International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.190

(07/2007)

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

Cable modems

Architecture of MediaHomeNet

ITU-T Recommendation J.190

ITU-T Recommendation J.190

Architecture of MediaHomeNet

Summary

ITU-T Recommendation J.190 establishes a flexible and forward-looking home-networking framework that provides a unifying theme for developing a coherent set of home-network interface specifications. The MediaHomeNet infrastructure, initially created for cable access networks, is now designed to be complementary to all IP-based access networks in order to support applications such as video distribution to STB defined in ITU-T Recommendation J.290 (next generation set-top box) and voice over IP defined in ITU-T Recommendation J.160 (IPCablecom) or ITU-T Recommendation J.360 (IPCablecom2), and RF-based broadcast services. MediaHomeNet identifies a set of fundamental architectural elements that can be flexibly combined in a set of configurations, allowing for the consideration of a wide variety of home-networking solutions.

Source

ITU-T Recommendation J.190 was approved on 29 July 2007 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, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

CONTENTS

ITU-T Recommendation J.190

Architecture of MediaHomeNet

1 Scope

This Recommendation establishes a flexible and forward-looking home-networking framework that provides a unifying theme for developing a coherent set of home-network interface specifications, while at the same time lending itself to future enhancement. The MediaHomeNet infrastructure, initially created for cable access networks, is now designed to be complementary to those of all IP-based access network applications such as video distribution to STB defined in [b-ITU-T J.290] (next generation set-top box) and voice over IP defined in [b-ITU-T J.160] (IPCablecom) or [b-ITU-T J.360] (IPCablecom2), and RF-based broadcast networks, but distinct and operational in the absence of deployment of these applications. This Recommendation identifies a set of fundamental architectural elements that can be flexibly combined in a set of configurations, allowing for the consideration of a wide variety of home-networking solutions.

2 References

None.

3 Terms and definitions

This Recommendation defines the following terms:

3.1 access node: As used in this Recommendation, an access node is a termination device that terminates the network end of an access network connection. The access node is technology specific; for example, in Annex A of [J.112] it is called the INA while in Annexes B and C it is the CMTS.

3.2 domains: The extent of home-network-compliant direct influence.

3.3 home access (HA): A device class that connects access network with home bridge.

3.4 home bridge (HB): A device class that connects home access with home client.

3.5 home client (HC): A device class that connects home bridge with home decoder.

3.6 home decoder (HD): A device class that terminates home network.

3.7 home network planes: User interfaces sharing the same Layer 1/Layer 2 or internal link.

3.8 IPNet2Home: The domain in MediaHomeNet that is well bounded and specified based on Internet protocol layer 3 interoperability, as opposed to other domains that can be independently, arbitrarily, or privately designed to an individual manufacturer's specification.

3.9 function: Capabilities that compromise logical elements.

3.10 LAN IP device: A component using the Internet protocols on a local area network.

3.11 logical element: A collection of one or more functions.

3.12 MediaHomeNet: An ITU-T project that includes an architecture and a series of Recommendations that support the delivery of services over home networks. A network that connects multiple elements in a home environment to allow delivery of multi-purpose, multimedia services.

3.13 multimedia terminal adapter (MTA): Defined by IPCablecom as an element that provides IP packetized multimedia services.

3.14 residential gateway: A logical element that provides in-premise and aggregated security, management, provisioning, and addressing services for logical elements within a compliant IPNet2Home network. In this Recommendation, it is also referred to as portal services (PS).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AN	Access Node
AV	Audio-Visual
BP	Boundary Point
BWMF	Bandwidth Management Function
CAP	IPNet2Home Address Portal
CAT	IPNet2Home Address Translation
CDP	IPNet2Home DHCP Portal
CMP	IPNet2Home Management Portal
CMTS	Cable Modem Termination System
CNP	IPNet2Home Naming Portal
CPT	IPNet2Home Address Passthrough
CQoS	IPNet2Home Quality of Service
CQP	IPNet2Home QoS Portal
CSP	IPNet2Home Security Portal
CTP	IPNet2Home Testing Portal
DHCP	Dynamic Host Configuration Protocol [b-IETF RFC 2131]
DNS	Domain Name System [b-IETF RFC 1034]
DQoS	Dynamic Quality of Service
DRM	Digital Rights Management
DVD	Digital Versatile Disk
EP	Endpoint
FAX	Facsimile (ITU-T Rec. T.30)
FW	Firewall
HA	Home Access
HB	Home Bridge
HC	Home Client
HD	Home Decoder
HE	Headend
HFC	Hybrid Fibre/Coax
HTTP	HyperText Transport Protocol
ICMP	Internet Control Message Protocol [b-IETF RFC 792]
IP	Internet Protocol

KDC	Key Distribution Centre (see Table 5-4)
LAN	Local Area Network
LAN-Pass	LAN Passthrough Address Realm
LAN-Trans	LAN Translated Address Realm
LC	Layer-1/2 Converter
MCF	Management Client Function
MPAC	Media Access Control layer
MPEG	Moving Picture Experts Group
MPF	Management Portal Function
MSF	Management Server Function
MTA	Multimedia Terminal Adapter
NAT	Network Address Translation [b-IETF RFC 1631], [b-IETF RFC 2663] and [b-IETF RFC 3022]
NMS	Network Management System
ONT	Optical Network Termination
PC	Personal Computer
PHY	Physical layer
Prop Trans	Proprietary Translated Address Realm
PS	Portal Services
QCF	QoS Client Function
QoS	Quality of Service
QPF	QoS Portal Function
QSF	QoS Server Function
RSVP	Resource ReSerVation Protocol [b-IETF RFC 2210]
SBM	Subnet Bandwidth Manager
SCF	Security Client Function
SNMP	Simple Network Management Protocol [b-IETF RFC 1157]
SPF	Security Portal Function
SSF	Security Server Function
STB	Set-Top Box
SYSLOG	System Logging
TCP	Transmission Control Protocol
TEL	Telephone
TFTP	Trivial File Transfer Protocol [b-IETF RFC 1350]
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USB	Universal Serial Bus

USFS	Upstream Selective Forwarding Switch
VPN	Virtual Private Network
WAN	Wide Area Network
WAN-Data	WAN Data Address Realm
WAN-Man	WAN Management Address Realm

5 Reference architecture

5.1 Introduction and motivation

In order to extend the advantages of multimedia services to all devices connected to a home network, the MediaHomeNet architecture provides a framework for home networking. The goal of MediaHomeNet, initially created for cable access networks and now designed to be complimentary to all IP-based access technologies, is to provide new IP-based services as well as RF-based ones to devices within the home, complementing access network, applications, such as video distribution services using next generation video set-top box (e.g., [b-ITU-T J.290]) and IPCablecom (e.g., [b-ITU-T J.160]), and broadcast network infrastructures. Specifically, MediaHomeNet provides an infrastructure, by specifying a home networking environment, over which IPCablecom and other related application services can be delivered, managed and supported. Wherever possible, the architecture framework incorporates ITU-T Recommendations and other existing standards.

The MediaHomeNet architecture is composed of two sub-architectures: IPNet2Home architecture and Proprietary architecture. The IPNet2Home architecture uses an IP-based access network for providing network capabilities. The Proprietary architecture uses the broadcast services on the RF-based network such as HFC or Radio on Fibre (e.g., ITU-T Recs J.185 and J.186).

The MediaHomeNet architecture supports a myriad of operator and service provider business models, and introduces additional features above and beyond existing home networking solutions. One of the goals of the MediaHomeNet architecture is the creation of an operator and service provider configurable gateway centric environment for residential use that will interoperate with existing IP-based home devices (LAN IP devices) and new IPNet2Home devices. The MediaHomeNet architecture must allow for remote detection, access or control of services and applications on the home network from either in-home or out-of-home.

It is a goal of IPNet2Home to remain independent of physical and data link protocols. Home networking technologies such as [b-ITU-T G.9951] are given as examples. IPNet2Home is focused on Layer 3 IP traffic in the home. Similarly, IPNet2Home does not place requirements on higher layers for specific application or codecs. The architecture targets supporting resource intensive services such as MPEG video streaming, toll quality IP telephony and gaming.

5.2 Requirements and terms of reference

MediaHomeNet brings operator driven management, provisioning, QoS, and security to the home. IPNet2Home brings operator driven management, provisioning, QoS, and security to the residential gateway and IP devices. In addition, visibility and remote diagnostics for home IP devices is enabled. A summary of the capabilities provided by the MediaHomeNet follows:

Management and provisioning

- Remote management and configuration of the residential gateway device;
- Simple residential gateway management proxy for IP-based home devices;
- Hands-off provisioning for residential gateway devices;
- Allow for conversions between IP protocol and proprietary protocol;

- Allow for retrieval of services provided by home devices;
- Detection of connection and disconnection to home devices.

Addressing and packet handling

- One-to-many address translation for home devices;
- One-to-one address translation for home devices;
- Non-translated addressing for home devices (for NAT phobic applications);
- Access network traffic protection from in-home device intra-communications;
- Home-addressing support during access network outage;
- Simple DNS server in the residential gateway;
- Allow for the management of addressing and packet handling of the proprietary home devices (address conversion, address assignment, address notification and address retrieval).

Quality of Service (QoS)

- Residential gateway device bridging functionality for network side QoS messaging from/to application side.

Security

- Residential gateway device authentication;
- Secure residential gateway management messages;
- Secure download of configuration and software files;
- Secure QoS on the access network;
- Remote residential gateway firewall management.

Video services

Video services are a core business for some operators and thus the distribution of video content over MediaHomeNet networks merits special consideration. The distribution of quality entertainment video entails the same categories of features as those for general IP networking, but in the case of video, these features often must meet more stringent additional requirements. For example, specific QoS and content protection requirements must be satisfied for the distribution of premium entertainment content. Video distribution requirements are detailed in this clause, and these requirements may be satisfied by a network that is physically separate from the IPNet2Home data network, or by a network that is physically converged with the IPNet2Home data network.

The key features of the MediaHomeNet architecture specific to video distribution include:

Quality of service

- Provide for the establishment of quality of service paths on home networks for video delivery, providing guarantees for parameters such as bandwidth, jitter and delay;
- Provide for the establishment of service priorities on home networks, enabling specific video streams to take precedence over others.

Content protection

- Authentication of all devices participating in the transmission and/or consumption of video content;
- Definition of a rich set of digital rights management content protection business rules (copy restrictions, number of plays, time-limits, etc.);
- Encryption/decryption of video content for transmission and consumption.

Video device provisioning

- Provide configuration of functional parameters which are specific to the task of delivering video over home networks.

Video device management

- Provide management of functional parameters that are specific to the task of delivering video over home networks;
- Provide event reporting for functions that are specific to the task of delivering video over home networks.

The remainder of this clause examines the MediaHomeNet Reference Architecture from five perspectives:

- MediaHomeNet architecture context (see clause 5.3);
- MediaHomeNet logical reference architecture (see clause 5.4);
- IPNet2Home functional reference model (see clause 5.5);
- MediaHomeNet messaging interface model (see clause 5.6);
- IPNet2Home information reference model (see clause 5.7).

5.3 MediaHomeNet architecture context

The scope of "home networking" spans a myriad of networking technologies (Layer-1/2 – PHY/MAC), delivery protocols, application devices, and services from the access and broadcast networks. MediaHomeNet addresses the bridging and controlling of the home network environment by focusing on IP elements with defined interfaces and proprietary elements that can communicate using proprietary protocols. In particular, IPNet2Home focuses on the residential gateway (PS) portion, layer-1/2 converters (LC) and boundary point (BP) as shown in Figure 5-1. The logical elements PS, LC, BP and EP will be introduced in clause 5.4.

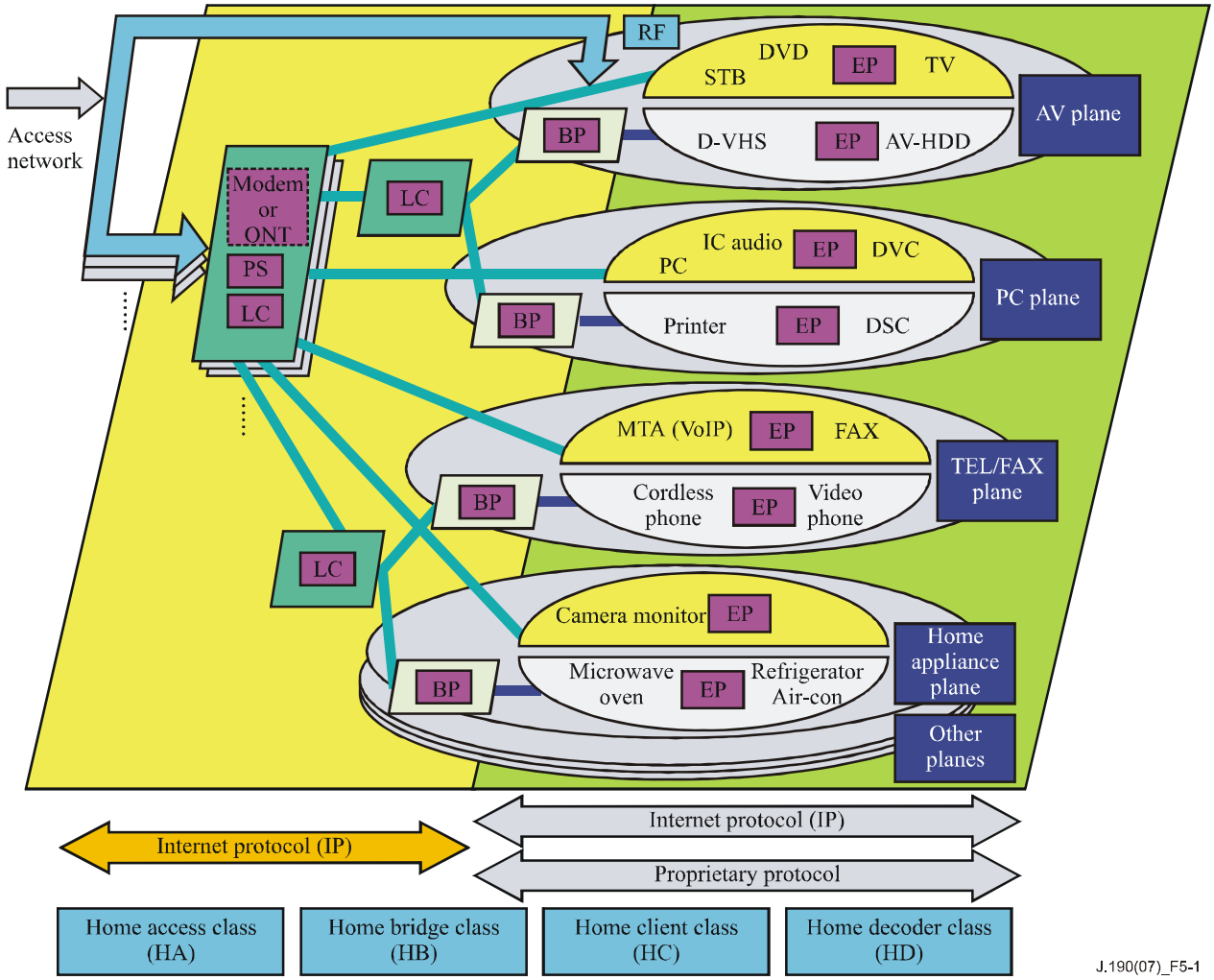

Figure 5-1 – MediaHomeNet context with home networking and access network

From the device point of view, all devices are categorized into four classes as shown in Figure 5-1:

- HA – Interface devices with access network;
- HB – Bridging devices between IPNet2Home domain networks;
- HC – Interface devices between IPNet2Home and proprietary domain devices;
- HD – Devices that can communicate by IP or proprietary protocols. (e.g., DVD, D-VHS, IC-Audio, Printer, etc.).

