guarantees for the content that flows from ASD to AOD over approved interfaces. Such devices will be able to receive protected QoS-sensitive content with network operator enforced-usage restrictions depending upon the approved interface.

Exclusivity of ASD & AOD

The ASD and AOD are mutually exclusive. A device can belong to only the ASD, or AOD, or neither.

Table 2 summarizes various functional requirements for devices in different domains.

Table 2 – Functional requirements of different domains and offered services

Functionality[a)]	**ASD – Network operator controlled flexible usage rights**	**GSD – Guarantees of QoS, Consistent UI**	**AOD**	**ASD+GSD**	**AOD+GSD**	**BED**
Security	Authentication plus CA or in-home DRM based on NG-STB-A CSP	None	Approved output interface security	Authentication & CA or in-home DRM	Approved output interface security	None
QoS	Prioritized QoS (UPnP QoS) – **Optional**	Parameterized QoS (IPCable2Home or UPnP)	None	Parameterized QoS (IPCable2Home or UPnP)	Parameterized QoS (IPCable2Home or UPnP)	None
Consistent UI	Desired	Yes	None	Yes	Yes	None
Management	IPCable2Home PS[b)] (for Gateway) or IPCable2Home BP[c)] (for client) – **Optional**	IPCable2Home PS (for gateway) or IPCable2Home BP (for client)	Selectable output control	IPCable2Home PS (for gateway) or IPCable2Home BP (for client)	IPCable2Home PS (for gateway) or IPCable2Home BP (for client)	Selectable output control
Discovery	UPnP/DLNA	UPnP/DLNA	None	UPnP/DLNA	UPnP/DLNA	None
Services	Protected, Non-QoS sensitive content services with full flexibility to set usage rights	Unprotected, QoS sensitive content services e.g., interactive game-playing, voice, video phone	Protected, non-QoS sensitive content services with limited flexibility to set usage rights	High-value content services with full flexibility to set usage rights	Protected, QoS sensitive content services with limited flexibility to set usage rights	Unprotected, non-QoS sensitive content

Table 2 – Functional requirements of different domains and offered services

a) This table assumes that all the devices in these domains have a home networking interface.
b) IPCable2Home PS includes the functionality of UPnP Control Point.
c) IPCable2Home BP is a superset of UPnP QoS and other UPnP functionality.
d) All UPnP and DLNA descriptions in Table 2 are informative.

If NG-STB-A home network management is unavailable, NG-STB-A-compliant CPE devices SHOULD be designed to continue to operate, although possibly at a reduced level. Programmable devices MAY be conforming when running certain applications, and non-conforming when running other applications.

This proposed NG-STB-A structure anticipates running compatible secure clients on PCs so that rights-managed content can be exchanged between SVDs and PCs. An example of an application might be to watch on a PC video from a DVR housed in an SVD. Alternatively, a PC could take on the role of a video or music server allowing for SVD access to the PC content. For example, a PC could serve as an advanced home answering machine or caller ID information could be displayed on a TV.

6.5.2 Digital rights management

Content is delivered to each SVD within the authorized service domain using the head-end managed CA. Each SVD includes peer-to-peer protocol support with copy protection provided by in-home networking digital rights management (DRM). The NG-STB-A plan assumes that each device includes secure clients that can mutually authenticate to each other using digital signatures or a standardized key exchange technology. The CSP MAY provide bridging capabilities between the cable network CA and the home network DRM.

In this proposed NG-STB-A in-home structure, an SVD on the network would have access to the features and content on any other device on either the GSD or ASD networks. By employing standardized algorithms for content encryption at the rights management system (RMS), the RMS shall be capable of supporting multiple video streams for recording, real-time viewing and multiple viewing sessions.

The NG-STB-A RMS will be capable of translating entitlements and copy protection states and transporting these rights throughout the in-home network. The NG-STB-A RMS will employ new concepts and technologies in the area of key management while functioning with existing legacy systems using key sharing or reconfiguration criteria. Keys and entitlements MAY be translated from the video stream copy control information (CCI), ECMs, and EMMs to be loaded directly into the decryption engines without exposure in the content decryption engine on the home network device.

In NG-STB-A's proposed in-home rights management system, a Rights file that contains access criteria to various service tiers and a content decryption key typically would be signed and encrypted. The content key would be the key used to decrypt the content and MAY need to be changed on a variable periodicity. The entitlements and copy protection restrictions would be decrypted and checked in the CPE against the customer access criteria in order to provide authorization. If authorization were granted, the content key would be issued by the CA element and used to decrypt the content at the CPE device on the home network.

The NG-STB-A RMS will perform all key generation processing, encryption, decryption, digital signature processing and key exchange algorithms inside tamper resistant hardware/software, which will be designed to completely prevent the modification or unauthorized disclosure/analysis of the processing, critical security parameters, and private keys.

6.5.2.1 CA-DRM linkage

The network CA will be responsible for managing the NG-STB-A RMS. All third-party DRMs MUST be approved as an acceptable output before the NG-STB-A RMS will perform a hand-off of the content and rights. The third-party DRMs will be treated as part of the approved output domain as defined above. To support any third-party DRM system not associated with the network CA, the NG-STB-A RMS will be used to translate rights into the third-party DRM. In addition, the NG-STB-A RMS will be used to authenticate any third-party DRM device before sharing content and rights information. The CSP will support this hand-off process.

6.5.3 Content sources and clients

The in-home network architecture is specified to aid the seamless interoperability of content sources and clients. Content stores (i.e., music, photo and video libraries) that exist on networked clients MAY be discovered, catalogued, and streamed to other devices on the home network, and even optionally offered to authorized devices outside of the home network.

A key objective for the in-home network architecture is to enable a convenient, unencumbered home network platform for the consumer while maintaining the integrity of protected (restricted) content within the authorized service domain (ASD). Several key assumptions are embedded within this framework:

- All content transport between devices connected to the in-home network is via IP (Internet Protocol).
- The network architecture will transport many different types of media, including video, audio, "stills" (e.g., JPEGs) and data.
- The network architecture will provide simultaneous support for network operator-supplied protected content and services, alternate-source protected content (e.g., a third-party music DRM solution), and non-protected content (regardless of source).

While there MAY be several in-home network architectures that achieve the desired goals, a number of key technical points MUST be considered:

- Only authorized (i.e., certified) devices MAY be part of the ASD.
- The architecture MUST support transmission and storage of both network operator delivered content and non-network operator delivered content.
- Network operator-delivered protected content MAY be stored and consumed within the ASD.
- Network operator-delivered protected content MAY only exit the ASD through approved outputs.
- Protected and non-network operator-delivered content MAY be consumed and stored within the ASD.
- If the communications link with the cable network is disrupted, the in-home network architecture SHOULD still function for up to a certain length of time, with the time-limit set by the cable operator.

6.6 Advanced digital advertizing

NG-STB-A will support program insertion and play out technologies on various media from analog to digital ad insertion, and it will enable a wide variety of advanced advertizing models[1] such as:

- Digital-into-digital advertizing;
- Targeted and addressable advertizing;
- Interactive advertizing (on all services);
- DVR advertizing:
  - Long form: Content distributed and stored locally on the DVR.
  - Replacement: Refresh previous recorded ad content on the DVR.
  - Network DVR: Refresh previous recorded ad content on the DVR.
- VoD advertizing:
  - VoD content advertizing support: Bumper or interstitial advertizing content.
  - Local VoD ad insertion: Support for local ad insertion in ad-supported VoD content.
  - VoD publishing for an advertizer.
- Data collection across all advertizing services to include synchronized content.
- Insertion of national, regional and local advertizing at all points within cable physical plant as well as from sources outside the plant such as the Internet.

7 Customer premises

This clause of the NG-STB-A plan describes the essential elements of NG-STB-A-compliant video and non-video CPE devices. Suppliers are welcome to develop innovative variations and combinations of these elements. The intent of the NG-STB-A plan is to provide equipment suppliers with a platform that is as unconstrained as possible.

7.1 Overview

The customer premises network segment involves significant opportunities and challenges vis-à-vis consumer electronics manufacturers, CE retailers, and regulations, as well as representing the largest overall investment given the large number of devices. CPE will vary in their capabilities. For example, options include support for gateway services in the home data network, and digital video recording (DVR). Table 3 summarizes key features and attributes of a range of NG-STB-A compliant CPE devices.

[1] Advanced digital advertizing would be an attractive service for the service operators who want to expand their business structures. It is required to harmonize business schemes between service operators and broadcasters.

Table 3 – CPE feature overview

	Baseline SVD	Extended SVD (Non-gateway)	Extended SVD (Gateway)	Media client
CSP support	✓	✓	✓	✓
Extended SVD functions other than gateway (e.g., DVR, security card, display)		✓	✓	TBD
Home network gateway (IPCable2Home portal services, UPnP control point)			✓	
Home network client (IPCable2Home boundary point, UPnP signalling, UPnP QoS)	✓	✓		✓
J.200 series capable	✓	✓	✓	Optional
USB 2.0 and/or Ethernet host	✓	✓	✓	✓
NOTE – All UPnP descriptions in Table 3 are informative.				

7.2 Subscriber video devices (SVDs)

Subscriber video devices (SVDs) include devices with a minimal core capabilities, up to devices that provide a richer set of capabilities.

This equipment will be provided either by the operator or at retail by consumer electronics suppliers. SVDs will operate as set-top or set-back boxes. Other SVDs could include two-way digital TV sets.

These devices are designated as SVDs because each provides more than the conventional set-top box functions, such as reconfigurable CA via an CSP, support for an advanced video codec, support for multiple video transport options, and for networking over the in-home network. Each SVD can access resources in or provide resources to other devices on the network. In other words, all SVDs MAY act as source or destination of content within the in-home network. Thus through the in-home network, the lowest order device can deliver some of the features and capabilities of the highest order device. The system compliant with this Recommendation provides for copy-protected and rights-managed interchange of content between any of the SVDs on the home network.

Figure 8 illustrates the SVDs' ability to network to other SVDs and to other compatible devices.

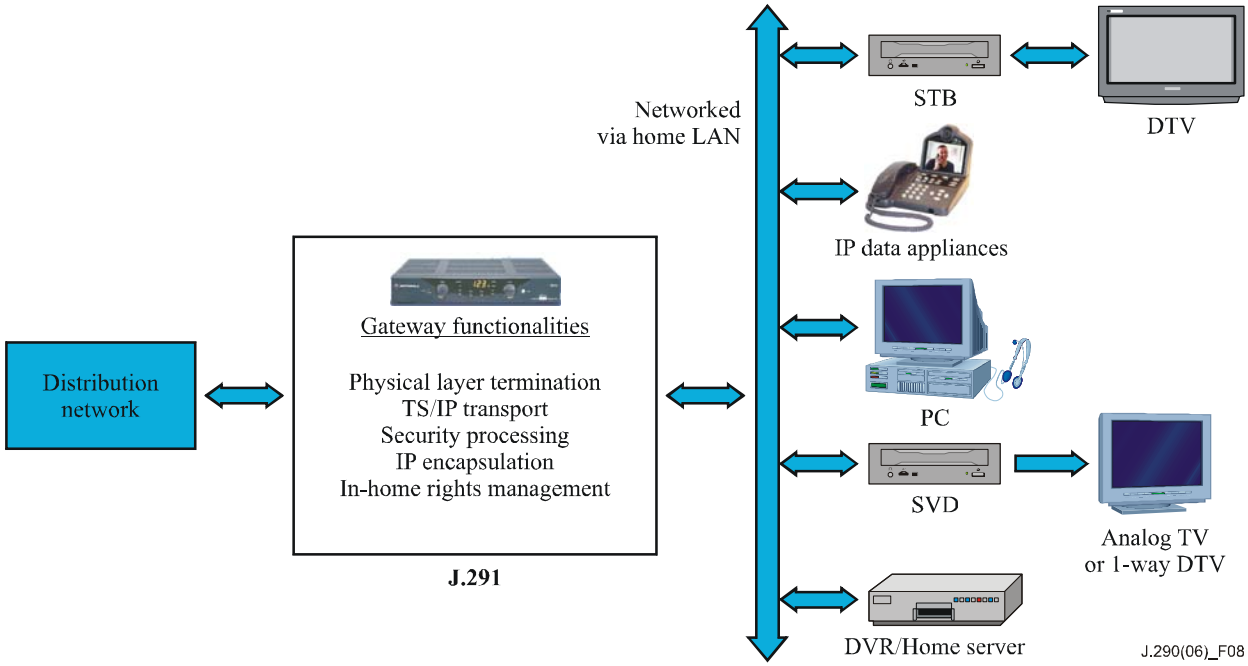


Figure 8 – Examples of CPE deployment for subscriber with IP-based home data network (In-home DRM system is applied)

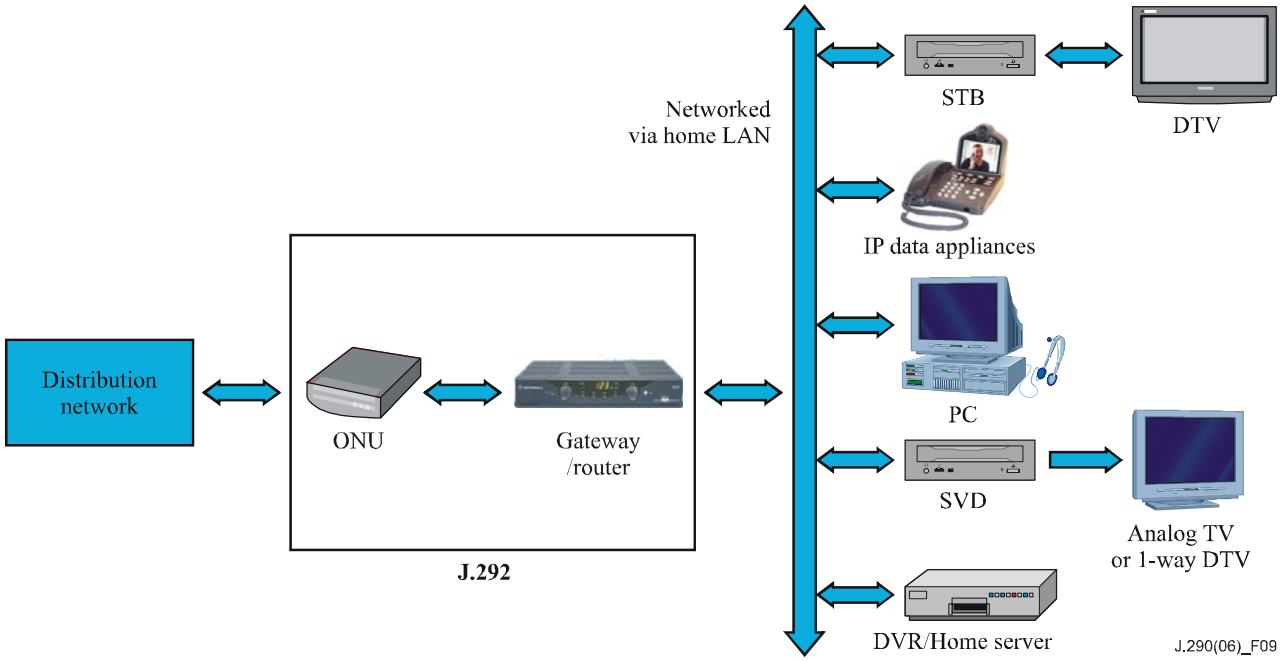


Figure 9 – Examples of CPE deployment for subscriber with IP-based home data network

SVDs have as their principle function the delivery of video entertainment. Additional devices MAY offer video communications and MAY be networked with SVDs, such as video conferencing devices and other forms of IP appliances. These devices will be defined in the market and are not detailed in this Recommendation.