NOTE – Device classes other than HA can also incorporate PS functionality.

Each device of HC and HD classes belongs to one of the service planes, for example, AV plane, PC plane, TEL/FAX plane, and home appliance plane. Further details concerning device classes and planes are contained in clause 5.4.3.

5.4 MediaHomeNet logical reference architecture

The MediaHomeNet logical reference architecture introduces several concepts that form the foundation for the extension of services to devices connected to the home network. These concepts will help in understanding the MediaHomeNet architectural framework. As shown in Figure 5-2, this clause introduces the concepts of domains, logical elements and device classes.

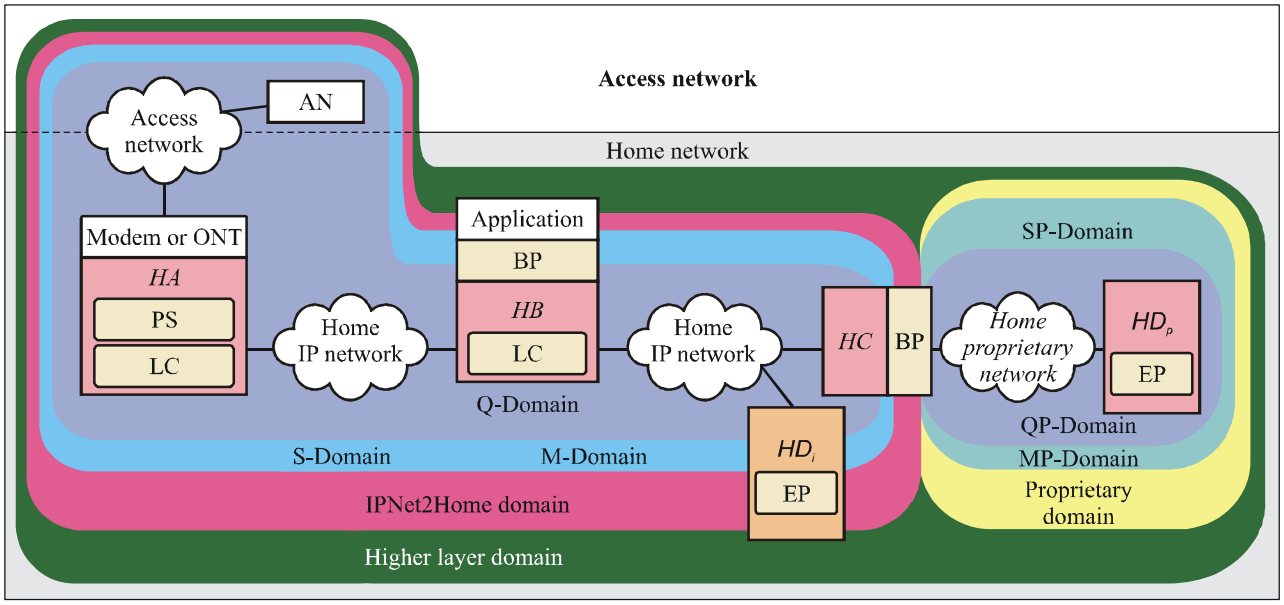

Figure 5-2 – MediaHomeNet key concepts

5.4.1 Domains

The MediaHomeNet architectural framework makes use of Domains. Domain represents a concept of functional control area. In the MediaHomeNet architecture, there are three Domains: IPNet2Home domain, proprietary domain, and higher layer domain. These domains represent the effective area of control and management. The IPNet2Home Domain contains the layer 3 messaging while the higher layer domain contains the end-to-end messaging to the EPs. The IPNet2Home domain has three sub-domains: Q, S and M domains. The proprietary domain has three sub-domains: QP, SP and MP domains.

A Domain represents a set of home network elements that are compliant with a set of requirements. Within the IPNet2Home architecture, the IPNet2Home Domain consists of a set of IPNet2Home architectural elements that are compliant with the IPNet2Home Recommendations. Elements that reside within the IPNet2Home Domain (i.e., compliant elements) are directly manageable by operators and can take advantage of their service offerings.

5.4.1.1 IPNet2Home domain

The IPNet2Home Domain is composed of three sub-domains referred to as the Q-Domain (QoS domain), the S-Domain (security domain), and the M-Domain (management domain), as mentioned before.

The Q-Domain consists of the set of elements that are compliant with the IPNet2Home QoS (CQoS) specifications, and can therefore deliver quality guaranteed services. Similarly, the M-Domain consists of the set of elements that are compliant with the IPNet2Home provisioning and management specifications, and can therefore be provisioned and managed by the operator or User. Finally, the S-Domain consists of the set of elements that are compliant with the IPNet2Home security specifications, and can therefore deliver security material managed by the operator and User.

As shown in Figure 5-2, the Q-Domain may be a subset of the M-Domain; all network elements providing CQoS are fully IPNet2Home manageable. This ensures that operators can manage products delivering CQoS-based services to the degree needed to fulfil service quality guarantees. In addition, the M-Domain extends beyond the Q-Domain, allowing IPNet2Home management of products that are not CQoS compliant. This enables IPNet2Home management for legacy products

that are not QoS capable, as well as for products delivering low-bandwidth applications for which QoS may not be appropriate.

5.4.1.2 Proprietary domain

The proprietary domain is composed of three sub-domains referred to as the QP-domain (QoS proprietary domain), the SP-domain (security proprietary domain), and the MP-Domain (management proprietary domain). These three sub-domains are for reference and for further study.

5.4.1.3 Service domain

In addition to Q-domain described in clause 5.4.1 and QP-domain in clause 5.4.1.2, the following service domains SHOULD be added to Q- and QP-domains as its sub-layer domains in order to assure the service quality in end-to-end basis.

Guaranteed service domain (GSD)

GSD is the domain for streaming contents such as voice, video-on-demand or game for which customer requires highest service quality. The network operator cannot control the rights of contents itself. The devices within GSD MUST be able to receive the fully-guaranteed QoS contents such as packets of VoIP, TV conference, VoD stream and Game, etc. in accordance with QoS grade. Some DRM information outside the domain MAY be contained in the contents. All the devices in the GSD MUST implement home networking technology that meets network operator requirements for the GSD. Such technology is called as GSD Technology. All the devices in the GSD MUST implement UPnP QoS specifications. The GSD Manager logical entity is responsible for managing QoS on the GSD. The GSD Bridge functionality bridges devices with different GSD home networking technologies.

Authorized service domain (ASD)

ASD is mainly for the contents downloading with operator protection. The devices in ASD MUST have device authentication function to receive the contents that are compliant with the policy of network operator. All the devices in ASD MUST have discovery mechanism defined by UPnP/DLNA specification.

Approved output domain (AOD)

AOD is the domain for the contents on portable/mobile equipment with non-QoS sensitive environment. The devices in AOD SHOULD be connected to ASD with the interface approved by network operator. It is required to protect the contents by means of DRM mechanism when the contents are transferred from ASD to AOD. The DRM mechanism implemented by devices in the AOD SHOULD respect the requirements identified in [b-ITU-T J.197] in conjunction with capability of redistribution control assigned by content providers.

Best-effort domain (BED)

BED is the domain for non-QoS sensitive contents. The devices in BED do not satisfy the requirements of the GSD. Devices residing in the BED are connected to the devices in the GSD using the BED Bridge. The BED Bridge is responsible for protecting the integrity of the GSD by policing the traffic flowing into the GSD that is originated from devices in the BED.

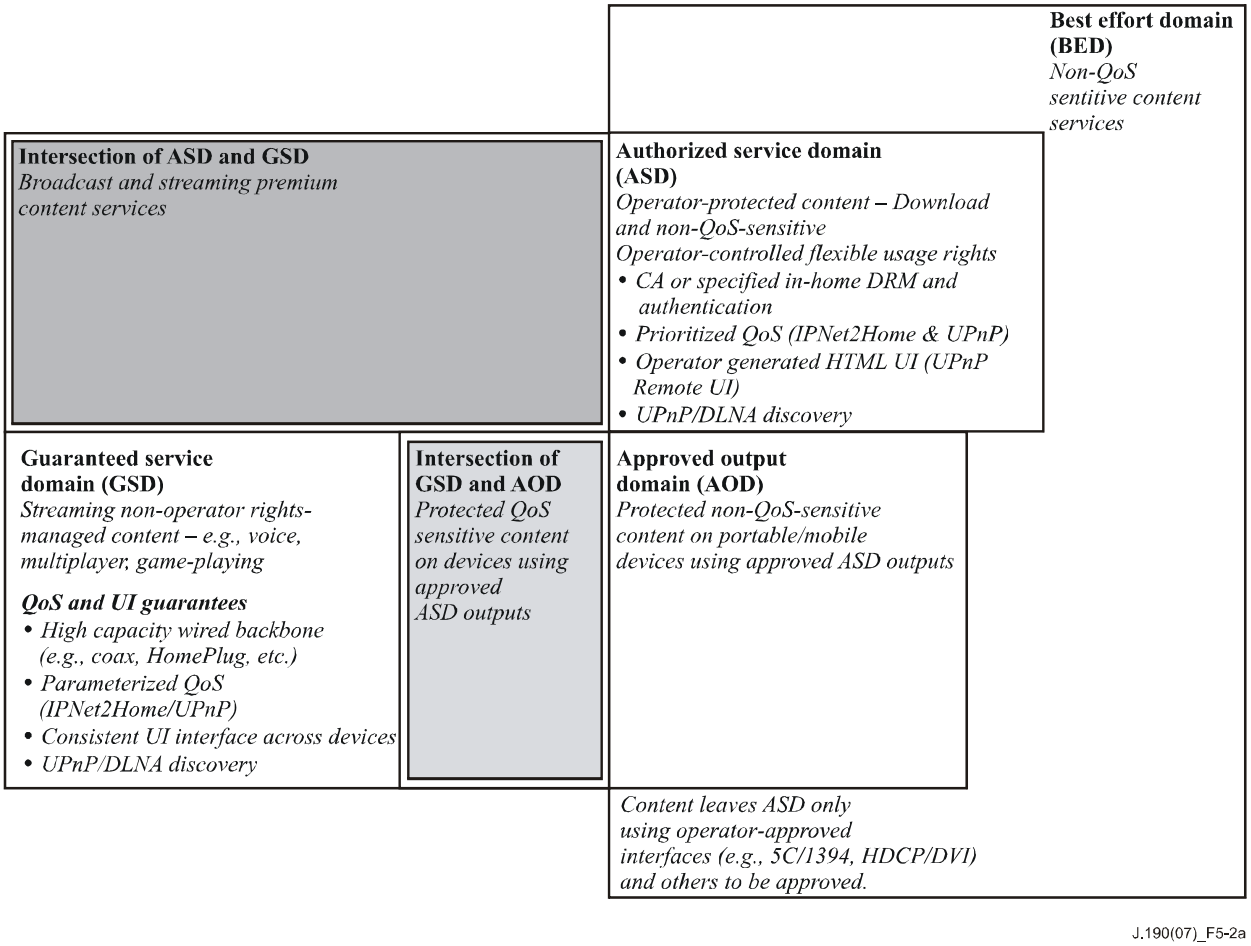

Figure 5-2a – Service domains

5.4.1.4 Higher layer domain

The higher layer domain contains the end-to-end messaging to the EPs that are above layer-3. Service providers may communicate parameters and data to the EPs. The higher layer domain is for reference and for further study.

5.4.2 Logical elements

As shown in Figures 5-1 and 5-2, the MediaHomeNet architectural framework introduces the concept of logical elements. There are four distinct classes of logical elements defined by the MediaHomeNet architecture framework; these are referred to as portal services (PS), layer-1/2 converters (LC), boundary points (BP) and endpoint (EP).

LCs, PSs, and BPs are logically bounded functional entities that can generate and respond to IPNet2Home-compliant messages. They include the ability to gather and communicate information as needed to manage and deliver services over IPNet2Home networks. They also contain the functionality necessary to carry out IPNet2Home-defined control of network traffic. IPNet2Home logical elements operate at the network protocol layer and above, thus remaining independent of any particular physical Layer-1/2 network technology.

As shown in Figure 5-3, layer-1/2 converters, portal services, boundary points and endpoints are used to extend the MediaHomeNet Domain, provide local MediaHomeNet services or terminate the IPNet2Home Domain.

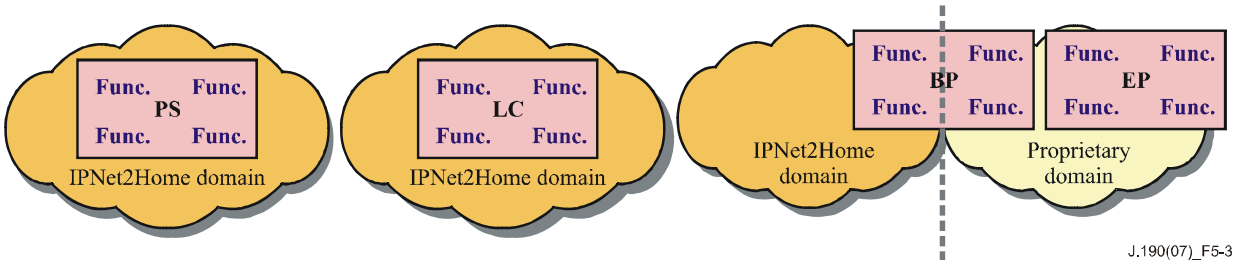

Figure 5-3 – MediaHomeNet logical elements

A **LC** is a logical element that interconnects IPNet2Home-compliant IP capable Layer-1/2 technologies. A LC also terminates and initiates management messages (such as to control interface packet forwarding rules, provisioning, gathering statistics, etc.) for itself. Packet forwarding between interfaces may occur at layer 2 (bridging), layer 2.5 (selective forwarding) or layer 3 (routing).

A **PS** is a logical element that provides in-premise and aggregated security, management, provisioning, and addressing services for logical elements within a compliant IPNet2Home network. In other Recommendations, sometimes this functionality is called "Residential Gateway".

A **BP** is a logical element that interconnects non-compliant home networks, devices and applications to a compliant IPNet2Home network.

An **EP** is a logical element that provides services to users based on IP or proprietary protocols. An EP terminates the Higher Layer control network.

LC and BP may be collectively referred to as LAN IP devices.

5.4.2.1 Logical elements are the MediaHomeNet network

The EP, BP, PS and LC logical elements form the foundation of the MediaHomeNet architecture and they fully define a MediaHomeNet network within the home. While Domains (introduced in clause 5.4.1) and device classes (introduced in clause 5.4.3) are structural aides only, IPNet2Home logical elements completely supply the in-home functionality defined by the IPNet2Home specifications. Each BP, PS and LC logical element is assigned a unique IP address that is used for provisioning and managing the element. An IPNet2Home network can be conceptualized as a set of PSs, BPs and LCs that are discovered and managed, and that interact with each other and with the IPNet2Home support infrastructure as needed to deliver services. The thrust of the IPNet2Home effort is the specification of logical element interfaces.