The baseline SVD includes the following functionalities:

- All digital, standard definition video decode (MPEG-2 and advanced codec).
- Stand-alone device (does not function as a TV).
- Supports both 1-way and 2-way services.
- J.200 series capable – The intent is to have SVDs run J.200 series middleware, dependent on reasonable licensing of the J.200 series technology.
- Compatible with the security model, as described earlier, with internal CSP.
- Video MAY be delivered as either MPEG transport packets over QAM, or over IP-based network. In addition, video MAY be delivered over in-home network.
- Supports MPEG-2 as well as the advanced video codecs described earlier.
- Supports audio coding, BC (ISO/IEC 13818-3) and/or AAC (ISO/IEC 13818-7) audio.
- Basic support for in-home networking is provided by the presence of a USB 2.0 and/or Ethernet (100BASE-TX) port. Various networking adapters can be attached to this port to provide PHY/MAC layer functionality for different in-home networking architectures (e.g., WiFi, CAT5).
- The baseline SVD is a guaranteed and authorized service domain device, as defined earlier.
- {informative text: The device will function as an in-home network client, which requires the device to function as IPCable2Home Boundary point and to provide UPnP signalling and UPnP QoS.}
- The device will also support an expansion port (type to be determined) that allows hardware renewability of the internal security mechanism.
- Video output is provided by a single RF composite video port, high definition video output or approved digital video interface.

Baseline SVDs MAY assist in the transition to all-digital services. Used for this purpose, baseline SVDs will allow subscribers who have analog TVs and other analog devices (e.g., VCRs) to continue to receive their existing services in a manner that is as transparent as possible even though the formerly analog channels will have been re-assigned to carry digitally compressed signals.

Baseline SVD functions are illustrated in Figure 10.

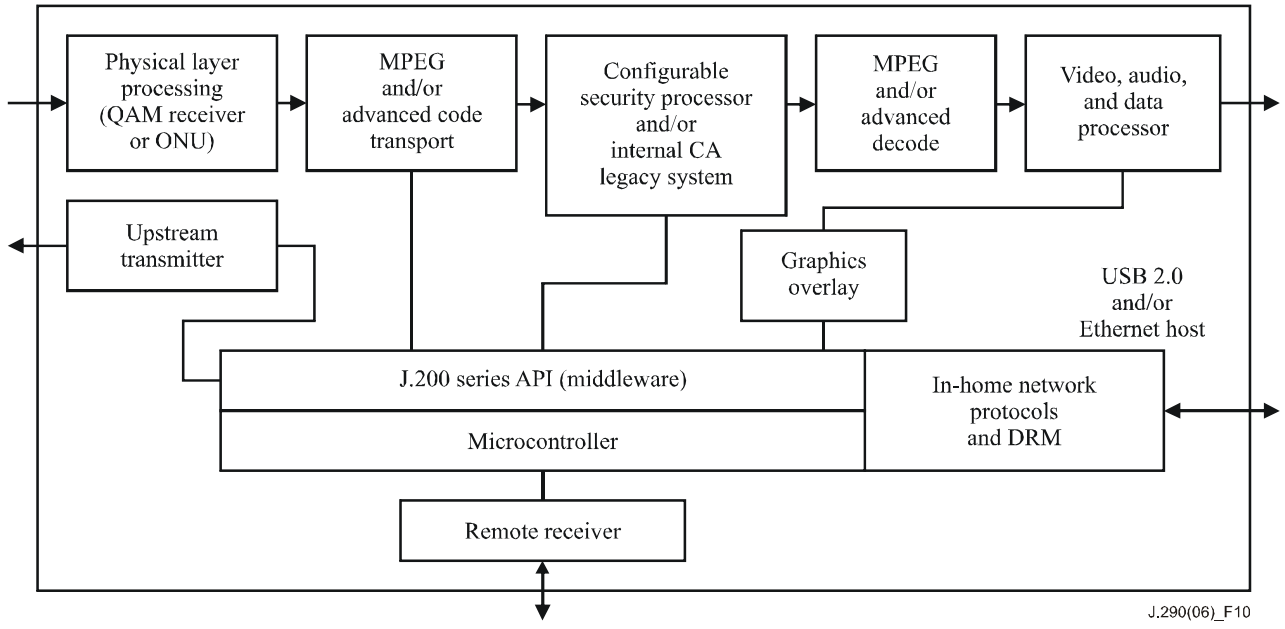


Figure 10 – Baseline SVD functions

SVD suppliers MAY provide additional extended functions in higher-end devices. For example, these features MAY support:

- High definition video signals, including the following authorized digital outputs: DVI (or HDMI) with HDCP and 1394 with DTCP.
- Support for receiving and processing multiple video programs.
- DVR functionality, including both internal and external storage.
- {informative text: Gateway functionality, which requires the device to support portal services and function as a UPnP Control Point.} In addition, devices that support gateway functionality shall support the ability to enable and disable this feature to avoid conflicts if multiple gateways are installed on the same network.
- Security card support.
- On-board support for networking connectivity (e.g., WiFi, CAT5). This support is in addition to the required baseline USB-2 port and associated network support.
- Associated display such that SVD functions as two-way DTV.

While this Recommendation does not require analog tuner support, an SVD that does include this feature would have to comply with applicable requirements concerning DTV devices that incorporate analog TV.

Figure 10 shows capabilities of a baseline SVD plus extended features that MAY be found in higher-end SVDs.