5.4.2.2 A closer look at boundary points and endpoints

The IPNet2Home boundary point (BP) is a key concept that warrants further discussion. As mentioned before, a BP connects an IPNet2Home network to non-compliant entities known as proprietary endpoints (EP). Proprietary endpoints may source or sink data content, but they reside outside of the IPNet2Home Domain. As such, a proprietary EP knows nothing about IPNet2Home layer-3 messaging and no IPNet2Home requirements can be placed on them. These entities may range from simple analog audio and video presentation devices to complex proprietary networked devices. Since the BP may provide a protocol conversion function, it is possible, in some instances, for the IPNet2Home layer-3 messaging to be extended to the proprietary EP. However, the conversion function is proprietary and outside the scope of IPNet2Home. Proprietary EPs can also send/receive higher layer control messages.

Boundary points may connect IPNet2Home networks to the following example types of proprietary EPs:

- embedded proprietary EP;
- external proprietary EP;
- proprietary EPs residing on non-compliant networks;
- proprietary EP-like applications;
- IPCablecom MTA.

An IPNet2Home boundary point can be thought of as an agent acting on behalf of one or more proprietary EPs, enabling them to consume services. In essence, a BP is a functional entity that indirectly enables IPNet2Home management of, and service delivery to, proprietary EPs. A BP presents a common specified interface on behalf of connected EPs independent of the actual characteristics of the EP being represented. A single BP may represent any number of EPs, and may choose to acquire a unique IP address for each EP that it exposes.

In the case of a simple embedded analog EP, a BP may do nothing more than convert IP streams to the appropriate format and pass the data on to the EP for consumer presentation. In contrast, a BP may be connected to a functionality-rich EP, in which case the BP and EP might engage heavily in bidirectional communications.

BPs may optionally act as a proxy function or as a translation function for the EPs. The proxy function allows the BP to act on behalf of one or more EPs, while the translation function translates the IPNet2Home-compliant protocols to Proprietary protocols.

5.4.2.3 Planes of EPs

As shown in Figure 5-1, the MediaHomeNet architectural context introduces the concept of user planes of EPs. There are four or more planes where several EPs are logically located for segregated services. Each EP receives services through the PS and LC(s), and BPs if EP uses proprietary protocol. In each plane, IP or appropriate protocols may be introduced. If EP uses proprietary protocol, the difference of protocols and interfaces between IPNet2Home domain and proprietary domain shall be absorbed or proxied in the Boundary Points.

The audio-visual (AV) plane is a set of EPs and one branch of proprietary home network for audio-visual services. Through the access network or IPNet2Home logical elements, the broadcast streams in MPEG format may flow to the AV plane.

The PC plane is provided for PC clients including PC peripherals. Through BP(s) of the PC plane, broadcast stream and/or webcast traffic may traverse to PC plane that provides media conversion facilities.

The TEL/FAX plane is a specified logical entity for telephone and facsimile services that require several levels of QoS grades, which may be based on IPCablecom frame structure.

The control plane is for home appliance clients that have control interfaces over IP or proprietary protocols. BP(s) for the control plane have a protocol conversion function between IP and proprietary protocols.

This Recommendation is not intended to limit the number of planes to four. Other planes can be additionally defined in accordance with the purpose of endpoints.

5.4.3 Device classes

The MediaHomeNet architectural framework introduces the concept of device classes to lend tangible context to the MediaHomeNet logical elements and combinations of these logical elements. The MediaHomeNet architectural framework concept of device classes places no restrictions on physical devices or combinations of logical elements within physical devices.

There are four classes of MediaHomeNet devices, referred to as HA (home access), HB (home bridge), HC (home client) and HD (home decoder). The HA, HB, HC and HD device classes are loosely distinguished by their placement in a MediaHomeNet network. These device classes provide an informative way of depicting collections of logical elements but are not considered definitive or restrictive. HA, HB, HC and HD are not addressable entities within the MediaHomeNet architecture.

As shown in Figure 5-1, vendors implement one or more logical elements in a device to create a product. The specific set of logical elements in a given device is left to the discretion of the vendor.

The **HA** device class represents a collection of one or more logical elements that extend the IPNet2Home Domain between the access networks including cable modem (e.g., [b-ITU-T J.112] and [b-ITU-T J.122]) and one or more IPNet2Home-compliant networks. The number of the access networks connected to a home network is not limited to one. If there are several number of access networks, the corresponding number of HA devices will be necessary for each access network. The HA device has a single interface for the access network such as cable modem RF-compliant one, a single PS logical element, and may have one or more IPNet2Home-compliant interfaces. HA encompasses a set of functions that handle IP packet routing, address conversion, security management between WAN (outside network) and LAN (inside network). Logical function elements of HA are called portal services (PS) and layer-1/2 converters (LC).

The **HB** device class represents a collection of one or more LC logical elements that extend the IPNet2Home domain to additional IPNet2Home-compliant networks and has at least two IPNet2Home-compliant interfaces. The LC logical elements can be implemented in the HA or HC device. HB may be used for interconnection between HDs within the same IP-based plane. All HBs are placed in the IPNet2Home domain.

The **HC** device class represents a collection of one or more BP logical elements that interconnects the in-home IPNet2Home domain and a proprietary network. HC devices connected with HA, possibly via HB, provide a function of commands and/or contents data control between home network devices (HD) and HA. Some consumer electronic devices such as STB, PC, TEL/FAX and control device, which typically provide services to users, may act as HC, if BP is implemented in those devices. HC also may provide a proxy function for protocol conversions between IP and Proprietary protocols. The proxy function enables transmission of commands and/or contents data to devices that work by proprietary protocols only. The logical function element of an HC is called boundary point (BP) and separates IPNet2Home and proprietary domains.

The **HD** device class represents a collection of one or more EP logical elements that provide services to users. The HD device class is categorized into two types, one is a type which supports proprietary protocols and the other one is a type which has an IP interface. HD devices provide services to users after exchange of commands and/or contents data through the IP transport or the proprietary protocols. The logical function element of an HD is called endpoint (EP). The interface between HC and HD supports proprietary protocols (such as IEEE 1394, USB, DECT, X.10, etc.) required by each plane.

As previously mentioned, MediaHomeNet device classes are loosely defined and non-restrictive. A MediaHomeNet device of a particular type may contain functionality typically associated with other device classes. To clarify the role and the functionality of each device class, Figure 5-3a illustrates the relationship between each device class of HA, HB, HC and HD, and it defines the interfaces between them.

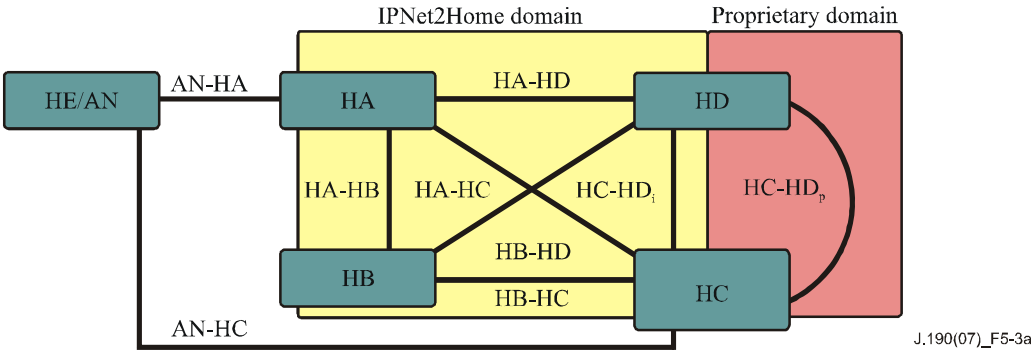

Figure 5-3a – Relationship between each device class

In this figure, XX–YY denotes an interface between device class XX and YY. Table 5-1a describes the interfaces defined in Figure 5-3a.

Table 5-1a – Descriptive texts of the interfaces defined in Figure 5-3a

Interface	Description
HA-HB	An interface for data transmission and controls between HA and HB. Since HB is basically assumed as bridge-like equipment, it will work independently from IP and higher layers.
HA-HC	An interface for data transmission and controls between HA and HC. In addition to the functionality of the interface HA-HB, this may include an IP layer control such as address configuration of HC.
HA-HD	An interface for data transmission and controls between HA and HD. If HD is HD_p that uses non-IP based proprietary protocol, data transmission is not included in the functionality of this interface.
HB-HC	An interface for data transmission and controls between HB and HC.
HB-HD	An interface for data transmission and controls between HB and HD, which is equivalent to the interface HB-HC. This interface is applicable only to the HD device that uses IP protocol (HD_i).
$HC\text{-}HD_p$	An interface for data transmission and controls between HC and HD with non-IP interface (HD_p). This interface includes all layers from the physical layer to the application layer.

5.4.4 Address realms

An address realm is defined as "a network domain in which the network addresses are uniquely assigned to entities such that datagrams can be routed to them" [b-IETF RFC 2663]. Within the MediaHomeNet architecture, address realms are categorized as WAN address realms, LAN address realms and the proprietary address realm. (See Figure 5-4.)

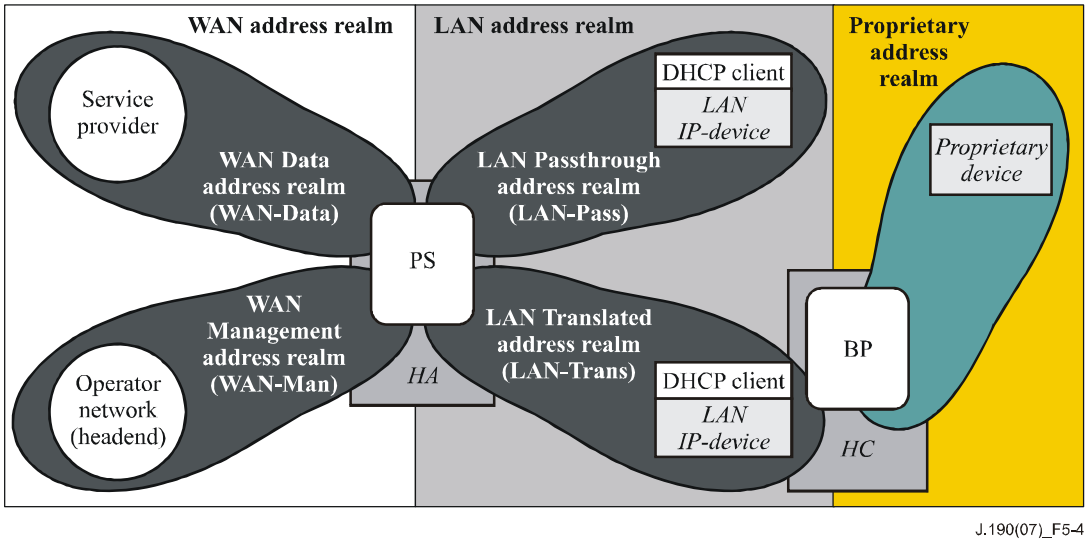

Figure 5-4 – MediaHomeNet address realms

WAN addresses reside in one of two realms: the WAN management address realm (WAN-Man) or the WAN Data address realm (WAN-Data). LAN addresses also reside in one of two realms: LAN Passthrough address realm (LAN-Pass) or LAN Translated address realm (LAN-Trans). The properties of these addressing realms are as follows:

- The WAN Management address realm (WAN-Man) is intended to carry network management traffic on the cable network between the network management system and the PS element. Typically, addresses in this realm will reside in private IP address space.
- The WAN Data address realm (WAN-Data) is intended to carry subscriber application traffic on the cable network and beyond, such as traffic between LAN IP devices and Internet hosts. Typically, addresses in this realm will reside in public IP address space.
- The LAN Translated address realm (LAN-Trans) is intended to carry subscriber application and management traffic on the home network between LAN IP devices and the PS element. Typically, addresses in this realm will reside in private IP address space, and can typically be reused across subscribers.
- The LAN Passthrough address realm (LAN-Pass) is intended to carry subscriber application traffic, such as traffic between LAN IP devices and Internet hosts, on the home network, the cable network, and beyond. Typically, addresses in this realm will reside in public IP address space.
- The proprietary translated address realm (Prop Trans) is intended to carry subscriber application traffic and convert user application and/or command using proprietary protocols. Addresses are assigned based on proprietary protocols at each plane that proprietary device belongs to. Proprietary translated address realm connects with LAN address realm via BP.

On the LAN side, the addresses in the LAN Passthrough address realm (LAN-Pass) are directly extracted from the addresses in WAN data address realm. LAN IP devices and applications such as IPCablecom services that are intolerant of address translation and require a globally routable IP address use LAN-Pass addresses. Additionally on the LAN side, LAN IP devices may use translated addresses from the LAN Translated address realm (LAN-Trans).

5.5 IPNet2Home functional reference model

IPNet2Home functions are layer-3 and above services. IPNet2Home Functions are located within the PS, LC, BP and the headend. There are IPNet2Home functions for each of the major IPNet2Home specification areas: provisioning and management, security and quality of service. The IPNet2Home functions for provisioning and management, security and QoS are briefly introduced in the following three subclauses.

5.5.1 IPNet2Home management functions

To support the IPNet2Home requirements during the provisioning and management of IP LAN-devices within the home, three management functions classes are defined within IPNet2Home:

- management server functions;
- management client functions;
- management portal functions.

Several of the management server functions reside within the operator headend (HE). Management client functions are typically found within LAN IP devices. Management portal functions are located within the PS logical element and may include server-like, client-like, and relay-like functionality to aggregate and translate messages between the operator headend and LAN IP devices. Examples of management server, client and portal functions are introduced in Tables 5-1b, 5-2 and 5-3 and are illustrated in Figure 5-5.

Table 5-1b – Management server function description

Management server functions	Description
Headend DHCP server	The IPNet2Home DHCP server is a headend component that provides address information for the WAN-Man and WAN-Data address realms to the PS protocols such as SNMP, SYSLOG and TFTP.
Headend DNS server	The IPNet2Home DNS server is a back-office component used to map between ASCII domain names and IP addresses.
Headend management messaging server	The IPNet2Home management messaging, download, event notification servers including protocols such as SNMP, SYSLOG and TFTP.

Table 5-2 – Management and provisioning portal function description

Management portal functions	Description
IPNet2Home address portal (CAP)	Within the PS, the CAP interconnects the WAN and LAN address realms for data traffic. (See CAT/Passthrough.)
IPNet2Home address translation (CAT)	A sub-function of the CAP, a CAT translates addresses on the WAN-Data side of the CAP to addresses within a single logical subnet on the LAN-Trans side.
IPNet2Home address passthrough (CPT)	A sub-function of the CAP, the CPT function bridges packets on the WAN-Data side of the CAP to the LAN-Pass side unchanged.
IPNet2Home upstream selective forwarding switch (USFS)	A sub-function of the CAP, the USFS function confines home networking traffic to the home network, even when the home networking devices generating this traffic reside on different logical IP subnets.
IPNet2Home management portal (CMP)	The function that provides an interface between the operator and the PS database.
IPNet2Home DHCP portal (CDP)	Address information functions (e.g., those transmitted via DHCP) including a server for the LAN realm and a client for the WAN realms.
IPNet2Home naming portal (CNP)	The CNP provides a simple DNS service for the LAN IP devices requiring naming services.
IPNet2Home testing portal (CTP)	The CTP provides a remote means to initiate pings and loopbacks within the LAN.

Table 5-3 – Management client function description

Management client functions	Description
LAN IP device DHCP client	The IPNet2Home DHCP client function is an in-home component used during the LAN IP device provisioning process to dynamically request IP addresses and other logical element configuration information.
LAN IP device echo (Loopback) responder	Within LAN IP device, the echo or loopback responder loops data sourced from the CTP loopback function back to the CTP loopback function.

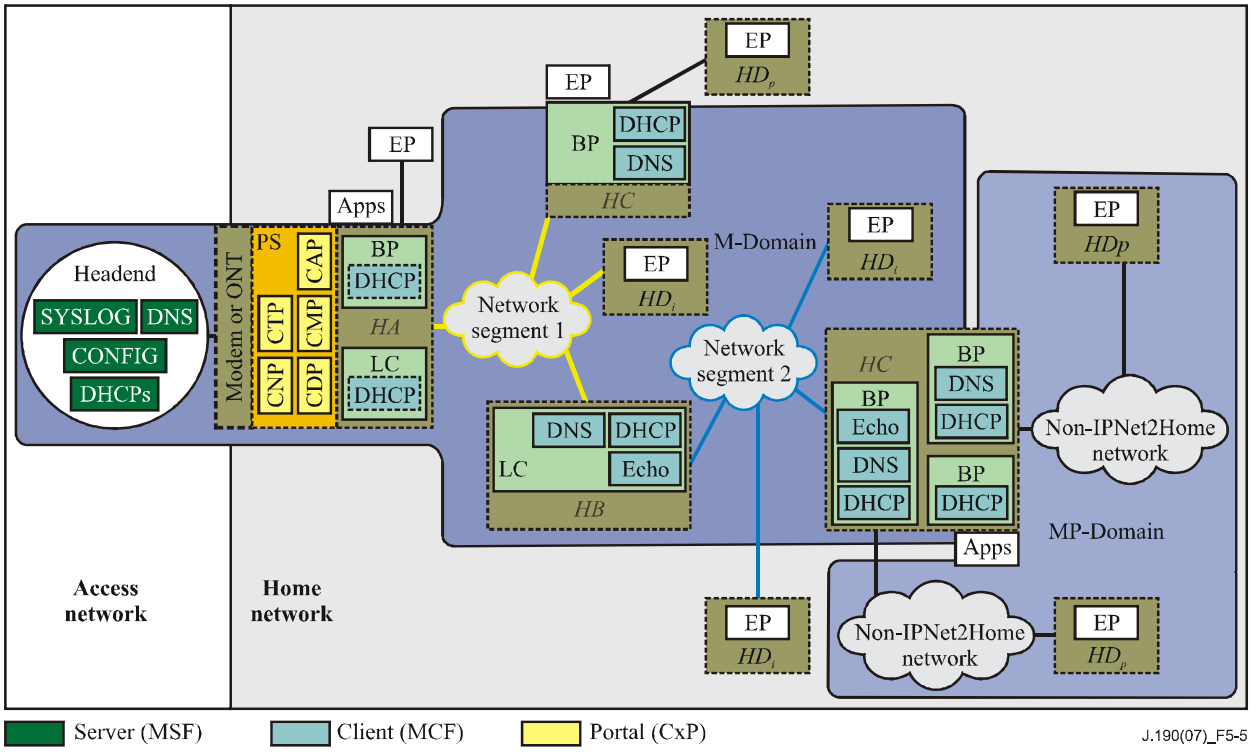

Figure 5-5 – Management client-server relationship to IPNet2Home domain

5.5.1.1 Packet handling and address translation

The key goals that drive the IPNet2Home packet handling capabilities include:

- Provide operator-friendly address translation functionality, enabling operator visibility and manageability of home devices.
- Prevent unnecessary traffic on the access and home network.
- Conservation of globally routable public IP addresses as well as private management addresses.
- Facilitate in-home IP traffic routing by assigning network addresses to LAN IP devices such that they reside on the same logical subnetwork.

IPNet2Home address translation and packet handling functionality is provided by the functional entity known as the IPNet2Home address portal (CAP). The CAP encompasses the following address translation and packet forwarding elements:

- IPNet2Home address translation (CAT) function;
- IPNet2Home address passthrough (CPT) function;
- upstream selective forwarding switch (USFS).

As shown in Figure 5-6, the CAT function provides a mechanism that interconnects the WAN-Data address realm and LAN-Trans address realm (via address translation), while CPT provides a mechanism to interconnect the WAN-Data address realm and the LAN-Pass address realms (via bridging). The CAT function is compliant with traditional network address translation (NAT) (section 2 of [b-IETF RFC 3022]). As with traditional NAT, there are two variations of CAT, referred to as IPNet2Home network address translation (C-NAT) transparent routing and IPNet2Home network address and port translation (C-NAPT) transparent routing. C-NAT transparent routing is the IPNet2Home compliant version of basic NAT (section 2.1 of [b-IETF RFC 3022]) and C-NAPT transparent routing is the IPNet2Home compliant version of NAPT (section 2.2 of [b-IETF RFC 3022]).

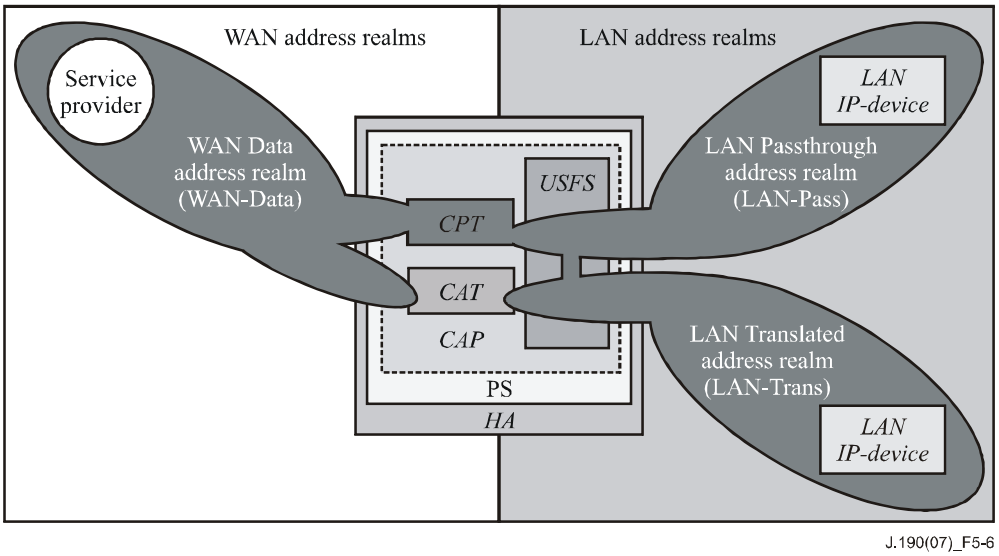

Figure 5-6 – IPNet2Home address portal (CAP) functions

Per [b-IETF RFC 3022], C-NAT transparent routing is "a method by which IP addresses are mapped from one group to another, transparent to end users", and C-NAPT transparent routing "is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports". Also, per [b-IETF RFC 3022], the purpose of C-NAT and C-NAPT functionality is to "provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses".

The IPNet2Home CPT function is an IPNet2Home specified bridging process that interconnects the WAN-Data address realm and the LAN-Pass address realm without address translation.

The IPNet2Home upstream selective forwarding switch (USFS) defines a function within the CAP with the capability of confining home-networking traffic to the home network, even when home-networking devices generating this traffic reside on different logical IP subnets. Specifically, this function forwards traffic sourced from an IP address in one of the LAN address realms, destined to IP addresses in one of the LAN address realms, directly to its destination. This direct forwarding functionality prevents the traffic from traversing the HFC network, and interconnects the LAN-Trans and LAN-Pass address realms.

5.5.2 IPNet2Home security functions

The security architecture provides security material and functionality for the other IPNet2Home functions and it also employs IPNet2Home functions to provide management of the security functions. The security capabilities are components of the following security entities:

- headend security servers;
- IPNet2Home security portal (CSP);
- firewall (FW);
- security clients (LC and BP).

The security functions within those entities are categorized as security server functions, security portal functions, and security client functions. The relationship between the different security elements and their classification as server, portal and client functions is presented in Figure 5-7 and described in Tables 5-4 and 5-5.

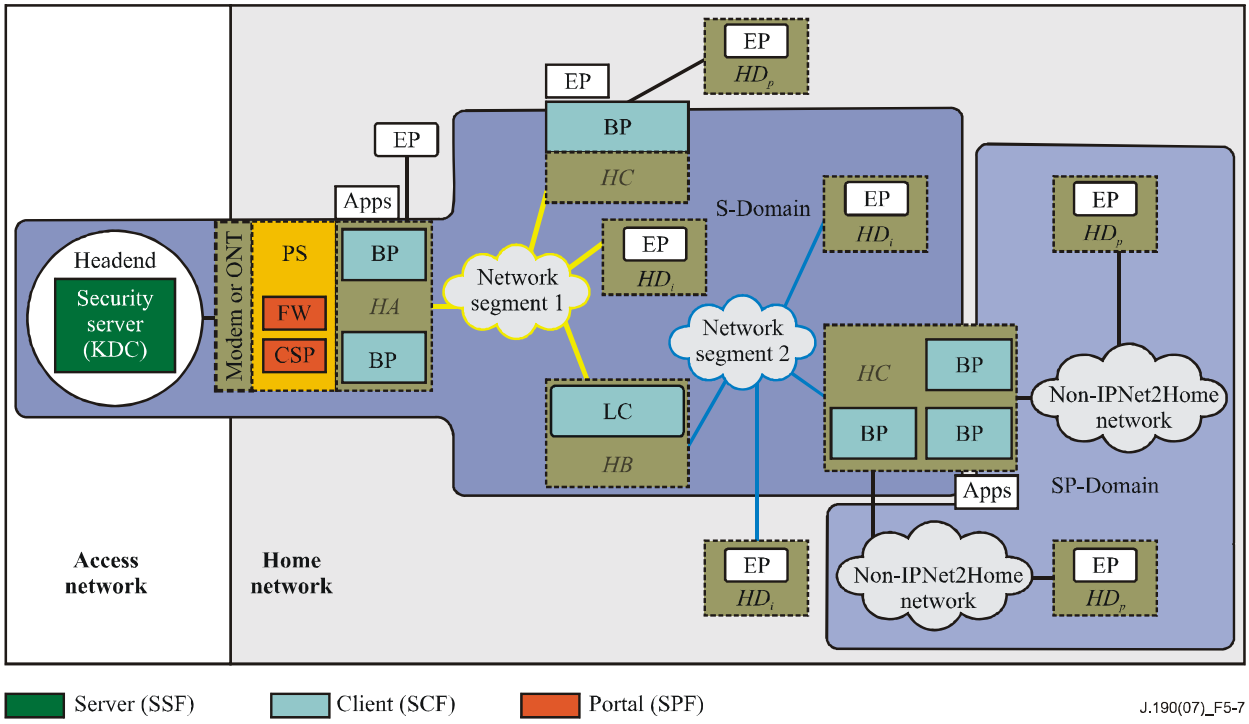

Figure 5-7 – IPNet2Home security elements

Table 5-4 – Security portal function description

Security portal functions	Description
IPNet2Home security portal (CSP)	The CSP acts as a portal for security material for all of the other IPNet2Home security functions within the PS and LAN IP devices. The CSP communicates on the WAN side with a security server (key distribution centre (KDC)).
Firewall (FW)	The firewall provides protection of the home network from malicious attack.

Table 5-5 – Security server function description

Security server functions	Description
KDC	The KDC servers in the headend provide for authentication services and key distribution for the home. They communicate with the CSP function to establish these services.

5.5.3 IPNet2Home QoS functions

The IPNet2Home QoS (CQoS) architecture provides quality of service using IPNet2Home defined bandwidth management and bandwidth reservation functions. The IPNet2Home QoS functions are components of the following QoS entities:

- IPNet2Home quality of service-domain (Q-Domain);
- CQoS set of functions within the layer-1/2 converter logical element (LC);
- CQoS set of functions within the boundary point logical element (BP);
- headend reservation server.

The CQoS functions within those entities are shown in Figure 5-8 and briefly described in Table 5-6.

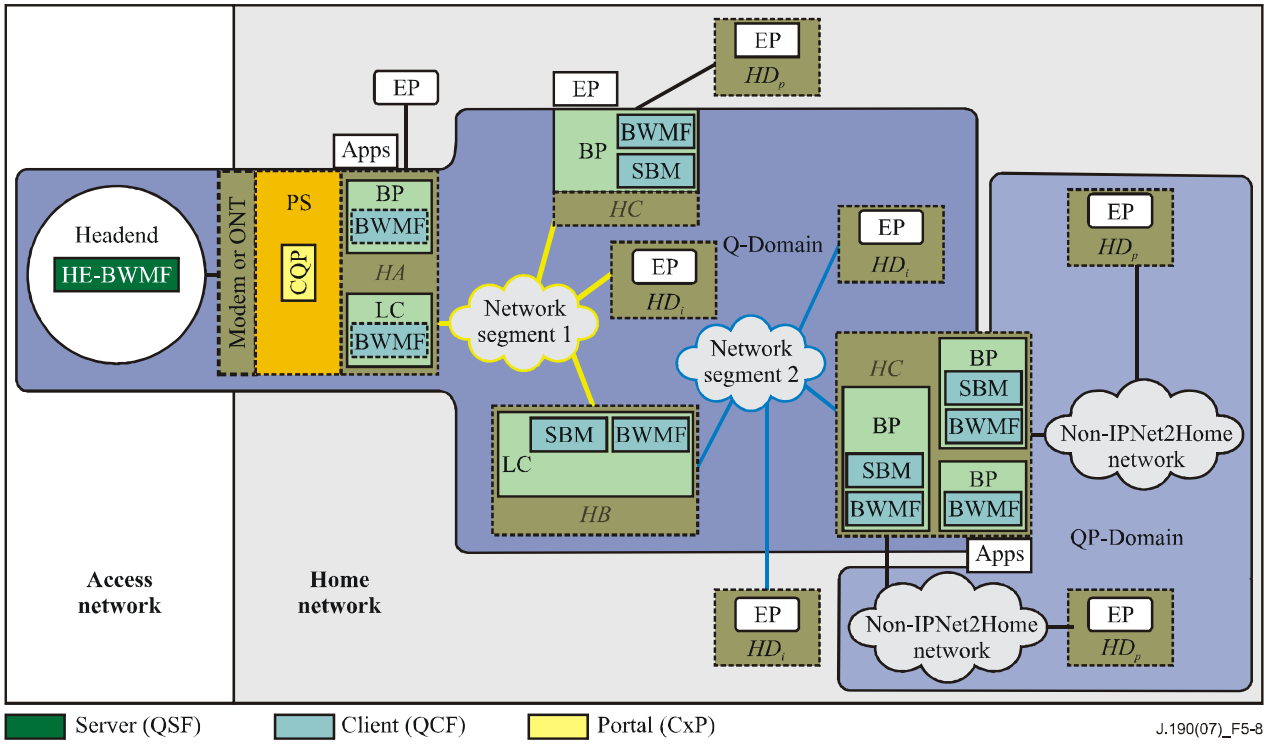

Figure 5-8 – IPNet2Home QoS elements

Table 5-6 – QoS function description

QoS function	Description
CQP	The CQP acts as a portal for QoS protocols for the IPNet2Home QoS functions within the PS and LAN IP devices. The CSP communicates on the WAN side with a HE-BWMF and BWMF clients in LAN IP devices. For example, CQP implements UPnP QoS policy holder service (UQPH) and UPnP QoS manager service (UQM) for communication with LAN IP devices.
BWMF	Provides bandwidth management functionality within a LC or BP, for example, using UPnP QoS manager [b-UQM], prioritized control, etc.
HE-BWMF	Provides bandwidth management functionality within the headend.
QCD	Provides QoS device service functionality within an LC and BP. This functionality facilitates QoS reservation establishment and bridging between different home networking technologies in the home, for example, using UPnP QoS device (UQD).