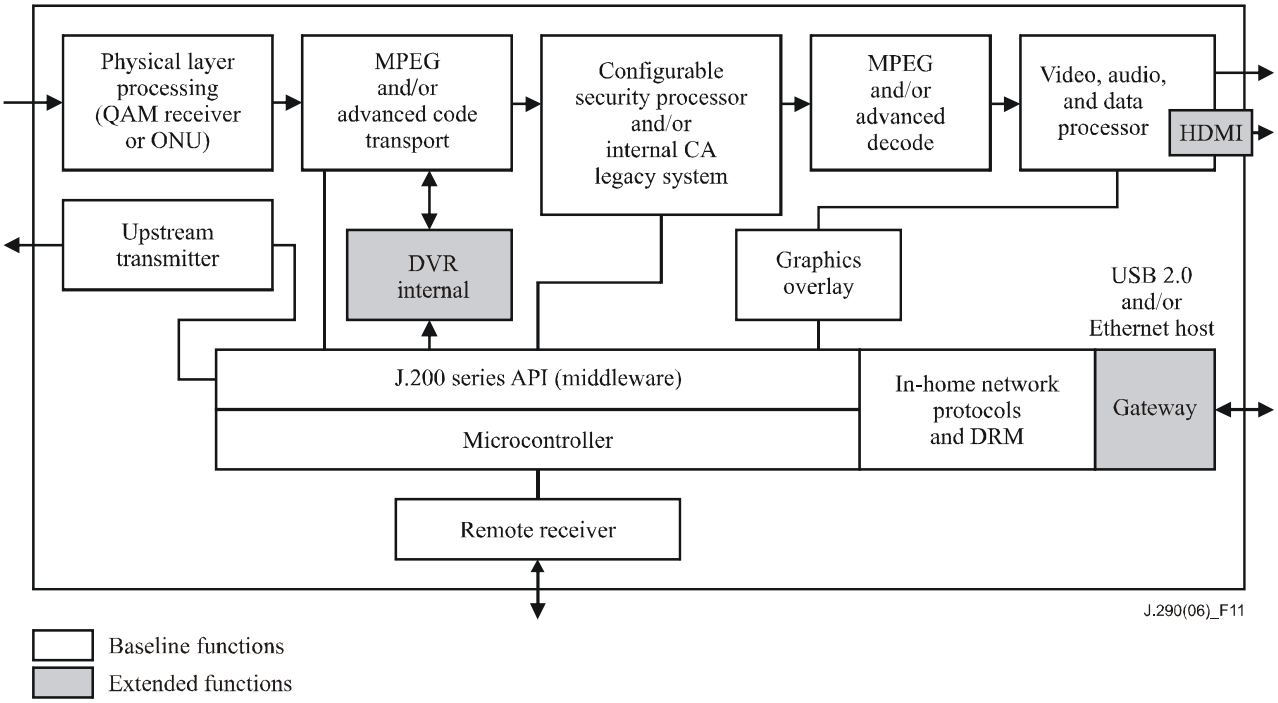


Figure 11 – SVD functions with possible extension

All SVDs will be required to meet appropriate content protection compliance and other rules to ensure that services delivered in the guaranteed and authorized service domains are delivered as intended by the cable operator.

7.3 Other CPE devices

The NG-STB-A plan describes examples of next generation network CPE in addition to options for SVDs.

7.3.1 Video media client

The video media client is a "tuner-less" device that is designed specifically to connect to other SVDs on the in-home network in order to receive video content. It MAY provide a rich application environment through on-board middleware and applications, or MAY instead present a "remote user interface" that is driven by the SVD serving its content.

Some of the baseline features for the media client include:

- Standard definition, digital only.
- In-home DRM support as provided by CSP.
- In-home networking client support.
- Device MAY function as an ASD device or as a GSD/ASD device.
- MPEG-2 and advanced codec support.
- Companion universal remote control or controlled via remote that communicates with source device.
- USB 2.0 for providing network connectivity.

Optional features of the media client include:

- High definition video support with associated approved digital outputs.

7.3.2 Non-video CPE

Given the proliferation of new video, data, and multimedia services, and increasing convergence between these services, it is likely that additional next generation non-video CPE will be developed that will connect directly and indirectly to the cable network.

Device manufacturers are already incorporating multiple functions into cable modems such as various combinations of layer 3 router firewalls, data hubs, voice telephony MTAs, and home networking transport (e.g., WiFi, HPNA, HomePlug, etc.), and are likely also to integrate some of the next generation network functions into future cable modems and other subscriber devices. Next generation network functions that are candidates for creative integration into CPE include in-home networking within and between the guaranteed and authorized service domains, and IPCable2Home functions that allow management and visibility of subscriber devices from the head-end.

Non-video CPE example: Multifunction gateway

The core of this device is currently available, including a cable modem, layer 3 router firewall, and a voice telephony MTA. A next generation version of this device would add IPCable2Home capabilities of visibility and remote management from the head-end. It would also include a bridging feature allowing interaction between SVDs compatible with the in-home network protocols and CPE on the in-home data network. Such a device would support applications such as:

- Allowing PCs with a suitable bridge to use the coax network as a means to access high-speed data services.
- Allowing consumer-owned PCs or servers on the in-home data or coax network to communicate displayable messages or control messages to SVDs.
- Enabling the telephony MTA to send caller ID messages (or other messages) to SVDs.
- Allowing SVDs to access billing or service information regarding subscribers' interactive multimedia/data services.

8 Security

8.1 Security hardware element

The next generation configurable security processor (CSP) hardware element will support the following several standardized algorithms for transport stream encryption at the head-end and decryption at the CPE. The following lists examples of the standardized algorithms that MAY possibly be supported by CSP.

- Data encryption standard (DES) – Electronic code book (ECB), Cipher block chaining (CBC) and other modes for residual blocks (Federal Information Processing standard, FIPS 46-2).
- Triple DES – ECB, CBC, and other modes for residual blocks (FIPS 46-2). This includes support for both two-key and triple-key encryption.
- Advanced encryption standard (AES) (Rijndael).
- DVB – Common scrambling algorithm (CSA).
- Multi2 (ISO/IEC 9979).

The CSP hardware element will be configurable ("renewable") and will employ technologies to support the decryption of at least the following four types of secure transport streams:

1) Triple DES – supporting ECB and CBC at a minimum as well as two-key and three-key modes.
2) DVB-CSA – as defined in DVB.
3) AES – using a new standardized key architecture with standardized ECM, EMM, unit seed, and unit ID methodology.
4) B-CAS – as defined in ARIB, which will be supported by the security cards.

Note that the CSP shall be defined in such a way that silicon providers will not be required to obtain licences for some security systems in order to build CSP functionality into their products. The CSP will be defined in a manner such that compliant silicon will be able to run the appropriate algorithms that are downloaded to the CSP when connected to the cable plant or that are provided by the security card.

8.2 Authentication

The hardware components of the CSP shall be capable of securely storing and performing digital signatures using various sizes (e.g., 1024, 2048 and 4096-bit) of RSA keys in hardware registers. The next generation components shall be capable of securely generating digital signatures inside tamper resistant hardware without exposing the private keys or the processing needed to generate the hash, and encrypt. The next generation network shall be capable of digitally signing messages used for authentication and providing integrity using a secure SHA-1 hash.

8.3 Key encryption keys

CSP hardware shall be capable of securely storing key encryption keys which could be in the form of symmetric or, preferably, asymmetric cryptography. The ability to use key pairs for transporting encrypted keys among CPE devices and to head-end devices is very desirable.

8.4 Unit address

Each CSP used in a CPE device shall be uniquely identified with a completely unique ID. This ID is used to address each CPE device for receipt of the entitlements for that specific CPE device. In some implementations, a MAC address MAY be used for this ID. The unit ID shall be able to be provided also by the security card.

8.5 Tamper resistance

The CSP shall be designed to meet FIPS-140 Level 2 security in most areas with some areas (hardware reconfiguration and firmware upgrades) requiring FIPS 140-2 Level 3 security which has tamper resistance in compliance with a certain criteria such as FIPS-140 Level 2 or Level 3. It shall also employ the latest technologies (for example, power plane distribution and cell fragmentation) in tamper resistance to prevent electron microscope analysis and surface shaving attacks.

8.6 Key management

The key hierarchy includes multiple keys as illustrated in Figure 12. In addition, Figure 13 illustrates decryption scheme where the security card is used.

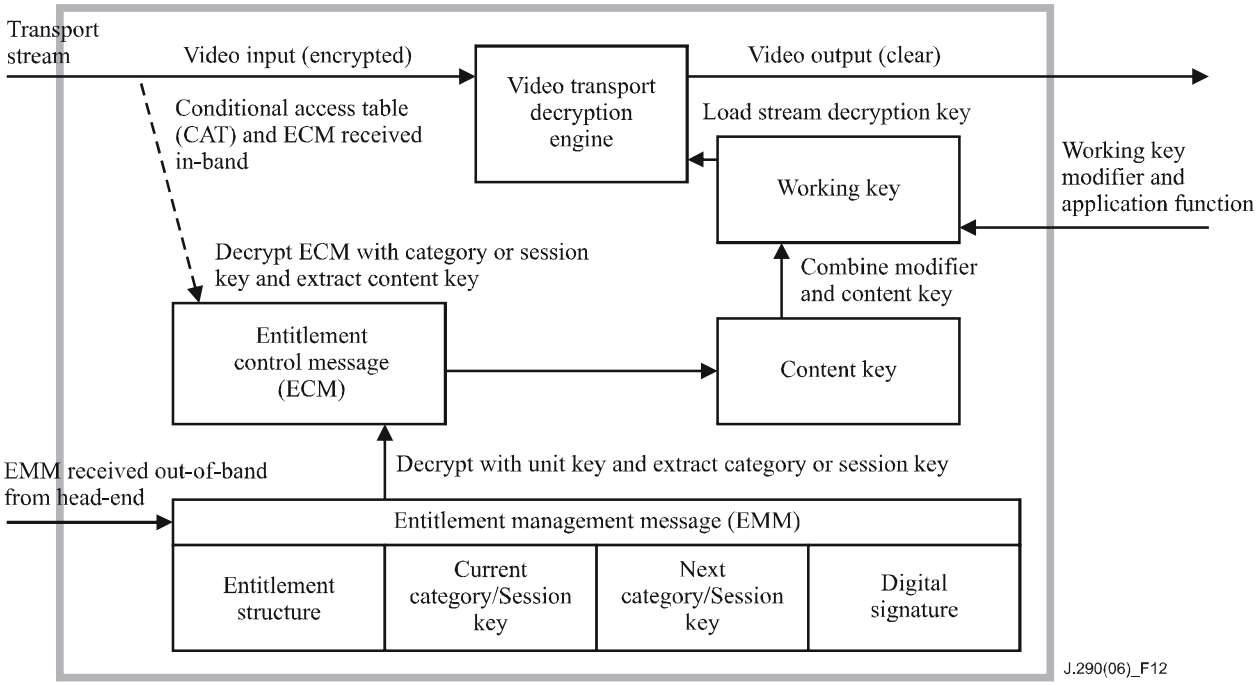


Figure 12 – Key hierarchy

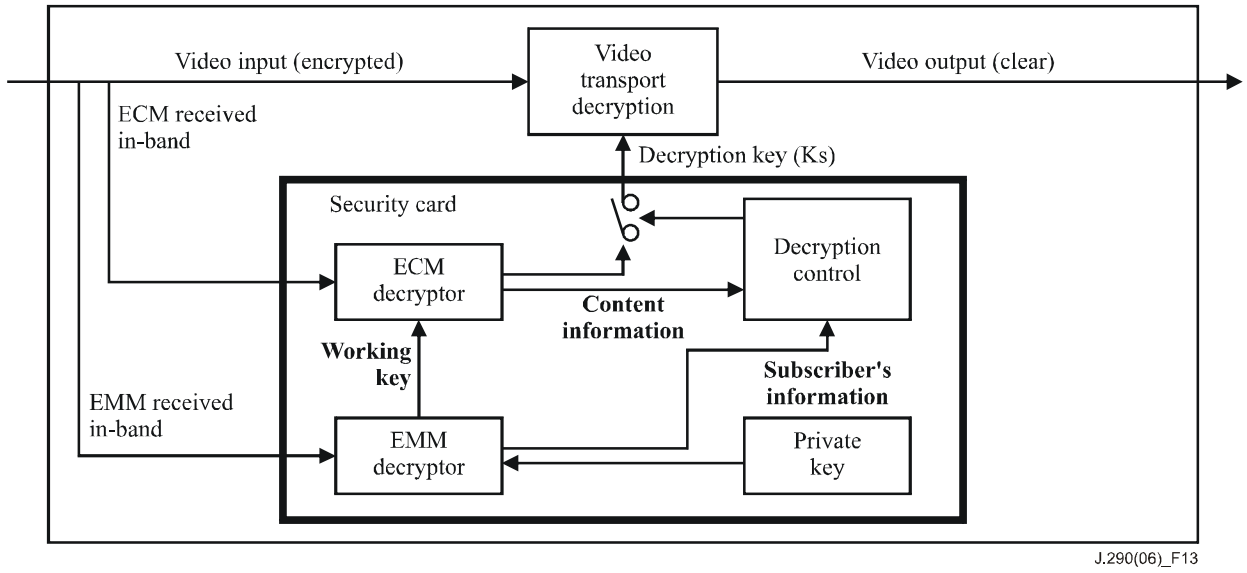


Figure 13 – Signal flow in use of security card

The CSP software and hardware SHOULD be designed to employ new concepts and technologies in the area of key management while functioning with existing legacy systems using key sharing or reconfiguration criteria. The CSP module shall support the following schemes:

1) Decrypted keys extracted in the CPE from the video stream and ECMs and EMMs shall be loaded directly into the decryption engines without passing over external interfaces including the transport decryptors.

2) ECMs and EMMs are extracted from the transport stream (in-band) and they shall be transferred directly into the security card device, where the working key is decoded and the stream decryption key is calculated.

8.6.1 Entitlement control messages (ECMs)

An ECM is an encrypted message that contains access criteria to various service tiers and a control word (CW). The control word is the seed key that is modified and used to decrypt the video stream and shall be able to be changed on a variable periodicity or in effect converted into a "working key". The ECM is decrypted and checked in the CPE against the access criteria in order to provide authorization. If authorization is granted, the CW will be released, converted to a working key and used to decrypt the content at the CPE device.

8.6.2 Entitlement management messages (EMMs)

Encrypted messages are created in the head-end and sent to the next generation CPE to authorize the CPE device for certain access criteria to content. The EMM contains the actual authorization data and shall be sent in a secure method to each CPE device. The EMM is addressed to a single CPE device and is uniquely encrypted so that only that device can decrypt the entitlements and validate them. The CSP shall support DigiCipher II, PowerKey, NDS, Nagravision, NCAS and B-CAS entitlement mechanisms and formats.

8.7 Copy protection

If an NGNA device employs a security card, the interface shall implement renewability and configurability in compliance with SCTE-41. In addition to supporting the current SCTE-41 transport stream requirements, CSP shall be capable of decrypting the following three types of standardized secure transport streams. Examples are listed as follows:

1) Copy protection – DES (as defined in SCTE-41, with the additional option of using DES CBC mode in addition to EBC mode).

2) Triple DES – Supporting ECB and CBC at a minimum.

3) AES – Using a new standardized key architecture with standardized ECM, EMM, key encryption keys and unit ID methodology.

4) Multi2 – Supporting ECB and OFB.

9 Head-end network architecture

Benefits of head-end integration, which is consistent with the version of NG-STB as an integrated multimedia, will include:

- More efficient use of system resources;
- Facilitate interworking of network elements supplied by multiple vendors to enable more open competition, to extend the service life of the installed base, to provide flexibility for new service introductions, and to provide scalability to accommodate a range of system sizes;
- Provide a platform for innovation and rapid service creation.

9.1 Head-end network delivery architecture

Figure 14 describes the overall head-end network delivery architecture.