5.5.4 Exchange of QoS information

HA device SHOULD have the functions of exchange or translation of QoS information between the access network and HD devices in the home network to assure the quality of end-to-end services. Access network generally controls the QoS of the traffic in accordance with network operator's policy between edge nodes, while the QoS request from each HD device is normally specified with in-home QoS mechanisms such as UPnP QoS. HA device, an entity of home gateway, SHOULD have the mapping facility of these different QoS mechanisms according to the policy of service operator.

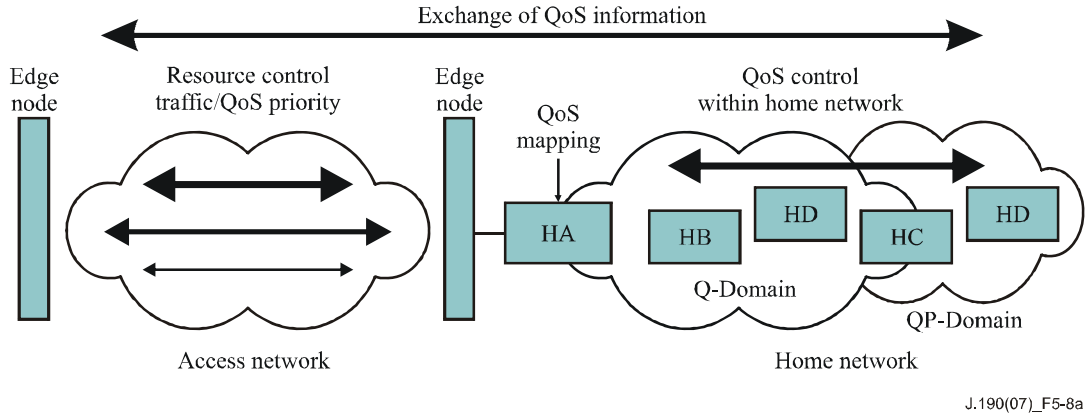

Figure 5-8a – Exchange of QoS information

At the border of IP and non-IP domain, BP SHOULD have a translation function between QoS requests from EP devices and QoS information required in the IP domain. In the non-IP domains, the QoS mechanism SHOULD be implemented in accordance with its proprietary protocols.

5.6 MediaHomeNet messaging interface model

The communication between the functions in logical elements occurs on MediaHomeNet-defined messaging interfaces. The types of messaging interfaces are differentiated by the elements that are involved in the communication. The MediaHomeNet messaging interfaces are illustrated in Figure 5-9 and summarized in Table 5-7.

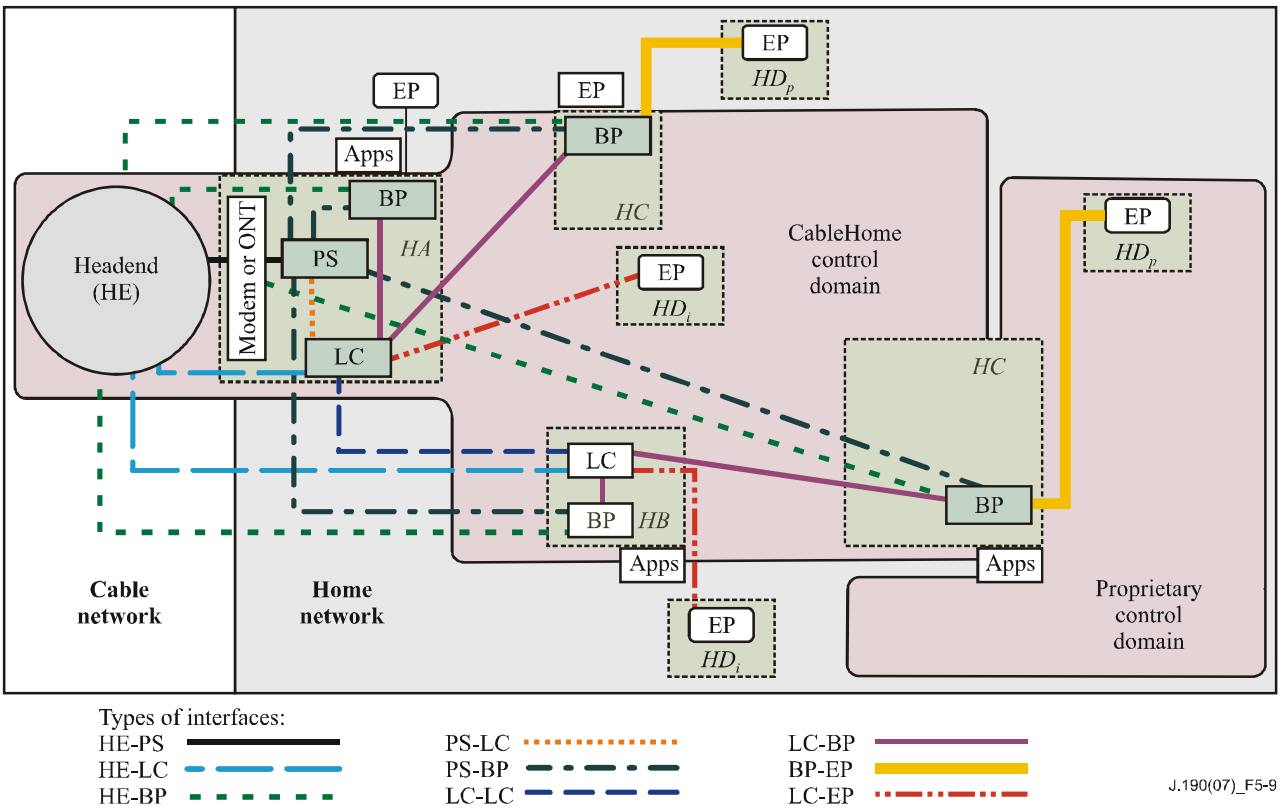

Figure 5-9 – MediaHomeNet reference interfaces

Table 5-7 – Valid functionality interface paths

Functionality	Considered protocol	HE-PS	HE-LC	HE-BP	PS-LC	PS-BP	LC-LC	LC-BP	BP-EP	LC-EP
QoS	ex. UPnP QoS		√	√			√	√		√
Name service	DNS	√			√	√				√
Software download	TFTP	√	√	√						
Address acquisition	DHCP	√			√	√				√
Management-WAN (single) (bulk) (logging)	 SNMP TFTP SYSLOG	 √ √ √								
Management-LAN (single) (user) (logging)	 UPnP, ex. HTTP ex. UPnP				 √ √	 √ √				 √ √
Security (key distribution) WAN		√								
Security (key distribution) LAN					√	√				√
Security (authentication) WAN		√								
Security (authentication) LAN					√	√				√
Ping	ICMP				√	√				√
Loopback	Echo				√	√				√
NOTE – The BP-BP interface is not applicable.										

5.7 IPNet2Home information reference model

The operation of the IPNet2Home management model is based upon a store of information maintained in the PS by the various PS functions (CAP, CDP, CMP, etc.). These functions must have a means of interacting via information exchange, and the PS database is a conceptual entity that represents a store for this information. The PS database is not an actual specified database *per se*, but rather a tool to aid in the understanding of the information that is exchanged between the various IPNet2Home elements.

Figure 5-10 shows the relationship between the database and the PS functions. Table 5-8 describes the typical information associated with each of these functions. Figure 5-11 shows a detailed example implementation indicating the set of information, the functions that derive the information, and the relationships between the functions and the information.

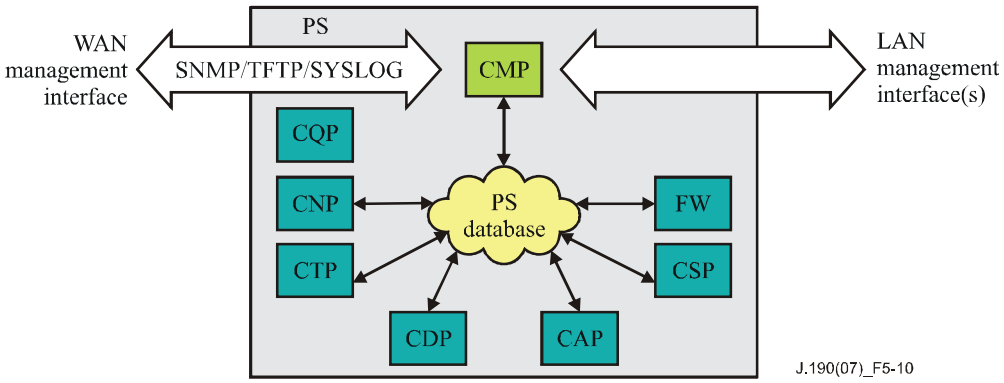

Figure 5-10 – PS function and database relationship

The PS database stores a myriad of data relationships. The CMP provides the WAN management interface to the PS database. The IPNet2Home functions within the PS enter and revise data relationships in the PS database. Additionally, the IPNet2Home functions within the PS may retrieve information from the PS database that is maintained by other IPNet2Home functions within the PS.

Table 5-8 – Typical PS database information examples

Name	Usage (in general)
CDP information	Information associated with addresses acquired and allocated via DHCP.
CAP information	Information associated with IPNet2Home address translation mappings.
CMP information	Information associated with the state of the management functions.
CTP information	Information associated with results of LAN test performed by the CMP.
CNP information	Information associated with LAN IP Device name resolution.
USFS information	Information associated with the upstream selective forwarding switch function.
CSP information	Information associated with authentication, key exchange, etc.
Firewall information	Information associated with the behaviour of the firewall (rule set) and firewall logging.
Event information	Information associated with the local log for all general events, traps, etc.

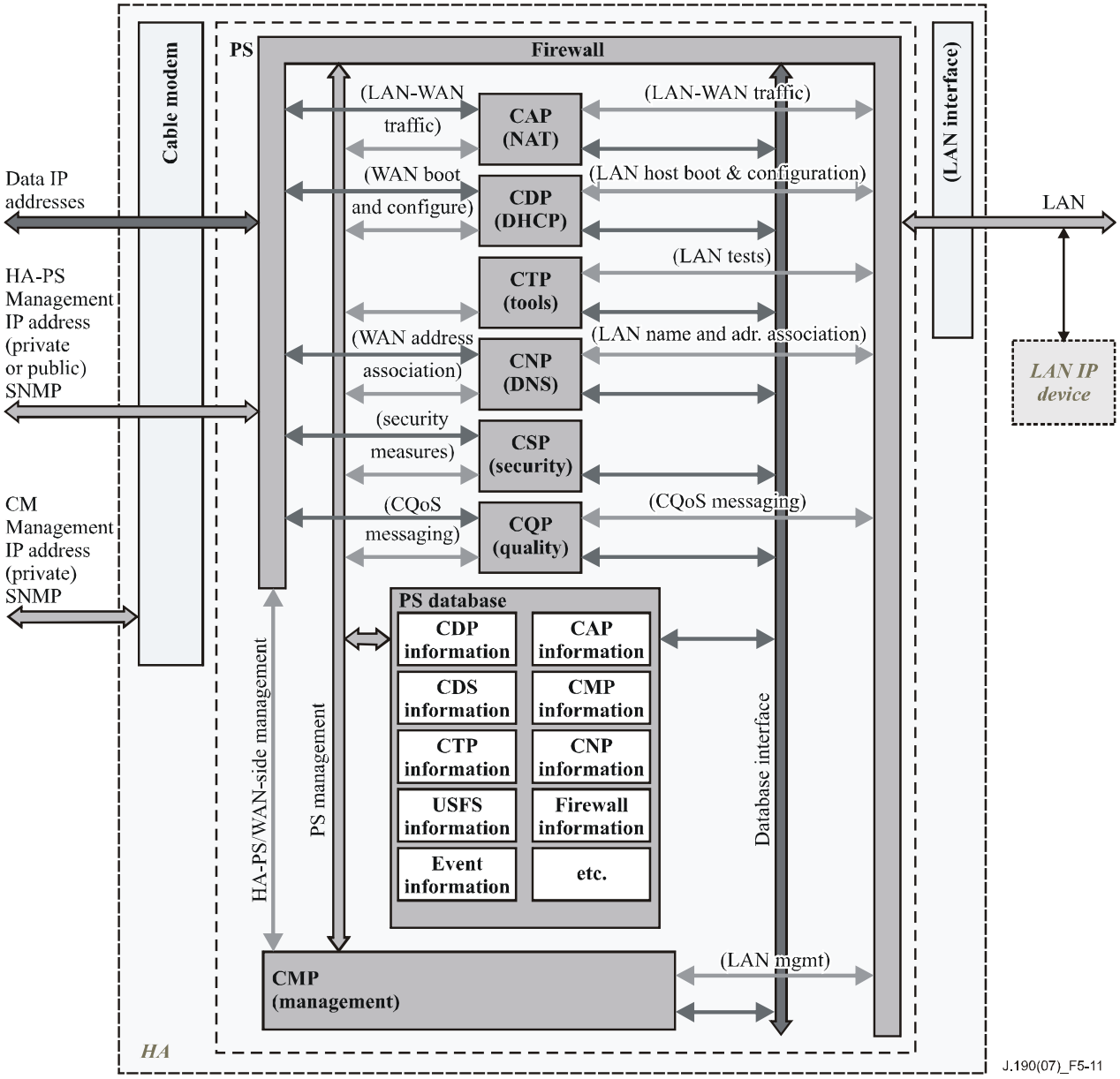

Figure 5-11 – PS database detailed example implementation for cable access network

The **PS** is managed from the WAN via the CMP, and to a large degree this involves access to the information in the PS database. Management is used for initialization and provisioning of the WAN side network elements, and diagnostics or status of the LAN. The diagnostics may rely on the CTP to get better visibility into the current state of the LAN. Connectivity and rudimentary network performance can be measured.

The **CNP** is the LAN domain name system (DNS) manager. All LAN-Trans LAN IP devices are configured by the CDP to use the CNP as the primary name server. The CNP resolves textual host names of LAN IP devices, returning their corresponding IP addresses and, in addition, refers LAN IP devices to external DNS servers for requests that cannot be answered from local information. The CNP only responds to DNS queries on the LAN-Trans realm.

The **CDP** contains the address functions to support the DHCP server in the LAN-Trans realm and a DHCP client in the WAN realms.

The **CAP** creates address translation mappings between the WAN-Data and LAN-Trans address realms. The CAP is also responsible for upstream selective forwarding switch decisions to preserve HFC upstream channel (WAN) bandwidth from the local LAN only traffic. Finally, the CAP contains the CPT function that bridges traffic between the LAN and WAN address realms.

The **CSP** provides PS authentication capabilities as well as key exchange activities.

The **CQP** is part of a system that enables IPCablecom quality of service (QoS) through the PS. The CQP, acting as a transparent bridge, forwards IPCablecom-compliant QoS messaging between IPCablecom applications and the IPCablecom QoS infrastructure.

The **firewall** is implementation-specific, and IPNet2Home does not specify the details of firewall implementation.

Appendix I

Home-networking requirements for cable-based services

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

I.1 Scope

This appendix provides an informative list of home-networking requirements in order to effectively provide for the delivery of cable-based services throughout the home.

I.2 Informative references

No more additional references than in the main body.

I.3 Terms and definitions

This appendix defines the following terms:

I.3.1 access node: As used in this appendix, an access node is a layer two termination device that terminates the network end of the cable modem connection. It is technology specific. In Annex A of [b-ITU-T J.112] it is called the INA while in Annex B it is the CMTS.

I.3.2 access point: The customer device that provides the functionality required to connect the home network to the cable network.

I.3.3 device of consumption: The customer device that terminates and uses the application being transported by the cable network and home network. Examples include printers, TV sets, etc.

I.3.4 home network: A short-range communications system designed for the residential environment, in which two or more devices exchange information under some sort of standard control.

I.3.5 service flow: A unidirectional, coherent stream of data used to provide all or part of a specific network-based service.

I.3.6 terminal devices: On the home network, these may include personal computers, computer peripherals, set-top boxes, network appliances, and specialized service termination devices (e.g., an IPCablecom MTA, or audio-visual equipment such as an MP3 player).

I.4 Abbreviations

This appendix uses the following abbreviations in addition to the ones in the main body.

CBR Constant Bit Rate

MAC Media Access Control

I.5 Introduction

The cable television physical platform provides the most capable means of delivering interactive broadband network-based services to a majority of households. It is in the best interests of both consumers and cable operators to extend this fundamental bandwidth advantage to every possible device within the home. This will benefit consumers by improving their home network and cable service experience. It also will benefit cable operators by creating enabling technologies that will positively allow them to differentiate their services and generate new revenue streams. Furthermore, it will benefit the producers of home-networking equipment by spurring the demand for their products, in addition to fueling the interactive applications and development industry.

In order to extend the fundamental bandwidth advantage of cable to all devices connected to the home network, it is necessary for home networks to satisfy a number of requirements pertaining to network performance, quality of service (QoS) and network management. These requirements look beyond the extension of cable modem QoS and IPCablecom support across home networks, to the future development of "network-aware" devices that allow cable operators to provision and manage cable services remotely. As such, these requirements should be regarded as building blocks that can be used to enable the delivery of future generations of cable-based services.

The purpose of this appendix is to identify the technology interface requirements that all appropriate home-networking technologies can use for access to the cable network. This appendix spans the description of service data types, requirements for system performance, QoS support, network-based management and local network management.

This appendix addresses networks that are installed in residences and used for the transport of information encoded in a digital format. The primary emphasis of this appendix will be on IP-based networks. However, some aspects also will apply to the primary distribution of digital media (digital video and audio information) over cable networks.

I.5.1 General description

A home network is a short-range communications system designed for the residential environment, in which two or more devices exchange information under some sort of standard control. Terminal devices on the home network may include personal computers, computer peripherals, set-top boxes, network appliances and specialized service termination devices (e.g., an IPCablecom MTA, or audio-visual equipment such as an MP3 player). A home network may use one or more physical media, and may be comprised of sub-networks that are connected via bridges. Physical media may include twisted-pair cable, coaxial cable, telephone wiring, power mains, optical fibre, RF wireless and IR wireless.

In order for a terminal device (node) on a home network to become a device of consumption for cable-based IP services, the device must be able to receive services provided by the cable operator over the cable access network. In order for this to happen, the home network must be connected to the cable data network through an access point which will contain the communications functionality of a cable modem (e.g., [b-ITU-T J.112] and [b-ITU-T J.122]) (but may not include all of the interfaces, e.g., Ethernet, stipulated by the cable modem specification). A service flow is a unidirectional, coherent stream of data used to provide all or part of a specific network-based service (e.g., one side of a full duplex IPCablecom two-way communication)[1]. The access point may be in one of many different forms, such as a cable modem, a set-top box with an embedded cable modem, or a residential gateway that integrates several of these functions.

Home networks are similar to local area networks (LANs) developed for the enterprise environment, but are expected to have the following differentiating characteristics:

- Home networks must be very simple to install, configure and maintain. Most homes do not have access to technical network management services.
- Home-network components need to be offered at consumer price points and capable of distribution through consumer electronics channels.
- Technologies comprising home networks will be more heterogeneous than typical business LANs.

---

[1] A more detailed definition of the term "service flow" comes from the J.112 specification: A **service flow** is a MAC-layer (Layer 2) transport service that provides unidirectional transport of packets either upstream or downstream, and is characterized by a set of quality of service (QoS) parameters such as latency, jitter and throughput assurance.

- Home networks may suffer a greater range and variety of signal impairments than a typical business environment due to the ad hoc nature of the in-home electronic environment.

Home networks may be called upon to support a wide variety of network interfaces as illustrated by Figure I.1.

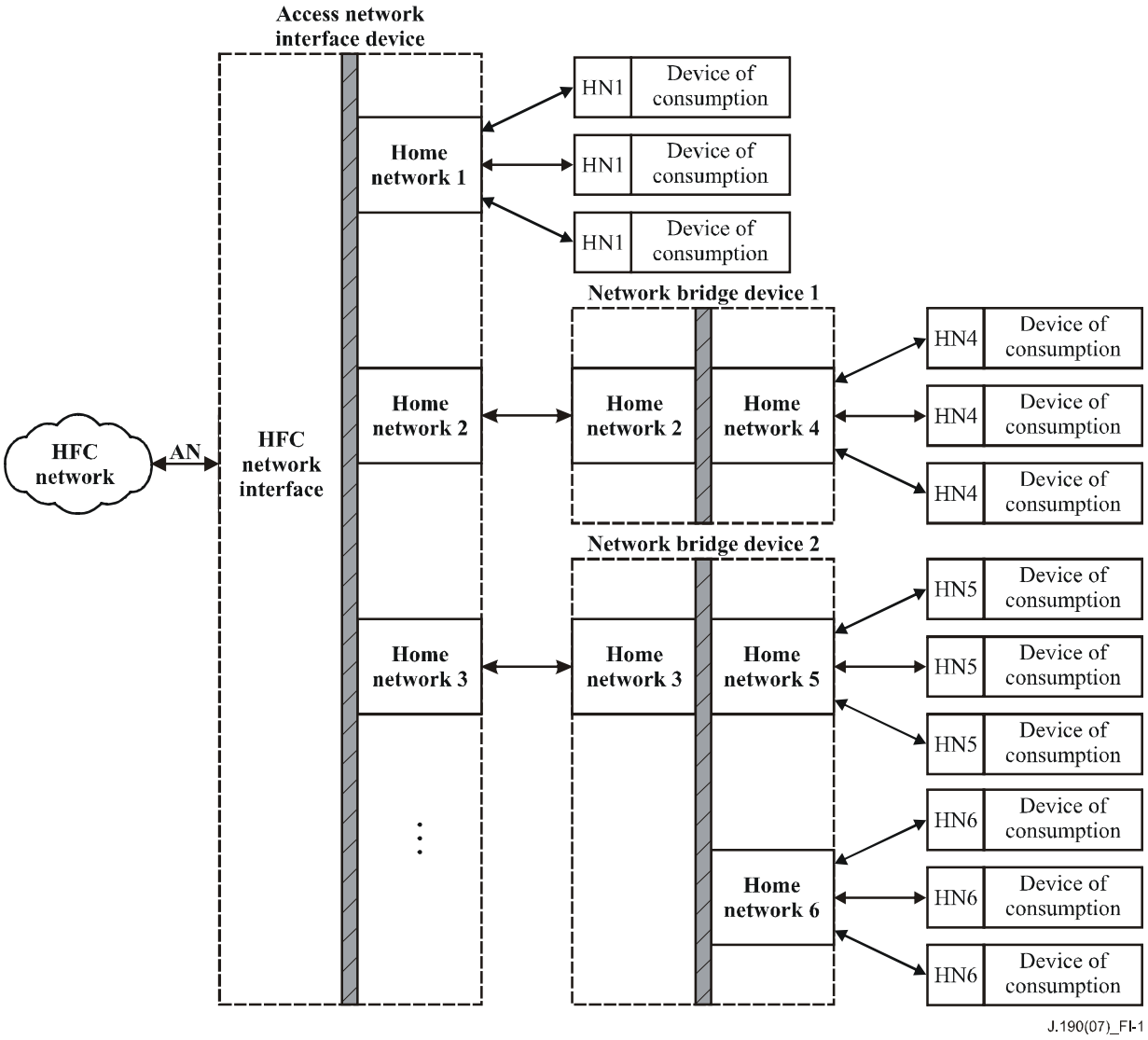

Figure I.1 – Generic home network interfaces

Figure I.1 illustrates several fundamental topological features of a home network. Services are delivered to the home through the hybrid fibre/coax (HFC) cable infrastructure over a cable modem platform. These services are then distributed throughout the home to one or more devices of consumption over the home network system, which may consist of a series of unlike networks.

Interfaces between the HFC network and home networks, and between subsequent home networks, are shown in Figure I.1 as network-specific lower layer interfaces joined through an undefined mapping function, depicted as a hash-marked bar. Some sub-networks may not directly interface to the HFC network, but can gain access through another network that does.

Access to the hybrid fibre/coax cable (HFC) network is provided through an access network interface device, which supports one or more interfaces to different home-network transport technologies. A device of consumption may be a node on the network with direct interface to the cable modem network, or it may be a node on subsequent networks, separated from the cable

modem network by another in-home network. A bridge device implements the interfaces between two or more in-home networks that are typically of different transport technologies. (The access network interface device may act as a bridge in certain implementations.) A fundamental requirement of home networks is that they deliver cable-based services seamlessly from the HFC network to devices of consumption.

I.5.2 Desired product benefits to consumers of a home network

Home PC and consumer electronics equipment owners will enjoy several benefits offered by networking their devices together:

- Sharing of files and scarce resources, e.g., scanners, printers, digital cameras and Internet access point.
- Seamless distribution of advanced broadband services, e.g., interactive games, remote network management, video-on-demand (VoD).
- Enhanced ability to control devices and monitor activities remotely.
- Convenience of access to network resources from anywhere in and around the house or even remotely.

I.5.3 Desired product benefits of home networks for the cable industry

Cable operators can expect to see some benefits from the installation of data networks in their subscribers' homes as well. Three advantages are listed below:

- Facilitate low-cost and scalable provisioning of high-speed data service.
- Enable or facilitate the delivery of revenue-generating advanced interactive services.
- Add value to attract potential high-speed data service subscribers.

I.6 Background: Cable data services

Cable operators intend to provide consumers a number of network-based services using the cable modem high-speed data platform. Several of these services are described here in order to provide an indication of the types of network traffic that the home network must support in order to provide consumers a "seamless" customer experience. These services are differentiated by a number of factors, including varying quality of service (QoS) levels and transport data rates.

I.6.1 High-speed data services

Cable-based, high-speed data service is the provision of an asynchronous connection to the Internet (or a "walled-garden" Intranet with an Internet gateway) using a physical connection via a cable modem with data communications support based on the standard suite of IP networking protocols. Data services can be divided into two groups: best effort and media streaming.

I.6.1.1 Best-effort services

Best-effort high-speed data services are offered on a best-effort basis with no guarantees on sustainable data rate, QoS or service availability. Examples of these services include Internet web surfing, file transfers/downloads, email, and various network management services such as application updates, service provisioning and performance monitoring.

I.6.1.1.1 Performance characteristics

Best-effort data packets are sent asynchronously, and the average data rate is determined by the content being accessed up to rate limits that may be enforced by the broadband service provider. The apparent (to the user) rate of data transfer may be determined by factors outside of the access network, such as network congestion on the backbone network and insufficient bandwidth on the connection between the AN and the backbone network. On the access network, sustained average

data rates of 25 kbit/s upstream and downstream data rates of 384 kbit/s for casual websurfing are regularly encountered.

Performance requirements for best-effort services can vary significantly depending upon the type of service used. General Internet web surfing usually requires at least an 80 kbit/s downstream rate and 25 kbit/s upstream rate to support tolerable interactive response times. End-to-end mean packet latency should not exceed 500 ms. Since Internet backbone latency delays are significant and hard to predict, any delay added by the cable or home network should be small. On a satisfactorily provisioned cable network, latency typically does not exceed 2 ms downstream and 10 ms upstream for best-effort traffic, assuming there is no significant contention with other higher priority services. Given that home networks are significantly smaller and less complex, packet latency delays should not exceed those of the cable network.

Best-effort services such as email or file transfer do not have strict packet latency or bandwidth requirements. However, network performance should be sufficient to support the transfer of typical email and file information within seconds of being sent.

I.6.1.1.2 Service attributes

Best-effort data services, which can include various levels of QoS, have different customer service attributes in the areas of service provisioning, network management, QoS and internetwork bridging with non-IP networks. These attributes are necessary in providing the customer with a quality, user-friendly experience. The technical requirement tables in clause I.7 were derived in order to support these attributes. The following list identifies each attribute in its respective group:

Service provisioning

- Networked devices will establish service with the cable network with a minimum of user intervention. Devices will meet or exceed "Plug and Play" expectations set by the PC industry where devices are capable of automatic configuration and operation when connected to the network.
- Communication between IP devices on different physical and logical networks within the home will be seamless (inter-network service delivery will be supported).
- Access to copyrighted content will be provided.
- Access to the Internet will be provided.
- The home network will have access to protection against malicious activity from the WAN, such as what is offered by a firewall.
- Billing services will be provided.
- Self-provisioning and service upgrades will be available for new services.

Network management

- The home network will recover gracefully from service disruptions.
- Adding devices to the network and removing devices from the network will not disrupt service to other connected devices.
- Loss of service from the service provider will not impair communication between networked devices within the home.
- Multiple networked devices in the home will be able to receive high-speed data service simultaneously.

QoS

- QoS guarantees as defined in service agreements and delivered over the cable modem platform will be preserved across the home network.

Internetwork bridging with non-IP networks

- Devices on IP networks will seamlessly exchange data and control information with devices on non-IP networks (support of cross-platform service delivery).

I.6.1.2 IP media streaming

IP media streaming refers to the transport of real-time audio and video (A/V) data using the Internet protocol (IP) suite across IP data networks such that data is played back as it is received by the network client. For many years, the method for broadcasting real-time A/V content has been a combination of both analog and compressed digital (MPEG) signalling. This architecture has mainly consisted of a unidirectional, point-to-multipoint broadcast configuration.

With the recent advances in digital-IP network technology, highly compressed real-time A/V streams with lower quality can now be transmitted with bidirectional, unicast, multicast, or broadcast capabilities. Although there are still challenges to overcome in providing sufficient bandwidth and maintaining real-time performance parameters, broadcast quality IP media streaming is being actively developed.