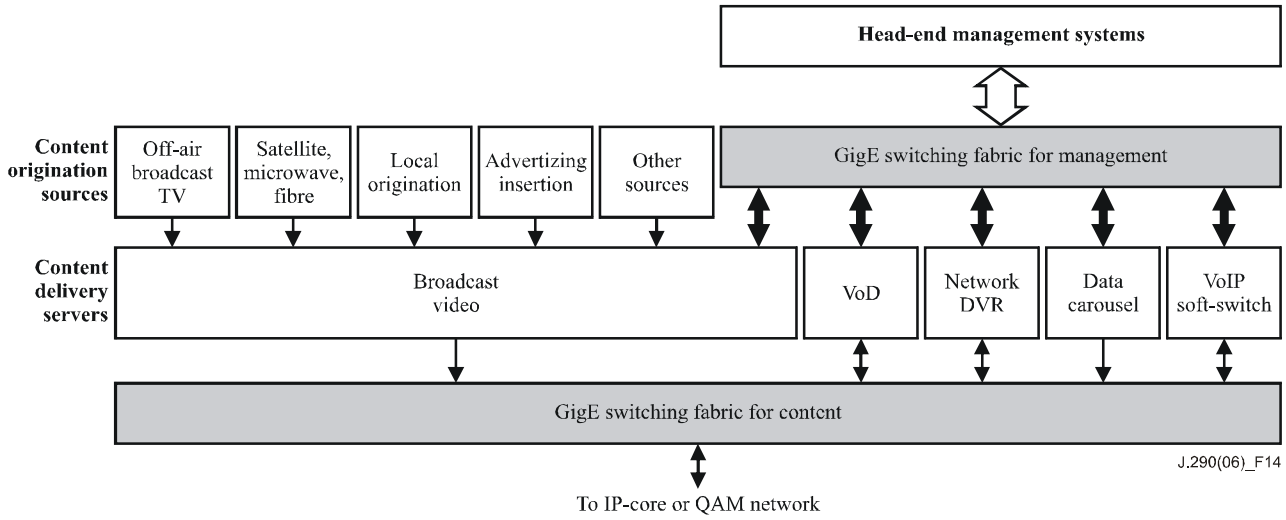


Figure 14 – Head-end network delivery architecture

Key next generation features of head-end network architecture include:

- The head-end network enables the delivery of digital video traffic and generic IP datagram traffic over a common head-end network infrastructure.
- Applications are managed across all services by session and resource management systems, which shall have the capability to operate autonomously in the event of communications failure with back-office systems.
- The control of the head-end servers are separate so that common third-party resource management and network operations applications can manage the head-end as an integrated system rather than as stand-alone service specific subsystems.
  - *GigE switching fabric for content*: The GigE switch fabric will be under the control of a network resource manager for content distribution and will ensure that any server can have data switched to any content source easily between content servers.
  - *Session and Resource Management system*: Application managers, session managers and resource managers will have functionality that gives the operator the ability to control and monitor traffic loads, QoS needs, and subscriber entitlements.
  - *Ethernet or GigE switching fabric for management*: The switching fabric will provide a standard management plane interface by means of an Ethernet or GigE switching fabric so that each service can be managed and controlled by external IT management systems via open APIs.
- IP is used for the network transport of control and management messages to CPE. The set of signalling protocols for video-based services is likely to include DSM-CC (digital storage media – command and control), RTSP, SIP, NCS/MGCP, and potentially XML-based "web services" protocols such as SOAP.

9.2 Session and resource management architecture

In order to satisfy the desire for common resource management across all services and applications, a framework for session and resource management is needed, as shown in Figure 15.

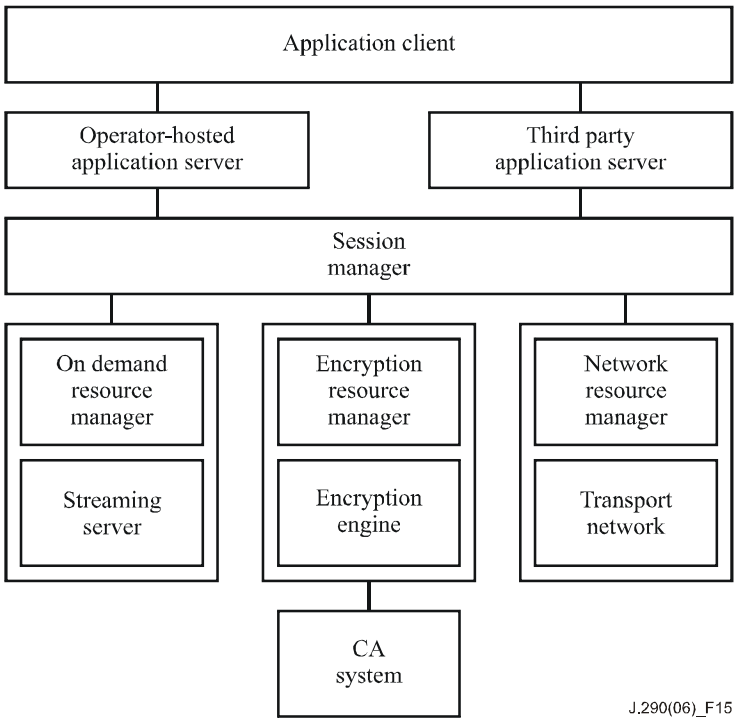


Figure 15 – Session and resource management framework

To increase efficiency in use of resources, the next generation head-end employs a session-based resource management architecture. Creation of such an architecture requires close control of the resources to ensure their efficient use. In an attempt to provide a generic framework, the session and resource management function is split into three domains: application, session and resource management. Each of these domains is discussed in detail in the following clauses.

9.2.1 Application manager

An application manager plays a coordinating role involving application signalling as well as interaction with the head-end resource management framework via the session manager. In most cases, the application manager is expected to be owned and operated by the service operator. However, there MAY be cases where the application manager is in fact outside the service operators control. Examples of operator-hosted application managers would be VoD services and telephony services. Examples of third-party application managers could be streaming audio/video, and gaming services.

In a VoD system, it is the session manager's responsibility to maintain and manage the life cycle of session rather than the application manager. For such cases, the client can set up a session directly with session manager or proxy through the Application Manager. Since the Application Manager does not need to manage the session itself, this architecture allows for different applications to use the same session manager for multiple on-demand services.

For IP-based applications and services, the typical implementation actually integrates the session manager into the application server; while they MAY reside in the same physical box, they are considered logically separate.

9.2.2 Session manager

The role of a session manager is to broker head-end resource requests on behalf of the application manager. While an application manager only knows the QoS needs for the session, the session manager needs to understand how to translate those QoS needs into the various system resources as well as identify non-QoS based resources the session MAY also require (i.e., encryption resources, server resources).

It is important to note that multiple instances of a session manager MAY exist in a given head-end and each session manager communicates with a set of resource managers. The set of resource managers a session manager communicates with is determined by the applications for which the session manager is expected to handle resource requests. Such an architecture allows for more rapid introduction of new services by not requiring a central 'super' session manager be upgraded every time a new service is trialled. It is envisioned that a given application manager will talk to a single session manager except where redundant session managers are implemented. Session managers need not be able to support all session types; in fact, it is likely that separate session managers will be deployed for different types of sessions, e.g., VoD versus switched broadcast.

The session manager will not make business-based policy decisions. Rather, it will coordinate application resource needs acting under the assumption that the request comes from a valid device and from a subscriber authorized to request such services. It MAY make resource-based policy decisions based on the current status of the system resources.

9.2.3 Resource manager

The resource manager deals primarily with allocating the resources necessary to satisfy a session request. Each head-end resource will have an associated (logical) resource manager. It is the resource manager's task to track all consumption of resources and allocate new resources as needed. Examples of resource managers are:

- On demand resource manager – Streaming server resources.
- Encryption resource manager – Stream encryption resources.
- Network resource manager – Switched IP network resources.

To further explain the session and resource management framework, the following description is referred:

- A VoD service follows the following flow: The client starts the session by making a request for a VoD asset to the application manager. Upon receipt of such a request, the application manager will forward the request to the appropriate session manager. The session manager will negotiate with multiple resource managers to obtain the corresponding resources. These MAY include (not necessarily in any order) server resource, network resource, encryption resource and edge resource.

10 Quality of service

Quality of service can be provided by generously over provisioning a network so that all packets get a quality of service sufficient to support QoS-sensitive applications. This approach is relatively simple, and is economically feasible for many broadband networks. The performance is reasonable, particularly if the user is willing to sometimes accept some degradation. For narrow-band networks more typical of enterprises and local offices, however, the costs of bandwidth can be substantial and over provisioning is hard to justify. Networks generally require following four key factors to establish end-to-end QoS in order to support both time critical services and high quality video services.

- Delay;
- Jitter;

- Packet loss;
- Bandwidth.

QoS functions provided in routers or switches MUST control these key factors and transmit packet to next hop. In these situations, two distinctly different philosophies are developed to satisfy the requirements.

10.1 IntServ and DiffServ

Early work used the "IntServ" philosophy of reserving network resources. In this model, applications used the resource reservation protocol (RSVP) to request and reserve resources through a network. While IntServ mechanisms do work, it is realized that in a broadband network typical of a larger service provider, core routers would be required to accept, maintain, and tear down thousands or possibly tens of thousands of reservations.

The second and currently accepted approach is "DiffServ" or differentiated services. In the DiffServ model, packets are marked according to the type of service they need. In response to these markings, routers and switches use various queuing strategies to tailor performance to requirements. At the IP layer, differentiated services code point (DSCP) markings use the 6 bits in the IP packet header. At the MAC layer, VLAN IEEE 802.1Q and IEEE 802.1D can be used to carry essentially the same information.

10.2 End-to-end QoS and service applications

Considering services that next generation STB SHOULD provide, the QoS mechanism MUST satisfy the requirement for high quality video and time critical service like VoIP. The guaranteed QoS mechanism, as defined in clause 6.5.1, MUST be implemented to do so.

Provisioning of guaranteed QoS mechanism differs in service application areas and in session structures among various networks. Type of QoS in this Recommendation is classified into three types: Session-based QoS, pre-provisioned Bandwidth QoS and prioritized QoS. The definition of each QoS type is shown as follows:

- Session-based QoS: Signalling is required for QoS route setting. It is secured at every time of service activation and released its bandwidth when service is closed.
- Pre-provisioned Bandwidth QoS: Signalling is not always required for QoS route setting. It is the type of QoS that reserves required bandwidth exclusively regardless of type of traffic or its presence.
- Prioritized QoS: In certain cases, prioritized QoS can satisfy the guaranteed QoS requirements as defined in clause 6.5.1 by over provisioning of bandwidth. Such over provisioning satisfies bandwidth constraints and in most cases will also satisfy jitter and delay if packet priority is strictly maintained without any interruptions due to bandwidth or processor limitations.

Note that service in this Recommendation means service from user's perspective and does not mean either ISP or telecommunication carriers.

Table 4 shows typical services and QoS required for media independent (MI) architecture (ITU-T Rec. J.292) and Cable architecture (ITU-T Rec. J.291).

Requirements for each service SHOULD be referred to ITU-T Rec. J.193 (2004). As for the relationship between service and QoS, refer to Appendix I.

Table 4 – Typical services and QoS required

Service	MI architecture	Cable architecture
Broadcasting TV	Pre-provisioned bandwidth	Pre-provisioned bandwidth
VoD	Session-based	Session-based
VoIP	Session-based	Session-based
Video phone	Session-based	Session-based
Internet	Best effort	Best effort

Table 5 depicts a relationship among QoS type, signalling and bandwidth assignment. Signalling here means all signal transactions for session setting between concerned devices.

Table 5 – Relationship among QoS type, signalling and bandwidth assignment

QoS type	Signalling	Bandwidth assignment
Session-based QoS	Applicable	Triggered by session, reserves bandwidth
Pre-provisioned bandwidth QoS	Not Applicable	Fixed bandwidth
Prioritized QoS	Not Applicable	Prioritized queuing, regardless of bandwidth Optional for DiffServ type QoS having bandwidth aspect

10.3 Requirements for QoS bridge

As shown in Figure 16, it is required logically to match QoS mechanisms of segment A (i.e., access network) and segment B (i.e., home network), that usually differs from each other. QoS bridge enables communication between them and its logical entity SHOULD be implemented into HA device in ITU-T Rec. J.190 or residential gateway.

10.3.1 Goal of QoS bridge

The goal of QoS bridge is to establish the end-to-end QoS route by matching of QoS mechanism logically between segment A and segment B, and to provide unified QoS interface to terminal devices by hiding different QoS mechanisms applied to segment A.

10.3.2 Functional requirements for QoS bridge

- *Place of implementation*

  QoS bridge function SHOULD be implemented in HA device specified in ITU-T Rec. J.190 or at an interface point of different QoS mechanisms defined in other QoS architecture.

- *Direction of QoS signalling*

  1) At least one directional QoS bridge function MUST exchange QoS signalling from segment A to segment B. Two directional QoS bridge is also required when the control of QoS is required from end terminal device to application server. Figure 16 shows an aspect of QoS bridge.

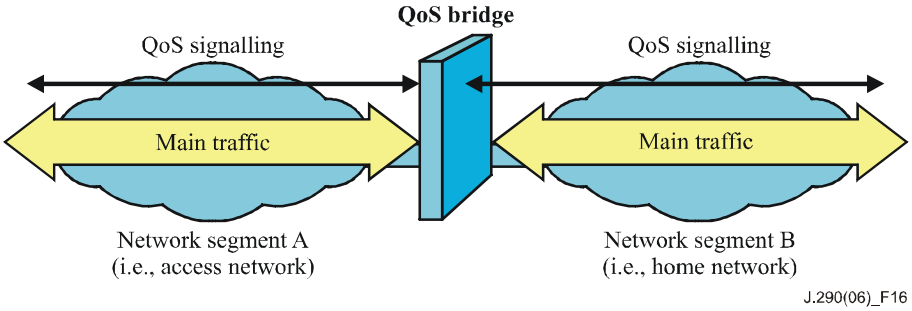


Figure 16 – Aspect of QoS bridge

QoS bridge, not like an L2-bridge, SHOULD be located in the area (Segment A/B in Figure 16) where different networks are interfaced, and SHOULD provide the following sub-functions:

a) To initiate, relay and terminate QoS signalling of each segment;

b) To mark, re-mark main signal traffic;

c) To shape main signal traffic.

2) QoS bridge SHOULD notify to terminal devices of its unavailability of QoS bridging, if segment A (access network) does not have QoS functions in upstream direction.

- *Management*

1) QoS bridge SHOULD ensure that QoS policy by the operator work with the QoS policy of segment B (home network) possibly provided by the end user. An end user MAY provide a policy management function for segment B.

2) QoS bridge SHOULD notify both parties of the mis-alignment of QoS policy between segment A and B, if it occurs.

- *Bridging function*

1) QoS bridge SHOULD maintain the priority of QoS class both in segment A and B, and provide the mapping tables to map their QoS classes. Figure 17 shows an aspect of QoS class mapping.