Terminal devices on home networks will receive and sometimes transmit streaming media content. Media types will consist of short audio and/or video clips such as movie trailers that last only a few minutes, or they may be full length movies, radio station broadcasts or live events that may last for several hours. It is also expected that, in the future, the broadcast of digital MPEG A/V streams will converge with IP digital-network media streaming to provide a single digital format for delivering data, voice and streaming A/V services to the home.

I.6.1.2.1 Service description

IP media streams are digitized audio and video signals that have been compressed into serial data streams for transmission over a unicast or multicast medium. They consist of variable size data packets transmitted on a periodic basis.

IP media-streaming packet structure consists of 40 bytes of header information and 64 to 1518 bytes of payload data. Header bytes are used for network routing, control and synchronization, which support IP, UDP, and RTP network and application protocols for real-time media streaming. Payload data may consist of any type of A/V data depending upon the codec method that source and destination applications use.

MPEG-2 is a popular systems transport technology due to its efficiency, flexibility, and quality in broadcasting A/V streams. It consists of multiple audio, video and data elementary streams that can be independently managed and synchronized for a given program. The compression algorithm, which is based upon the perception characteristics of the human eye and ear, can support multiple data rates from low to high speeds, which in turn effects the quality of playback. Currently, most streaming-media applications are tailored for use on low-speed (dial-up) data rate systems. As bandwidth capacity increases and real-time parameters are maintained, the quality of IP media streams will become equivalent to or better than broadcast technologies we already use.

While MPEG-2 can stand on its own and is currently used for broadcasting digital A/V signals in cable and satellite networks, it lacks the one-to-one or one-to-group addressing characteristics that IP was designed for. It also does not have a good mechanism for supporting "guaranteed delivery" of data like IP control protocols that are used to retransmit lost packets and provide flow control for data connections.

IP media streaming will require an efficient transport mechanism for the distribution of A/V content between devices across IP networks. The combination of MPEG-2 codec data and IP networking protocols is one method that can support these requirements. While the additional overhead and contention characteristics of IP networks will reduce the efficiency of MPEG-2 streams, technology

developments in header compression, network QoS, and increased bandwidth capability will minimize these negative effects making them insignificant.

For low bandwidth A/V streaming applications, new codec standards are emerging named MPEG-4 and MPEG-7. MPEG-4 provides the standardized technological elements enabling the integration of the production, distribution and content access paradigms for the fields of digital television, interactive graphics and interactive multimedia. MPEG-7, formally named "Multimedia Content Description Interface", aims to create a standard for describing the multimedia content data that will support some degree of interpretation of the information's meaning, which can be passed onto, or accessed by, a device or a computer code. MPEG-7 is not aimed at any one application in particular; rather, the elements that MPEG-7 standardizes shall support as broad a range of applications as possible and would include identifying the characteristics of audio/video streaming feeds and file downloads.

I.6.1.2.2 Performance characteristics

The degradation of IP A/V streams are mainly caused by compression ratio, corrupted data bits (measured by the bit error ratio) and packet delays. The compression ratio is usually determined by the bandwidth allocation. The less bandwidth there is available, the more compression is needed for a given A/V stream. Bandwidth requirements vary for different types of media streams and different levels of quality. The following list indicates the IP payload rate requirements for different services:

IP media streaming service	Payload data rate
Standard audio (mono)	96 to 256 kbit/s
CD-quality audio (stereo)	192 to 256 kbit/s
Low-quality video	64 to 500 kbit/s
High-quality video	1.5 Mbit/s to 10 Mbit/s
High-definition video	19.68 Mbit/s

The cable industry expects to simultaneously support a multiplicity of these services, and the aggregate data rates are expected to exceed 50 Mbit/s.

Bit error ratio is determined by the measurement of loss or corruption of data as it traverses the network medium. It should not exceed 10^{-6} to avoid noticeable artifacts in the playback of A/V streams that are irritating to the listener/viewer. This threshold is lower, around 10^{-8}, for IP media streams that are expected to be higher quality such as CD-quality audio and broadcast quality video.

Packet delays are typically caused by network-forwarding equipment such as routers or bridges that contribute a variable amount of propagation and jitter delay as data packets enter and leave each device. Although protocol processing adds to packet delays, the main variable delay component is caused by traffic congestion due to multiple services using the same network medium whose combined bandwidth demands exceed that which is available.

To reduce packet jitter and propagation delays for real-time IP media streaming services, application-specific protocols called UDP and RTP are used in conjunction with IP and QoS mechanisms for control and synchronization of payload A/V data. Networks that implement QoS will minimize multiple service contention and improve the quality of IP A/V stream distribution. While these streams do not require QoS for operation, those with it will benefit from a higher quality and more robust playback.

IPCablecom protocols, developed by cable industry members and product vendors, can be used by IP media streaming service providers for enhanced QoS communications over the cable network. These protocols provide a dynamic mechanism using the cable modem QoS implementation for supporting end-to-end, real-time communications.

I.6.1.2.3 Service attributes

IP media streaming services have different customer service attributes in the areas of service provisioning, network management, QoS and internetwork bridging with non-IP networks. These attributes are necessary in providing the customer with a quality, user-friendly experience. The technical requirement tables in clause I.7 were derived in order to support these attributes. The following list identifies each attribute in its respective group:

Service provisioning

- Service support for the delivery of independent simultaneous audio and video streams to multiple devices on a home network must be provided.
- Easy customer access to streaming media products and account information must be available.
- Service offering must support both broadcast and on-demand delivery of media streams.

Network management

- All home-network devices must be able to receive streaming media services.
- Tools for monitoring and controlling network loading and performance must be available to both cable operator and home-network consumer.
- Verification of service delivery and proper operation data must be available for both cable operator and home-network consumer.
- Firewall and other gateway applications can be managed by the cable operator to ensure the delivery quality of the streaming media services.
- Copy protection of copyrighted content must be supported and passed when appropriate.

QoS

- Streaming media quality levels must be maintained across the cable and home network.

Internetwork bridging with non-IP networks

- Home networks must support cross-platform streaming media service delivery.

I.6.2 IPCablecom

The term "IPCablecom" is a name given to a set of interface specifications and protocols that have been developed by the cable television industry and product vendors to deliver voice and video services over the hybrid fibre/coax (HFC) cable systems utilizing a cable modem. IPCablecom utilizes a network superstructure that overlays the two-way, data-ready broadband cable access network. While the initial IPCablecom offering is packet-based voice communications for existing and new cable subscribers, the long-term project vision encompasses a large suite of packet-based services.

I.6.2.1 Service description

IPCablecom consists of a variety of functional components, each of which must work in harmony to create a consistent and cost-effective delivery mechanism for packet-based services. These components include service signalling, QoS, security, provisioning and billing protocols.

As mentioned earlier, the first service to be developed under this set of characteristics is IP telephony, but the characteristics of IPCablecom extend far beyond this particular service offering. Other services may include interactive gaming with real-time voice communications among players, videoconferencing, etc.

I.6.2.2 Performance characteristics

The particular performance characteristics required will be different for each IPCablecom service deployed. For basic IP telephony, each two-way conversation will require a full duplex data payload of 128 kbit/s (64 kbit/s in each direction) for each active conversation. Network capacity should support a minimum of four simultaneous conversations supported per subscriber. The maximum packet latency should not exceed 20 ms between the AN and terminal device on the home network. The maximum end-to-end packet delay should not exceed 200 ms to maintain "toll quality" voice responsiveness. To avoid a noticeable, irritating degradation in sound quality, the packet loss rate should not exceed 1%. IPCablecom telephony traffic is usually assigned the highest level of priority on the cable modem QoS system.

I.6.2.3 Service attributes

IPCablecom services have different customer service attributes in the areas of service provisioning, network management, QoS and internetwork bridging with non-IP networks. These attributes are necessary in providing the customer with a quality, user-friendly experience. The technical requirement tables in clause I.7 were derived in order to support these attributes. The following list identifies each attribute in its respective group:

Service provisioning

- The service will support broad family of multimedia services including telephony.
- The service will support creation of new service types and features including cross-platform delivery.
- Support of multiple line telephony: Any session may be routed to any terminal device on the home network.
- Support of self-provisioning of IPCablecom services and service upgrades.

Network management

- Multiple simultaneous sessions for IPCablecom and other services will be supported.
- Phone calls and other sessions will be billed to the appropriate (terminal) number.
- Outside plant network operations will be maintained with carrier grade reliability.
- Assistance in fault isolation will be provided.
- The home network will support bandwidth on demand to appropriately support delivered services.

QoS

- QoS support will be provided for real-time CBR services.
- Services will be delivered with carrier-grade quality, including low latency and packet loss between the AN and user device of consumption.

Internetwork bridging with non-IP networks

- The service will support message forwarding to non-IP networks (i.e., call waiting display on TV).

I.6.3 General issues

I.6.3.1 Security needs

- Service content confidentiality/encryption and copy protection can be best provided by service-/application-specific sources. Therefore, since the IPNet2Home architecture is not service-/application-specific, it is considered outside the scope for IPNet2Home to define these specific mechanisms.

- The amount of trust needed for IPNet2Home elements is about the same amount needed for authenticating a cable modem. There may exist a subset of elements with less trust (e.g., a serial number instead of a certificate) contained within devices not directly connected to the HFC network (HB/HC devices).

I.6.3.2 Network address management needs

- When NAT is provided in residential gateways, it will be necessary to comply with IPNet2Home addressing requirements.
- Distribution and control of addresses to the home will be administered by a single address management system residing on the cable infrastructure.

I.7 Service support requirements

Services delivered from the service provider to users over home networks are listed and described in the previous clause. This clause describes capabilities that home networks must support in order to ensure seamless delivery of cable-based services to users. These capabilities include requirements for system interface and performance, QoS, network management, security and network address management.

I.7.1 System interface and performance requirements

The cable modem high-speed data network is a fundamental-enabling technology that allows cable operators to make a wide variety of service offerings. A service offering to a consumer may be comprised of a single service type (e.g., best-effort high-speed data access with unlimited usage or a IPCablecom-based telephony offering). It is more likely, however, that a service offering will be comprised as a bundle of a variety of service types and offered in access-level tiers[2].

Three fundamental requirements for home networks are:

- Home networks must allow multiple devices to share a single high-speed data network access point (cable modem).
- Home networks must enable the simultaneous consumption of multiple service types by multiple devices.
- A home-networking technology must not adversely affect services delivered over the HFC infrastructure in such a way as to degrade performance upstream or downstream from its position in the home network.

The consumption of multiple services is limited by several factors. These include access network management tools that enforce service tier parameters, the ability of the Internet infrastructure and access network to support the data load demanded by the user population, and the ability of the home network infrastructure to support the load demand placed on it by its users.

As the density of electronic systems within the home increases, the possibility of electro-magnetic interference (EMI) between systems increases. Radio frequency emissions, voltage transients, and all other undesired output from a home networking device or medium must be controlled or otherwise limited to keep performance parameters within bounds specified in Table I.1 and in cable modem Recommendations.

---

[2] Access-level tiers can be differentiated by both the mix of service types offered and by consumption limits on access network bandwidth.

Table I.1 – Performance requirements for IP and packet-based home-networking services

Service	Relative priority	MAC payload rate (per stream)	Minimum simultaneous streams	Minimum physical layer data rate	Maximum bit error ratio	Maximum latency	Maximum jitter
IPCablecom services							
High-quality narrow-band voice telephony	High	32 to 64 kbit/s	8 (4 conversations @ 2 streams per conversation)	750 kbit/s	10^{-6}	5 ms nominal, 10 ms maximum	±5 ms
Low-quality narrow-band voice telephony	Low to Medium	6 to 16 kbit/s	8 (4 conversations @ 2 streams per conversation)	200 kbit/s	10^{-6}	10 ms nominal, 30 ms maximum	±20 ms
Time-critical packet services (e.g., videoconferencing)	High	4 to 13 kbit/s for voice and 0.032 to 1.5 Mbit/s for audio/video	4 (2 conversations @ 2 streams per conversation)	8 Mbit/s	10^{-8}	5 ms nominal, 10 ms maximum for full duplex services	±5 ms
High-speed data services							
Best-effort service	Low	Up to maximum available physical layer rate	N/A	2 Mbit/s	10^{-6}	500 ms	N/A
QoS (SLA) service	Medium to high	10 Mbit/s	2	10 Mbit/s	10^{-8}	10 ms nominal, 30 ms maximum	±10 ms
IP media streaming							
Standard audio	Low to Medium	96 to 256 kbit/s	3	1 Mbit/s	10^{-6}	200 ms	±20 ms
CD-quality audio	Medium	192 to 256 kbit/s (stereo)	3	1 Mbit/s	10^{-8}	100 ms	±10 ms

Table I.1 – Performance requirements for IP and packet-based home-networking services

Service	Relative priority	MAC payload rate (per stream)	Minimum simultaneous streams	Minimum physical layer data rate	Maximum bit error ratio	Maximum latency	Maximum jitter
Lower-quality video streaming	Medium to High	64 to 500 kbit/s	3	2 Mbit/s	10^{-6}	100 ms	±10 ms
Higher-quality video streaming	High	1.5 Mbit/s to 10 Mbit/s	1	10 Mbit/s	10^{-8}	50 ms	±10 ms
Broadcast-quality video							
SDTV	High	3 to 7 Mbit/s	2	10 Mbit/s	10^{-8}	Nominal delay of 90 ms	Interpacket ±10 ms
HDTV	High	19.68 to 38 Mbit/s	1	38 Mbit/s	10^{-8}	Nominal delay of 90 ms	Interpacket ±10 ms

The service load on the in-home network will vary from user to user and from household to household. For example, a single person living alone can easily be envisioned to simultaneously watch a streaming video (e.g., a football game), best-effort web service (access football scores), receive a fax (confirmation of a hotel reservation previously booked on a travel web site), and talk on the telephone. A household with two adults and several children may desire to simultaneously consume multiple-streaming audio, a streaming video, several best-effort web service sessions, multiple telephone calls, and inside-the-home (device-to-device) network traffic. The home network will be called on to simultaneously support all of these sessions, typically, 3 simultaneous HDTV streams. This aggregate service load is expected to exceed 100 Mbit/s.

As network-based services are delivered to devices of consumption on the home network, the service must flow through the physical and logical interfaces between unlike networks. The interfaces to home networks must be compatible with cable modem technology. Services and capabilities provided by a cable modem should be preserved in subsequent networks in the home.

Network performance requirements for each of the service types described in clause I.6 are summarized in Table I.1. Table entries are intended to serve as a reference for home-networking product developers. A description of each of the performance parameters follows:

– **Relative priority**: The priority (low, medium or high) a service should receive for access to the communication channel, relative to other services.

– **Payload rate**: The net rate of data delivered to the user, in bits per second.

– **Minimum simultaneous streams**: The minimum number of service flows simultaneously active that a home-networking technology must be able to support.

– **Minimum physical layer data rate**: The minimum rate of data traffic including overhead information, in bits per second; also referred to as the channel rate or the raw data rate.

– **Maximum bit error ratio**: The maximum allowable rate of incorrect or lost data bits received by the device of consumption.

– **Maximum latency**: The maximum allowable one-way data delay in the home network between the access network interface, e.g., the cable modem, and the intended device of consumption.

– **Maximum jitter**: The maximum allowable intra-packet time of arrival variation between successive packets.

NOTE – In the following tables, the requirements are listed with a reference index to allow easy referral. The indices typical start with an abbreviation related to the subject area. The reference indices are not always sequential.