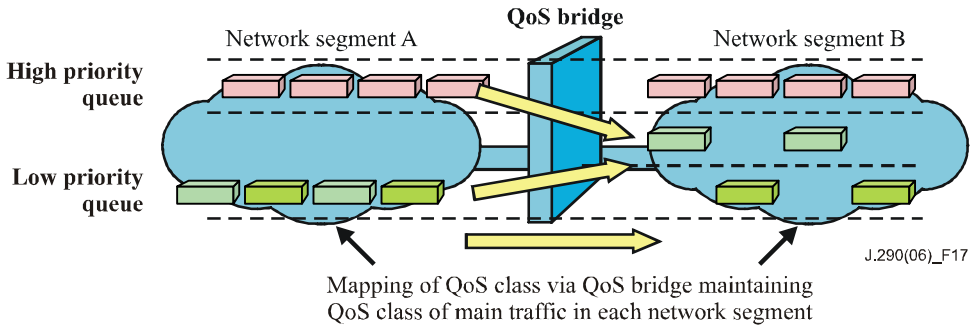


Figure 17 – Aspect of QoS class mapping

2) QoS bridge SHOULD have functions for initiation, relaying and termination of QoS signalling both in segment A and B. Figure 18 shows a treatment of QoS signalling.

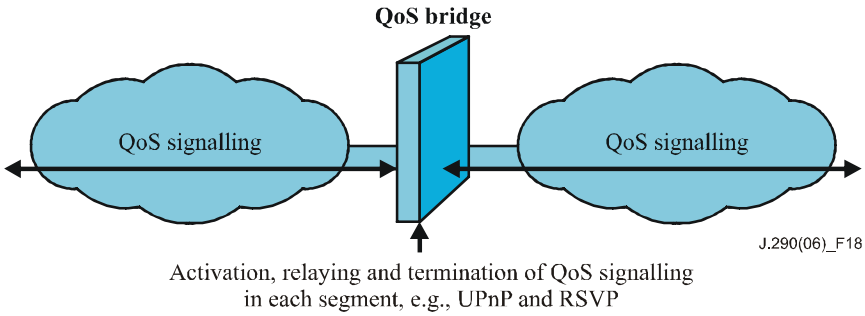


Figure 18 – A treatment of QoS signalling

- *Policing*

Provisioning of end-to-end QoS and requirements for QoS bridge are described in previous clauses; however, the mechanism of packet prioritization is required for actual QoS control. Figure 19 shows an example of QoS process flow.

1) Classification:

   To classify QoS label based on packet checking and set-up. Set-up here means ToS label, UDP port number, Protocol and IP address, etc.

2) Policing:

   To discriminate packet matching comparing received traffic rate and provisioned policer. Policer here is a policing entity, more specifically means policing tables provided by operator or customer.

3) Marking:

   To judge whether the packet is matched, to be forwarded based on set parameters, to be marked down (next priority), or to be discarded.

4) Queuing and scheduling:

   To make a queue with packets having the same QoS label (i.e., priority queuing), then to send packets in accordance with weighting discipline.

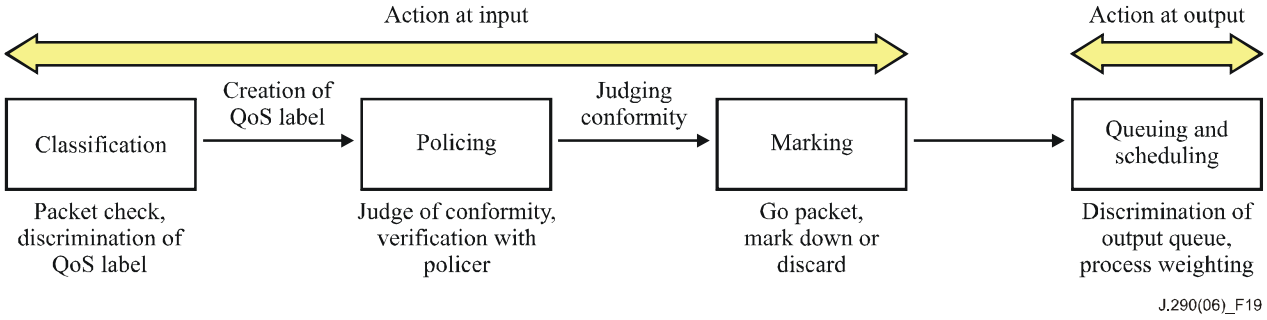


Figure 19 – An Example of QoS process flow

Packet prioritization SHOULD support IP precedence, DSCP (differentiated services code point) in DiffServ QoS mechanism and/or CoS (class of service) defined in IEEE 802.1Q. Figure 20 shows an aspect of queuing priority between core network and access network. Queuing policy MUST be provided with ToS (type of service) priority as a pre-process of bandwidth assignment. As for further details of QoS priorities, see clause 9/J.292.

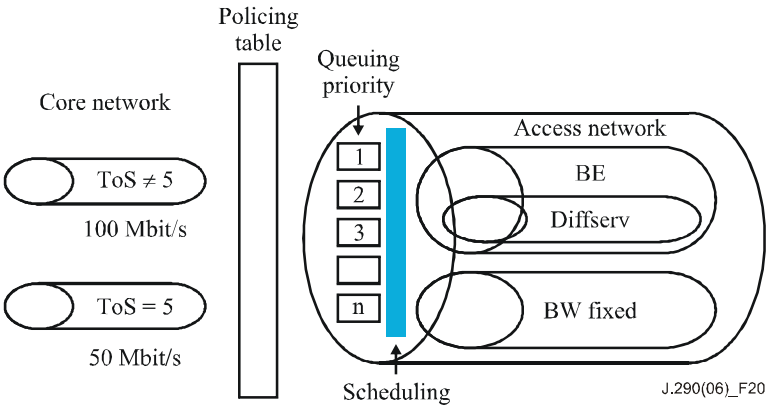


Figure 20 – An aspect of queuing priority between core network and access network

Appendix I

Relationship between MI and cable type services and QoS type

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

This appendix complements information of Table 4 in clause 10. Table I.1 shows the relationship between MI type service and QoS type for quality assured services. This table shows a desirable combination between service and QoS type and does not exclude other possible combinations.

Table I.1 – Relationship between MI type service and QoS type

	Pre-provisioned BW	**Session-based**	**DiffServ**	**Best effort**
Broadcasting TV	✓			
VoD	✓	✓		
VoIP	✓	✓		
Video phone	✓	✓	✓	✓
PC phone				✓

Table I.2 shows the relationship between Cable type service and QoS type for quality assured services. This table shows a desirable combination between service and QoS type and does not exclude other possible combinations.

Table I.2 – Relationship between cable type service and QoS type

	Pre-provisioned BW	**Session-based**	**DiffServ**	**Best effort**
Broadcasting TV	✓			
VoD		✓		
VoIP		✓		
Video phone		✓	✓	✓
PC phone				✓

Bibliography

[b-ITU-T J.112] ITU-T Recommendation J.112 (1998), *Transmission systems for interactive cable television services*.

[b-ITU-T J.122] ITU-T Recommendation J.122 (2002), *Second-generation transmission systems for interactive cable television services – IP cable modems*.

[b-ITU-T J.125] ITU-T Recommendation J.125 (2004), *Link privacy for cable modem implementations*.

[b-ITU-T J.126] ITU-T Recommendation J.126 (2004), *Embedded Cable Modem device specification*.

[b-ITU-T J.192] ITU-T Recommendation J.192 (2005), *A residential gateway to support the delivery of cable data services*.

[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 television applications*.

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

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