I.7.2 Service provisioning requirements

Installing and configuring home networks and initiating service are fundamental tasks that must be accomplished before the cable operator can provide the broadband products described earlier. The requirements listed in Table I.2 provide the basic functionality needed to enable these tasks and to provide reliable network operation once service is established.

Table I.2 – Cable service provisioning requirements

Number	Requirement
S.1	**Ease of installation**: Home-network devices must be easy to install and configure for operation, much like a home appliance.
S.2	**Self-provisioning**: Devices connected to the home network must support self- and remote provisioning of broadband services, including network configuration and device-specific service-enabling tasks.
S.3	**Network management**: All network management features and functions relevant to services provisioned to devices on the home network must be preserved across home-network interfaces, including when NAT is employed. Examples include IP address assignment, security, remote provisioning and diagnostics.
S.4	**Protocol translation**: Home-network bridging devices must properly perform required protocol translations.
S.5	**Device connection**: Home networks must support connection and disconnection of terminal devices without interrupting service or degrading the performance of other devices connected to the network.
S.6	**Firewall security**: Home networks require protection from malicious attacks or access across external networks, such as the protection offered by the firewall. The protection service must be easy for the subscriber to manage and must function over multiple active gateway devices.
S.7	IPNet2Home will provide a mechanism by which the PS can download and process IPNet2Home configuration files.
S.8	IPNet2Home will provide a mechanism by which the PS can achieve time synchronization with the headend network.

I.7.3 Network management requirements

As consumers install data networks in their homes, their need for network management support will soon follow. They will come to realize how they have taken for granted the valuable services provided by their office information systems group. Unfortunately, most consumers will not be able to afford their own personal network administrator.

Reducing the complexity of managing home networks will be a key issue for both consumers and service providers impacting the rate at which home networks are deployed and the overall success of the home-networking market. The best way to deal with this issue is through network/product design, available tools and network management services.

The end-to-end network systems management requirements identified in Table I.3 relate to how broadband providers monitor, configure and remotely manage home networks.

Table I.3 – End-to-end network management requirements

Number	Requirement
Mgmt.1	**Interface for management and diagnosis**: Interfaces should support management of cable-based services provisioned across the home network (e.g., SNMP V1/V2c/V3).
Mgmt.2	**Diagnostic tools**: Diagnostic tools having local and remote monitoring capabilities that can monitor home-network operation and help the consumer and broadband provider identify problem areas must be provided (e.g., ping and data loopback on port 7).
Mgmt.4	**Interface for event reporting**: Interfaces should support reporting of events.
Mgmt.5	Interfaces will support the management and diagnosis features and functions required to support cable-based services provisioned across the home network.
Mgmt.6	**Stand-alone operation**: Loss of connection between broadband service provider(s) and the home network must not disable or degrade the operation of internal home-networking functions.
Mgmt.7	**Recovery**: The home network must recover gracefully from a power outage and devices connected to the home network must return to the operational state they were in prior to the outage.
Mgmt.8	Home-network devices will be easy to install and configure for operation, much like a home appliance.
Mgmt.9	The need exists for interfaces to support the management and diagnosis features and functions required to support cable-based services provisioned across the home-network.
Mgmt.10	Local and remote monitoring capabilities that can monitor home-network operation and help the consumer and cable operator identify problem areas are needed.
Mgmt.11	**Device visibility**: A method must be provided to the cable network NMS to gather identification information about each IP device connected to the home-network.
Mgmt.12	**Device connection state**: A method must be provided to the cable network NMS to detect whether a connected device is in an operable state.
Mgmt.13	Provide domain name system (DNS) from a server in the PS to DNS clients within LAN IP devices, for name resolution of LAN IP devices (independent of the state of the WAN connection).
Mgmt.14	Provide DNS referral to headend DNS servers, for DNS clients within LAN IP devices, for resolution of non-local hostnames.
Mgmt.15	**IP address management**: The home network must accommodate cable network-based IP address management as first priority and provide an in-home IP address assignment mechanism to keep the home network functioning properly if the network-based service becomes unavailable. IP address assignment and configuration must occur automatically as devices are connected to the network, and IP address management must be scalable to support the expected increase in the number of IP devices in homes.
Mgmt.16	**Direct connectivity**: A method must be provided to the cable network NMS to establish a direct IP communication with an IPNet2Home-compliant element connected to the home network.
Mgmt.17	**Address assignment configuration**: A method must be provided to the cable network NMS to configure the number and type of IP addresses assigned to elements connected to the home network.

I.7.4 Quality of service support requirements

As the number of home-networking devices and services increase, so will data traffic congestion. This will cause increases in variable packet and data propagation delays that may exceed end-to-end service latency requirements. These effects will have a negative impact on real-time services and degrade the overall performance of the home network.

Therefore, home-networking technologies must have the grade of service and QoS (QoS) features (shown in Table I.4) to reduce the impact on real-time services.

Table I.4 – Quality of service support requirements

Number	Requirement
Q.1	**QoS mechanism**: All home networks must have a QoS mechanism capable of extending cable modem QoS to the device of consumption.
Q.2	**Smart forwarding**: To reduce traffic on low bandwidth networks, bridging points between networks (physical or logical) must forward only data destined for known addresses on the network.
Q.3	**Service priority**: Services received from the broadband network must have higher priority on the home network than traffic generated by devices connected to the home network unless overridden by the subscriber.
Q.4	**Service integrity through gateway**: If cable network access (gateway) applications such as firewalls and address translators are active in the home network, they must not corrupt or degrade the forwarding or reception of broadband services.
Q.5	**Standard QoS signalling**: The home network must use UPnP QoS signalling protocol for activating technology-specific QoS mechanisms as data services traverse end-to-end over various network technologies to the device of consumption in the home.
Q.6	**Data throughput**: Network interface devices must transfer data at a rate that meets or exceeds the aggregate load of connecting networks. The packet loss rate should average 10^{-8} under normal conditions.

I.7.5 Security requirements

IPNet2Home security requires a standard mechanism for authenticating a residential gateway and securing management messages between the cable headend and the residential gateway. It also needs a standard interface for the remote management and monitoring of firewall functions in a residential gateway (see Table I.5).

Table I.5 – Security requirements

Number	Requirement
SEC.1	The service provider must have the ability to remotely manage IPNet2Home-compliant firewall products, with user approval.
SEC.2	A firewall event logging/messaging interface that allows the service provider to monitor and review firewall activity must exist.
SEC.3	Firewall and network management messages between the cable headend and residential gateway must be authenticated and encrypted to protect against unauthorized monitoring and control.
SEC.4	A mechanism must exist to ensure the authenticity of IPNet2Home elements on the service provider's HFC network.
SEC.5	The home security level will be such that it is not easy for the average subscriber to gain unauthorized access to the HFC network and cable-based services.
SEC.6	Once a subscriber's account has been established, authentication of the IPNet2Home residential gateway with the service provider's provisioning system must be automatic.
SEC.7	The operator will have the ability to securely download software images, configuration files and firewall rule sets to the PS element.
SEC.8	IPNet2Home security will provide the necessary support for IPCablecom Secured DQoS through the firewall.
SEC.9	Network management messages between the cable headend and HA will be authenticated and optionally encrypted to protect against unauthorized monitoring and control.

I.7.6 IPNet2Home network address management (NAM) requirements

The NAM specification defines a standard mechanism for assigning IP addresses to the residential gateway and in-home devices that enable IP service delivery and network management capabilities (see Table I.6).

A device that provides a cable-friendly address translation (CAT) will need to be defined that is effectively transparent to the cable network, providing awareness of and management access to home devices.

Table I.6 – Network address management requirements

Number	Requirement
NAM.1	**Device accessibility**: IPNet2Home addressing mechanisms must be service-provider-controlled, and must provide the service provider with knowledge of and accessibility to IPNet2Home devices.
NAM.2	**Auto-addressing**: IPNet2Home address acquisition and management processes must not require human intervention (assuming that a user/household account has already been established).
NAM.3	**Scalability**: IPNet2Home address acquisition and management must be scalable to support the expected increase in the number of IP devices in homes.
NAM.4	**Routing integrity**: IPNet2Home addressing must do nothing that will compromise current cable network routing architectures (for example, source-based routing, MPLS).
NAM.5	**Multi-homing**: IPNet2Home addressing must avoid imposing multi-homing of in-home client devices.
NAM.6	**Persistent device addressing**: It is preferred that addresses for IPNet2Home devices remain the same after events such as a power cycle or Internet provider switch.
NAM.7	**Address server outage**: In-home communication must continue to work as provisioned during periods of remote address server outage. Addressing support must be provided for newly added devices and address expirations during remote address server outages. In addition, local name resolution must be provided during remote address server outages.
NAM.8	**Spurious HFC traffic**: IPNet2Home traffic management mechanisms must insulate the cable network from traffic generated by in-house peer-to-peer communications.
NAM.9	**Address conservation**: IP Addresses must be conserved when possible (both globally routable addresses and private cable network management addresses).

I.7.7 Video distribution requirements

Video services are a core business for cable operators and thus the distribution of video content over IPNet2Home networks merits special consideration. The distribution of entertainment quality video entails the same categories of features as those for general IP networking, but in the case of video, these features often must meet more stringent as well as additional requirements. For example, specific QoS and content protection requirements must be satisfied for the distribution of premium entertainment content. Video distribution requirements are detailed in this clause, and these requirements may be satisfied by a network that is physically separate from the general IP data network, or by a network that is physically converged with the general IP data network.

The following assumptions are being made for the IPNet2Home video distribution system:

- It is assumed that MPEG-based broadcast and unicast video sources, as well as IP-based video sources, must be supported by the IPNet2Home architecture.
- The primary focus for the IPNet2Home video network is the distribution of entertainment quality video. It is assumed that this functionality, once established, will be sufficient to support the delivery of informational quality video.

- Consideration of analog video transmissions in the home is out of scope for IPNet2Home.

The following categories of requirements for IPNet2Home video delivery are considered below: general, content protection, quality of service, video format and transport, video device provisioning and video device management.

I.7.7.1 General video distribution requirements

Number	General system design requirement
VGen.1	**Multiple types of video sources**: The home distribution of MPEG-based broadcast and unicast video sources, as well as IP-based video sources must be supported.
VGen.2	**Digital video distribution**: The home distribution of video in digital format must be supported.

I.7.7.2 Content protection requirements

Number	Content protection system design requirement
VPrt.1	**Rich DRM rule set**: A rich set of business rules (copy, playback, view time, etc.) must be provided in the content protection interface to enable a wide variety of business models.
VPrt.2	**Extent of content protection**: Content protection must be provided, as established by a DRM business rule set, for all devices participating in the transmission and/or consumption of video content.
VPrt.3	**Client authentication**: Authentication must be supported for all elements participating in the transmission and/or consumption of video content.
VPrt.4	**Encryption**: Content encryption must be supportable for video transmissions in the home.
VPrt.5	**Conditional access**: Conditional access rules must be maintained.
VPrt.7	**Transport independence**: The content protection mechanisms must be independent of the physical transport media, as well as of the transport protocol.
VPrt.8	**Dynamic management**: Information used to protect content (e.g., keying material) must be dynamically configurable and manageable by the network operator.

I.7.7.3 Quality of service requirements

Number	QoS system design requirement
VQoS.1	**Reservation types**: Both static (i.e., config-file or SNMP) and dynamic (i.e., UPnP QoS-based) QoS reservation mechanisms must be supported.
VQoS.2	**Network performance assessment**: The QoS characteristics must be discernible for each physical home-network segment in a service path.
VQoS.3	**In-service modification**: UPnP QoS based signalling between the service source and the client device that allows in-service renegotiation of reservation parameters must be supported. This permits the protection of service in the event that the performance of an in-progress QoS session falls below the established QoS parameters.
VQoS.4	**Admission control**: The QoS policy management and admission control must be administrable by the service provider (based upon priority, revenue opportunity, etc.) using UPnP QoS messaging.
VQoS.5	**Home service levels**: The IPNet2Home video distribution system must provide for service priorities on home networks, enabling specific video streams to take precedence over others.

I.7.7.4 Video format and transport requirements

Number	Video transport and format system design requirement
VTrans.3	**IP and non-IP transport**: Both IP and non-IP-based video transport over home networks must be supported.
VTrans.4	**Video format independence**: The home network must support multiple video encoding formats (e.g., MPEG 2/4, proprietary).

I.7.7.5 Video device provisioning requirements

Number	Device provisioning system design requirement
VProv.1	**Restricted access**: Client devices must be configurable to a state in which addressing and service flows are provided and controlled by the service provider.
VProv.2	**Provisioning of video-specific functions**: Functions that are specific to the delivery of video (for example CODEC parameters, buffer sizes, etc.) must be provisionable.

I.7.7.6 Video device management requirements

Number	Device management system design requirement
VMgmt.1	**Provisioning of video-specific functions**: Functions that are specific to the delivery of video (for example, CODEC parameters, buffer sizes, etc.) must be manageable.

Bibliography

[b-ITU-T G.9951] ITU-T Recommendation G.9951 (2005), *Phoneline networking transceivers – Foundation*.

[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 (2007), *Second-generation transmission systems for interactive cable television services – IP cable modems*.

[b-ITU-T J.160] ITU-T Recommendation J.160 (2005), *Architectural framework for the delivery of time-critical services over cable television networks using cable modems*.

[b-ITU-T J.197] ITU-T Recommendation J.197 (2005), *High level requirements for a Digital Rights Management (DRM) bridge from a cable access network to a home network.*

[b-ITU-T J.290] ITU-T Recommendation J.290 (2006), *Next generation set-top box core architecture*.

[b-ITU-T J.291] ITU-T Recommendation J.291 (2006), *Next generation set-top box cable architecture*.

[b-ITU-T J.292] ITU-T Recommendation J.292 (2006), *Next generation set-top box media independent architecture*.

[b-ITU-T J.360] ITU-T Recommendation J.360 (2006), *IPCablecom2 architecture framework.*

[b-IETF RFC 347] IETF RFC 347 (1972), *Echo Process*.

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

[b-IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program – Protocol Specification.*

[b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol – DARPA Internet Program – Protocol Specification*.

[b-IETF RFC 1034] IETF RFC 1034 (1987), *Domain names – Concepts and facilities.*

[b-IETF RFC 1157] IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP).*

[b-IETF RFC 1350] IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2).*

[b-IETF RFC 1631] IETF RFC 1631 (1994), *The IP Network Address Translator (NAT).*

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

[b-IETF RFC 2210] IETF RFC 2210 (1997), *The Use of RSVP with the IETF Integrated Services.*

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations.*

[b-IETF RFC 2814] IETF RFC 2814 (2000), *SBM (Subnet Bandwidth Manager): A Protocol for RSVP-based Admission Control over IEEE 802-style networks.*

[b-IETF RFC 2979] IETF RFC 2979 (2000), *Behavior of and Requirements for Internet Firewalls*.

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

[b-UQA] UPnP QoS Architecture:2, 16 October 2006.

[b-UQM] UPnP QoS Manager:2, *Service Template Version 1.01*, 16 October 2006.

[b-UQP] UPnP QoS Policy Holder:2, *Service Template Version 1.01*, 16 October 2006.

[b-URD] UPnP QoS Device:2, *Service Template Version 1.01*, 16 October 2006.

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, 2008